Kaspersky Security 10 for Mobile

Guide d'installation

Cher utilisateur !

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

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

Date d'édition : 22/01/2013

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

TABLE DES MATIERES

PRESENTATION DU GUIDE

Ce document est le *Guide d'installation de Kaspersky Security 10 for Mobile*.

Ce guide s'adresse aux experts techniques responsables pour l'installation et l'administration de Kaspersky Security 10 for Mobile (ci-après : Kaspersky Security), ainsi que pour le support aux entreprises qui utilisent Kaspersky Security.

Ce guide a pour objectifs :

- Fournir une description générale du fonctionnement de Kaspersky Security 10, des configurations requises, des scénarios type de déploiement, des particularités de l'intégration aux autres applications.
- Aider à établir un schéma de déploiement de Kaspersky Security 10 for Mobile dans le réseau d'entreprise.
- Décrire la préparation à l'installation de Kaspersky Security 10 for Mobile, l'installation et l'activation de l'application.
- Donner des conseils sur le support et l'administration de Kaspersky Security 10 for Mobile après son installation.
- Présenter les sources complémentaires d'informations sur l'application et les méthodes pour obtenir un support technique.

DANS CETTE SECTION

DANS CE DOCUMENT

Ce document contient les sections suivantes.

Sources d'informations sur l'application (cf.la page 8)

Cette section contient la description des sources d'informations sur l'application et les renseignements sur les sites Web que vous pouvez consulter pour discuter du fonctionnement de l'application.

Kaspersky Security 10 for Mobile (cf.la page 10)

Cette section reprend les informations sur l'affectation, les fonctionnalités principales et la structure de l'application Kaspersky Security 10 for Mobile.

Schémas typiques de déploiement de l'application (cf.la page 15)

Cette section décrit les schémas typiques de déploiement de l'application Kaspersky Security 10 for Mobile.

Préparation de l'installation de l'application (cf.la page 21)

Cette section décrit la procédure de configuration de la gestion des appareils mobiles via Kaspersky Security Center pour le déploiement de l'application Kaspersky Security.

Notification sur les marques

Cette section énumère les marques des propriétaires étrangers, utilisés dans le document.

Index

Cette section permet de trouver rapidement les informations souhaitées dans le document.

CONVENTIONS

Le texte du document est suivi des éléments de sens sur lesquels nous attirons votre attention : avertissements, conseils, exemples.

Les conventions sont utilisées pour identifier les éléments de sens. Les conventions et les exemples de leur utilisation sont repris dans le tableau ci-dessous.

Tableau 1. Conventions

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
N'oubliez pas que...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent les informations sur les actions indésirables potentielles qui peuvent amener à la perte des informations, à une défaillance du matériel ou à un échec du système d'exploitation.
Il est conseillé d'utiliser ...	Les remarques sont encadrées. Les remarques peuvent contenir des conseils utiles, des recommandations, des valeurs spécifiques des paramètres ou des cas particuliers importants dans le fonctionnement de l'application.
Exemple : ...	Les exemples sont présentés sur un fond jaune sous le titre "Exemple".
La *mise à jour*, c'est ... L'événement *Bases dépassées* survient.	Les éléments de sens suivants sont en italique : • nouveaux termes ; • noms des états et des événements de l'application.
Appuyez sur la touche **ENTER**. Appuyez sur la combinaison des touches **ALT+F4**.	Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Il faut appuyer simultanément sur ces touches.
Cliquez sur le bouton **Activer**.	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont en caractères mi-gras.
Pour planifier une tâche, procédez comme suit :	Les phrases d'introduction des instructions sont en italique et ont l'icône "flèche".
Dans la ligne de commande, saisissez le texte help Les informations suivantes s'affichent : Indiquez la date au format JJ:MM:AA.	Les types suivants du texte apparaissent dans un style spécial : • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir par l'utilisateur.
<Nom d'utilisateur>	Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable. Par ailleurs, les parenthèses angulaires sont omises.

SOURCES D'INFORMATIONS SUR L'APPLICATION

Cette section contient la description des sources d'informations sur l'application et les renseignements sur les sites Web que vous pouvez consulter pour discuter du fonctionnement de l'application.

Vous pouvez ainsi choisir celle qui s'adapte le mieux à votre situation en fonction de l'importance et de l'urgence de la question.

DANS CETTE SECTION

SOURCES D'INFORMATIONS POUR UNE AIDE AUTONOME

Vous pouvez utiliser les sources suivantes pour rechercher les informations sur l'application :

- page du site de Kaspersky Lab ;
- page sur le site du support technique (base de connaissances) ;
- aide électronique ;
- La documentation.

Si vous ne pouvez pas résoudre le problème, nous vous recommandons de vous adresser au Service d'assistance technique de Kaspersky Lab (cf. section "Support technique par téléphone" à la p. 55).

Une connexion Internet est requise pour utiliser les sources d'informations sur le site Web de Kaspersky Lab.

Page du site de Kaspersky Lab

Le site Web de Kaspersky Lab contient une page particulière pour chaque application.

La page (http://www.kaspersky.com/fr/targeted_security) fournit des informations générales sur l'application, ses fonctionnalités et ses particularités.

La page http://www.kaspersky.com/fr/ contient le lien sur la boutique en ligne. Le lien permet d'acheter l'application ou de renouveler le droit d'utilisation de l'application.

Page sur le site du support technique (banque de solutions)

La Base de connaissances est une section du site Internet du Support Technique contenant les recommandations pour travailler avec les applications de Kaspersky Lab. La Base de connaissance est composée des articles d'aide regroupés selon les thèmes.

La page de l'application dans la Base de connaissances (http://support.kaspersky.com/fr/ks10mob) permet de trouver les articles qui proposent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application.

Les articles peuvent répondre à des questions en rapport non seulement avec Kaspersky Security, mais également avec d'autres applications de Kaspersky Lab. De plus, ils peuvent fournir des informations sur le Support technique en général.

Aide électronique

L'aide électronique de l'application est composée de fichiers d'aide.

L'aide contextuelle reprend les informations sur chacune des fenêtres de l'application : la liste, la description des paramètres et les liens pour les tâches qui utilisent ces paramètres.

Documentation

La distribution de l'application contient des documents qui vous permettent d'installer et d'activer l'application sur les ordinateurs du réseau d'entreprise, de configurer les paramètres de son fonctionnement et d'obtenir des renseignements sur les méthodes principales d'utilisation de l'application.

DISCUSSION SUR LES LOGICIELS DE KASPERSKY LAB DANS LE FORUM

Si votre question n'est pas urgente, vous pouvez la soumettre aux experts de Kaspersky Lab et aux autres utilisateurs de nos applications dans notre forum (http://forum.kaspersky.fr).

Sur le forum, vous pouvez consulter les sujets publiés, ajouter des commentaires, créer une nouvelle discussion ou lancer des recherches.

CONTACTER LE SERVICE COMMERCIAL

Si vous avez des questions sur la sélection, sur l'achat ou sur la prolongation de la durée d'utilisation de l'application, vous pouvez contacter nos experts du service commercial à l'aide d'un des moyens suivants :

- En appelant à notre office central à Moscou (http://www.kaspersky.com/fr/contacts).
- En envoyant un message avec la question à l'adresse de messagerie sales@kaspersky.com.

La réponse sera donnée en français ou en anglais suivant votre demande.

CONTACTER LE SERVICE DE GEOLOCALISATION ET DE REDACTION DE LA DOCUMENTATION TECHNIQUE

Pour contacter l'Équipe de rédaction de la documentation, envoyez un message à docfeedback@kaspersky.com. En tant que sujet du message, il faut indiquer "Kaspersky Help Feedback: Kaspersky Security 10 for Mobile".

KASPERSKY SECURITY 10 FOR MOBILE

Kaspersky Security 10 for Mobile assure la protection des appareils mobiles tournant sous les systèmes d'exploitation Android, iOS, BlackBerry, Microsoft® Windows Mobile et Symbian contre les virus et les autres programmes qui constituent une menace, contre les appels et les SMS indésirables, ainsi que les menaces Web. L'application permet de contrôler l'activité réseau de l'utilisateur et de protéger les informations confidentielles contre tout accès non autorisé. L'application met à disposition de l'utilisateur de différents composants pour faire face à de différents types de menaces. Cela permet de configurer en souplesse les paramètres de l'application en fonction des besoins d'un utilisateur particulier. L'accessibilité des composants varie en fonction du système d'exploitation de l'appareil mobile.

Kaspersky Security 10 for Mobile prend en charge le système d'administration à distance de Kaspersky Security Center. Ce système permet à l'administrateur du réseau d'entreprise d'effectuer à distance les actions suivantes :

- installer l'application sur les appareils mobiles ;
- configurer les paramètres de fonctionnement de l'application pour un groupe d'appareils ou pour un appareil distinct ;
- générer des rapports sur le fonctionnement des composants de l'application installée sur les appareils mobiles ;
- supprimer l'application depuis les appareils tournant sous Android.

L'application Kaspersky Security 10 for Mobile est équipée des composants de protection suivants :

- **Anti-Virus**. Ce composant permet de détecter et de neutraliser les menaces sur l'appareil mobile à l'aide des bases antivirus de l'application et du service nuage de Kaspersky Security Network. L'Anti-Virus comprend les composants suivants : la protection, l'analyse et la mise à jour.
    - La **protection** permet de découvrir les menaces dans les fichiers ouverts, d'analyser les nouvelles applications et de prévenir l'infection de l'appareil en temps réel.
    - La **Protection** est lancée à la demande pour tout le système de fichiers, la mémoire vive ou un dossier distinct. L'analyse complète permet de rechercher la présence éventuelle d'objets malveillants dans tout le système de fichiers de l'appareil tandis que l'analyse d'un dossier porte sur un dossier en particulier. L'analyse complète et l'analyse d'un dossier détectent les menaces dans les fichiers installés, mais non ouverts, ainsi que les menaces dans les fichiers qui sont actuellement ouverts. L'analyse de la mémoire permet de détecter les menaces uniquement dans les fichiers ouverts.
    - **La mise à jour** permet de télécharger de nouvelles bases antivirus de l'application.
- **Protection Vie Privée**. Ce composant permet de masquer les informations confidentielles de l'utilisateur lorsque son appareil est utilisé par une tierce personne. Il peut masquer ou afficher toutes les informations relatives aux numéros des abonnés indiqués, telles que données dans la liste de contacts, l'historique des conversations et des échanges SMS avec ces contacts. Le composant permet également de masquer l'acceptation des appels entrants et des SMS en provenance des numéros indiqués.
- **Antivol**. Ce composant protège les informations stockées dans l'appareil contre tout accès non autorisé en cas de perte ou de vol. Le composant permet de verrouiller et de localiser l'appareil ou de supprimer les données de l'appareil à l'aide d'une instruction SMS ou de Kaspersky Security Center.
- **Filtre des appels et SMS**. Le composant permet de bloquer les SMS et les appels indésirables en fonction du mode sélectionné. Le filtrage des SMS et des appels s'effectue à l'aide des listes des contacts autorisés et interdits. En fonction des paramètres, le composant bloque ou accepte les appels et les SMS en provenance de contacts interdits et autorisés. En plus du mode sélectionné, le composant permet d'activer l'autorisation des événements entrants de tous les numéros repris dans le répertoire téléphonique de l'appareil (Contacts) ou le blocage des appels ou messages en provenance de numéros contenant des lettres.
- **Protection Internet**. Le composant permet de bloquer les sites Internet malveillants qui distribuent un code malveillant, les sites Internet fictifs (d'hameçonnage) qui servent à voler les données confidentielles de l'utilisateur telles que mots de passe pour les banques en ligne, les enchères en ligne et les systèmes de paiement afin d'obtenir l'accès à ses comptes financiers. Le composant analyse les sites Web avant leur

ouverture à l'aide du service nuage de Kaspersky Security Network. A l'issue de l'analyse, la protection Internet ouvre le site considéré comme inoffensif et bloque le site considéré comme malveillant. Le composant prend également en charge le filtrage des sites Web en fonction des catégories définies dans Kaspersky Security Network ce qui permet à l'administrateur de limiter l'accès aux pages Web dans la catégorie "Jeux de hasard", "Réseaux sociaux", etc.

- **Pare-feu**. Le composant contrôle les connexions de réseau de l'appareil mobile. Il permet de définir les connexions qui seront autorisées ou bloquées.

- **Contrôle des Applications**. Le composant permet de configurer à l'aide de Kaspersky Security Center les paramètres de lancement des applications sur l'appareil mobile de l'utilisateur. L'administrateur peut indiquer des applications obligatoires pour l'installation sur l'appareil de l'utilisateur et créer des listes d'applications dont le lancement est autorisé ou interdit. Le composant bloque toute tentative de lancement d'applications interdites et consigne les informations sur les tentatives de cet accès dans les rapports de Kaspersky Security Center. Le composant prend également en charge la création et l'utilisation du conteneur qui est une enveloppe spéciale pour les applications mobiles permettant de coordonner les activités des applications incluses dans le conteneur pour assurer la protection des données d'entreprise stockées dans l'appareil. Les applications dans le conteneur peuvent être utilisées comme des applications autorisées ou obligatoires pour l'installation.

- **Gestion de l'appareil**. Ce composant permet de configurer l'utilisation obligatoire du mot de passe pour déverrouiller l'appareil mobile et la longueur minimale de ce mot de passe. En plus, il permet d'interdire l'utilisation des réseaux Wi-Fi, de la caméra et du module Bluetooth sur l'appareil.

- **Cryptage**. Protège les informations contre toute utilisation par une tierce personne en cas d'accès non autorisé à l'appareil. Lorsque l'appareil passe en mode économie d'énergie le composant crypte les dossiers non système sélectionnés qui sont stockés dans la mémoire de l'appareil ou sur la carte mémoire. Pour accéder aux données dans les dossiers cryptés, il faut saisir le code secret.

DANS CETTE SECTION

NOUVEAUTES

La nouvelle version de Kaspersky Security 10 for Mobile a reçu les améliorations suivantes :

- Un nouveau schéma de déploiement de l'application sur les appareils tournant sous Android via Kaspersky Security Center à l'aide d'une diffusion des messages textes vers les numéros des téléphones d'utilisateurs ou des messages électroniques vers les adresses de messagerie d'entreprise d'utilisateurs.

- La prise en charge des appareils tournant sous le système d'exploitation Android version 4.0 ou supérieure.

- La prise en charge des appareils mobiles tournant sous iOS. Pour ce système d'exploitation, Kaspersky Security 10 bloque les sites Web appartenant à des catégories spécifiées et détecte le jailbreaking du système.

- L'installation à distance de l'application sur les appareils tournant sous iOS et son administration à l'aide de Kaspersky Security Center.

- Désormais, l'application peut bloquer des ressources Web en fonction des catégories spécifiées dans le service nuage Kaspersky Security Network ce qui permet de limiter l'accès aux ressources Web classées malveillantes, d'hameçonnage ou appartenant à une autre catégorie indésirable.

- La prise en charge de la création et l'utilisation des conteneurs qui sont des programmes mobiles dans une enveloppe spéciale permettant de coordonner les activités des applications incluses dans le conteneur pour assurer la protection des données d'entreprise stockées dans l'appareil. Les applications dans le conteneur peuvent être utilisées comme des applications autorisées ou obligatoires pour l'installation.

- L'analyse heuristique lors du fonctionnement de la protection.
- La détection de l'accès à l'appareil avec les privilèges de l'administrateur (l'accès racine) pour les appareils tournant sous Android et du jailbreaking pour les appareils tournant sous iOS, ainsi que la sélection des actions à effectuer dans les deux cas.
- Les appareils tournant sous Android ont reçu les améliorations suivantes :
  - Kaspersky Security Center permet d'indiquer les applications dont le lancement sur l'appareil est autorisé ou interdit et de spécifier les applications obligatoires pour l'installation sur l'appareil de l'utilisateur.
  - L'application assure l'analyse de nouveaux programmes après l'installation à l'aide du service nuage Kaspersky Security Network.
  - La détection des logiciels publicitaires et des programmes que les individus malintentionnés peuvent utiliser pour nuire à l'appareil et aux données de l'utilisateur.
  - activation de l'application Kaspersky Security 10 en tant qu'administrateur de l'appareil. Cette opération donne l'accès à des fonctionnalités avancées de la protection des appareils tournant sous Android.
  - suppression de l'application de l'appareil depuis ses paramètres sur l'appareil ou à distance à l'aide de Kaspersky Security Center.
- Des fonctionnalités supplémentaires pour le composant Antivol : désormais vous pouvez lancer l'Antivol à distance et supprimer toutes les données de l'appareil à l'aide d'une instruction envoyé à l'aide de Kaspersky Security Center.
- Les fonctionnalités du composant Filtre des appels et SMS sont améliorées : désormais, vous pouvez importer les listes des contacts autorisés et interdites depuis le journal des appels et la liste des SMS.
- La liste des événements consignés dans les rapports sur le fonctionnement de l'application a été élargie.

DISTRIBUTION

La distribution de l'application Kaspersky Security 10 for Mobile contient les composants suivants :

- sc_package — qui contient un ensemble de fichiers d'installation (cf. section "Distribution complète de Kaspersky Security 10" à la page 13) pour quatre systèmes d'exploitation pris en charge par Kaspersky Security 10.
- sc_plugin qui contient un module externe d'administration de l'application (cf. section " Distribution du module externe d'administration Kaspersky Security 10 for Mobile " à la page 13) Kaspersky Security 10 à l'aide de Kaspersky Security Center.
- standalone qui continent des fichiers d'installation de l'application (cf. section " Distributions pour une installation autonome" à la page 14) pour tous les systèmes d'exploitation pris en charge. Ces fichiers permettent d'installer l'application sans l'administrateur.

DANS CETTE SECTION

DISTRIBUTION COMPLETE DE KASPERSKY SECURITY 10

La distribution de l'application comprend une archive autodécompactable sc_package qui contient des fichiers nécessaires à l'installation de l'application sur toutes les plates-formes mobiles Android, BlackBerry, Symbian et Windows Mobile :

- `adb.exe, AdbWinApi.dll, AdbWinUsbApi.dll` – kit des fichiers de l'installation du logiciel sur les appareils sous le système d'exploitation Android ;
- `endpoint_8_0_0_37_fr.cab` — fichier d'installation pour le système d'exploitation Microsoft Windows Mobile ;
- `endpoint8_mobile_8_1_44_fr.sisx` — fichier d'installation pour le système d'exploitation Symbian ;
- `endpoint8_Mobile_8_1_29_fr.zip` — fichier d'installation pour le système d'exploitation BlackBerry ;
- `installer.ini` – fichier de configuration contenant les paramètres de connexion au Serveur d'administration ;
- `KSM_10_1_75_fr.apk` — fichier d'installation pour le système d'exploitation Android ;
- `kmlisten.exe` est un utilitaire de livraison du package de distribution sur un appareil mobile via une station de travail.
- `kmlisten.ini` est un fichier de configuration contenant les paramètres pour l'utilitaire de livraison du package d'installation ;
- `kmlisten.kpd` — fichier contenant la description du logiciel ;
- dossier technique :
  - Guide d'installation de Kaspersky Security 10 for Mobile ;
  - aide contextuelle du module externe d'administration de Kaspersky Security 10 for Mobile ;
  - aide contextuelle de l'application pour le système d'exploitation Android ;
  - aide contextuelle de l'application pour le système d'exploitation iOS ;
  - aide contextuelle de l'application pour le système d'exploitation BlackBerry ;
  - aide contextuelle de l'application pour le système d'exploitation Symbian ;
  - aide contextuelle de l'application pour le système d'exploitation Windows Mobile.

DISTRIBUTION DU MODULE EXTERNE D'ADMINISTRATION DE KASPERSKY SECURITY 10 FOR MOBILE

La distribution de l'application comprend une archive autodécompactable sc_plugin contenant un fichier exécutable klcfginst.exe qui est un fichier d'installation du module externe d'administration de l'application Kaspersky Security 10 for Mobile à l'aide du système d'administration à distance de Kaspersky Security Center.

DISTRIBUTIONS POUR UNE INSTALLATION AUTONOME

La distribution de l'application comprend le dossier standalone qui contient les fichiers d'installation pour tous les systèmes d'installation pris en charge :

- `KSM_10_1_75_fr.apk` est un fichier d'installation de l'application de Kaspersky Security 10 pour le système d'exploitation Android ;
- `KSM_10_1_32_unsigned.app.zip` est un fichier d'installation de l'application de Kaspersky Security 10 pour le système d'exploitation iOS ;
- `endpoint_8_0_0_37_fr.cab` — fichier d'installation pour le système d'exploitation Microsoft Windows Mobile ;
- `endpoint8_mobile_8_1_44_fr.sisx` — fichier d'installation pour le système d'exploitation Symbian ;
- `endpoint8_Mobile_8_1_29_fr.zip` — fichier d'installation pour le système d'exploitation BlackBerry ;
- Dossier technique :
  - Guide d'installation de Kaspersky Security 10 for Mobile ;
  - aide contextuelle du module externe d'administration de Kaspersky Security 10 for Mobile ;
  - aide contextuelle de l'application pour le système d'exploitation Android ;
  - aide contextuelle de l'application pour le système d'exploitation Windows Mobile ;
  - aide contextuelle de l'application pour le système d'exploitation Symbian OS ;
  - aide contextuelle de l'application pour le système d'exploitation BlackBerry.

CONFIGURATIONS LOGICIELLES ET MATERIELLES

Pour pouvoir utiliser l'application Kaspersky Security 10 for Mobile sur les appareils mobiles d'utilisateurs, ces appareils doivent avoir la configuration logicielle suivante :

- Android 2.2, 2.3, 3.0, 3.1, 3.2, 4.0, 4.1.
- Apple iOS 4.0, 4.1, 4.2, 4.3, 5.0, 5.1, 6.0.
- BlackBerry 4.5, 4.6, 4.7, 5.0, 6.0, 7.0, 7.1.
- Symbian OS 9.1, 9.2, 9.3, 9.4 Series 60® UI.
- Symbian^3, Symbian Anna, Symbian Belle (uniquement pour les appareils mobiles Nokia®).
- Windows Mobile 5.0, 6.0, 6.1, 6.5.

Pour déployer Kaspersky Security 10 for Mobile dans le réseau, le système d'administration à distance doit avoir la configuration logicielle suivante :

- Kaspersky Security Center 10.0.

SCHEMAS TYPIQUES DE DEPLOIEMENT DE L'APPLICATION

Cette section décrit les schémas typiques de déploiement de l'application Kaspersky Security 10 for Mobile.

Les schémas de déploiement de Kaspersky Security dépendent du système d'exploitation installé sur les appareils mobiles des utilisateurs.

DANS CETTE SECTION

SCHEMAS DE DEPLOIEMENT DE L'APPLICATION POUR DES APPAREILS TOURNANT SOUS ANDROID

L'installation de l'application sur un appareil tournant sous le système d'exploitation Android peut s'effectuer de l'une des manières suivantes :

- Via l'envoi aux utilisateurs de notifications électroniques avec le lien vers la distribution de l'application (cf. section "Schéma de déploiement via l'envoi de notifications électroniques " à la p. 16).
- Via l'envoi aux utilisateurs de messages textes (SMS) avec le lien vers la distribution de l'application (cf. section " Schéma de déploiement via l'envoi de messages textes" à la p. 17).
- Via les postes de travail auxquels les utilisateurs connectent les appareils mobiles (cf. section " Schéma de déploiement via le poste de travail " à la p. 18).

Avant d'installer l'application, vous devez ajouter les appareils mobiles des utilisateurs aux ordinateurs administrés et créer une stratégie de groupe pour transférer les données sur la licence ainsi que les paramètres de fonctionnement de l'application vers les appareils mobiles. Après cela, préparez la distribution de l'application pour l'installation sur les appareils mobiles des utilisateurs. La copie de la distribution sur les appareils mobiles et l'installation de l'application sur les appareils mobiles de l'utilisateur sont exécutées indépendamment.

Les utilisateurs peuvent également installer la distribution de Kaspersky Security sur leur appareil mobile sans l'intervention de l'administrateur (cf. section "Installation de l'application sans l'intervention de l'administrateur" à la p. 18) comme une application standard d'Android.

DANS CETTE SECTION

SCHEMA DE DEPLOIEMENT VIA L'ENVOI DE NOTIFICATIONS ELECTRONIQUES

Le schéma de déploiement de l'application via l'envoi d'un courrier électronique permet aux utilisateurs d'ajouter spécifiquement une distribution de l'application préparée contenant les paramètres de connexion au serveur d'administration ainsi il ne leur est pas nécessaire de les indiquer manuellement. Cette distribution s'appelle paquet d'installation autonome.

Le schéma comprend les étapes suivantes :

1. Configuration de l'administration des appareils mobiles via Kaspersky Security Center. Cette étape permet de connecter les appareils mobiles au serveur d'administration (cf. section "Préparation de l'installation de l'application" à la p. 21).

2. Installation du module externe d'administration de Kaspersky Security 10 for Mobile.

3. Création des groupes pour les appareils mobiles faisant partie des ordinateurs administrés dans le système Kaspersky Security Center.

   Les appareils équipés de Kaspersky Security 10 for Mobile seront placés ajoutés à ces groupes manuellement ou selon des règles du transfert automatique.

4. Création d'une stratégie de groupe pour la gestion des paramètres de Kaspersky Security 10 for Mobile.

5. Création des règles de déplacement automatique des appareils mobiles dans le groupe.

6. Analyse des comptes des utilisateurs sur l'existence de messagerie électronique.

7. Création du paquet d'installation pour Kaspersky Security 10 for mobile.

8. Configuration des paramètres du paquet d'installation pour Kaspersky Security 10 for mobile.

9. Création du paquet autonome d'installation pour Kaspersky Security 10 for mobile.

   Cette étape permet au paquet autonome de contenir les paramètres de connexion au serveur d'administration et accessible au dossier partagé et au serveur web de Kaspersky Security Center. Lors de la diffusion, vous pouvez spécifier n'importe quelle ressource et indiquer le lien nécessaire ou activer le paquet autonome d'installation dans le courrier comme fichier joint.

10. Composition et envoi du courrier avec un lien vers le paquet autonome aux utilisateurs d'appareils mobiles.

    Le lien peut être envoyé sous forme d'un texte ou d'un code QR qui sera lu directement par l'appareil mobile.

11. Téléchargement du paquet autonome d'installation sur l'appareil mobile. Cette étape permet à l'utilisateur de télécharger sur l'appareil la distribution de l'application préconfigurée jointe au courrier ou située sur une ressource partagée.

12. Installation de l'application sur l'appareil mobile.

13. Activation de l'application (cf.la page 49) sur les appareils mobiles des utilisateurs.

Le schéma susmentionné de déploiement de l'application sur l'appareil tournant sous Android convient uniquement pour l'installation de Kaspersky Security 10 for mobile. Le module externe d'administration de Kaspersky Security 10 for Kaspersky Security Center peut également gérer les appareils équipés d'une précédente version de l'application. Pour utiliser toutes les fonctionnalités de l'application, les spécialistes de Kaspersky Lab recommandent de mettre à jour la dernière version (cf. section "Mise à jour de la dernière version de l'application" à la p. 32).

SCHEMA DE DEPLOIEMENT VIA L'ENVOI DE MESSAGES TEXTES

Le schéma de déploiement de l'application via l'envoi à l'aide de messages textes permet aux utilisateurs d'ajouter spécialement la distribution de l'application préparée contenant les paramètres de connexion au serveur d'administration, ainsi il ne leur est pas nécessaire de les indiquer manuellement. Cette distribution s'appelle paquet d'installation autonome.

L'envoi de messages textes (SMS) avec un lien vers le paquet autonome d'installation est possible uniquement sur un appareil équipé du module GSM.

Le schéma comprend les étapes suivantes :

1. Configuration de l'administration des appareils mobiles via Kaspersky Security Center. Cette étape permet de connecter les appareils mobiles au serveur d'administration (cf. section "Préparation de l'installation de l'application" à la p. 21).
2. Installation du module externe d'administration de Kaspersky Security 10 for Mobile.
3. Création des groupes pour les appareils mobiles faisant partie des ordinateurs administrés dans le système Kaspersky Security Center.

   Les appareils équipés de Kaspersky Security 10 for Mobile seront placés ajoutés à ces groupes manuellement ou selon des règles du transfert automatique.
4. Création d'une stratégie de groupe pour la gestion des paramètres de Kaspersky Security 10 for Mobile.
5. Création des règles de déplacement automatique des appareils mobiles dans le groupe.
6. Configuration du mode de livraison des messages textes (SMS) aux utilisateurs.
7. Analyse des comptes des utilisateurs sur l'existence de numéros de téléphone.
8. Création du paquet d'installation pour Kaspersky Security 10 for mobile.
9. Configuration des paramètres du paquet d'installation pour Kaspersky Security 10 for mobile.
10. Création du paquet autonome d'installation pour Kaspersky Security 10 for mobile.

    Cette étape permet au paquet autonome de contenir les paramètres de connexion au serveur d'administration et accessible au dossier partagé et au serveur web de Kaspersky Security Center. Lors de l'envoi, vous devez sélectionner le chemin d'accès au serveur web de Kaspersky Security Center.
11. Composition et envoi du message texte avec un lien vers le paquet autonome d'installation aux utilisateurs d'appareils mobiles.
12. Téléchargement du paquet autonome d'installation sur l'appareil mobile. Cette étape permet à l'utilisateur de télécharger sur l'appareil la distribution de l'application au serveur web de Kaspersky Security Center.
13. Installation de l'application sur l'appareil mobile.
14. Activation de l'application (cf.la page 49) sur les appareils mobiles des utilisateurs.

Le schéma susmentionné de déploiement de l'application sur l'appareil tournant sous Android convient uniquement pour l'installation de Kaspersky Security 10 for mobile. Le module externe d'administration de Kaspersky Security 10 for Kaspersky Security Center peut également gérer les appareils équipés d'une précédente version de l'application. Pour utiliser toutes les fonctionnalités de l'application, les spécialistes de Kaspersky Lab recommandent de mettre à jour la dernière version (cf. section "Mise à jour de la dernière version de l'application" à la p. 32).

SCHEMA DE DEPLOIEMENT VIA LE POSTE DE TRAVAIL

Déploiement de l'application via le poste de travail lorsque les utilisateurs connectent les appareils mobiles aux ordinateurs de bureau.

Le déploiement via le poste de travail s'effectue selon les étapes suivantes :

1. Configuration de l'administration des appareils mobiles via Kaspersky Security Center. Cette étape permet de connecter les appareils mobiles au serveur d'administration (cf. section "Préparation de l'installation de l'application" à la p. 21).

2. Installation du module externe d'administration de Kaspersky Security 10 for Mobile.

3. Création des groupes pour les appareils mobiles faisant partie des ordinateurs administrés dans le système Kaspersky Security Center.

   Les appareils équipés de Kaspersky Security 10 for Mobile seront placés ajoutés à ces groupes manuellement ou selon des règles du transfert automatique.

4. Création des règles de déplacement automatique des appareils mobiles dans le groupe.

5. Création d'une stratégie de groupe pour la gestion des paramètres de Kaspersky Security 10 for Mobile.

6. Création du paquet d'installation pour l'installation à distance de Kaspersky Security 10 for mobile.

7. Configuration des paramètres du paquet d'installation pour l'installation à distance de Kaspersky Security 10 for mobile.

8. La création de l'installation à distance permet de répartir la distribution de l'application Kaspersky Security 10 for mobile sur les postes de travail des utilisateurs et d'installer l'utilitaire de livraison de la distribution sur les appareils mobiles.

9. Téléchargement de la distribution de l'application sur l'appareil mobile. Cette étape permet, à l'aide de l'utilitaire kmlisten.exe, à l'utilisateur de copier la distribution de l'application sur l'appareil mobile.

10. Installation de l'application sur l'appareil mobile. Cette étape permet à l'utilisateur de lancer l'installation de l'application sur l'appareil mobile.

11. Activation de l'application (cf.la page 49) sur l'appareil mobile de l'utilisateur.

INSTALLATION DE L'APPLICATION SUR UN APPAREIL SANS L'INTERVENTION DE L'ADMINISTRATEUR

Le téléchargement immédiat du fichier d'installation sur l'appareil est utilisé lorsque les utilisateurs sont en mesure d'installer seuls l'application, par exemple en téléchargeant le fichier d'installation sur Google Play.

Dans ce cas, ne préparez pas la distribution de l'application, l'utilisateur indiquera lui-même les paramètres de connexion au serveur d'administration (cf. section "Préparation de l'application au fonctionnement sur l'appareil " à la p. 48) lors du lancement initial de l'application.

Le schéma de déploiement comprend les étapes suivantes :

1. Configuration de l'administration des appareils mobiles via Kaspersky Security Center. Cette étape permet de connecter les appareils mobiles au serveur d'administration (cf. section "Préparation de l'installation de l'application" à la p. 21).

2. Installation du module externe d'administration de Kaspersky Security 10 for Mobile.

3. Création de groupe pour placer les appareils mobiles sur lesquels sera répartie la distribution de l'application Kaspersky Security 10 for mobile.

4. Création des règles de déplacement automatique des appareils mobiles dans le groupe.

5. Création de stratégies pour la gestion des paramètres de Kaspersky Security 10 for mobile.

6. Installation de l'application sur l'appareil mobile. Cette étape permet à l'utilisateur de lancer l'installation de l'application sur l'appareil mobile.

7. Configuration initiale de l'application. Cette étape permet à l'utilisateur d'indiquer les paramètres de connexion de l'appareil mobile au serveur d'administration (cf. section "Préparation de l'application au fonctionnement sur l'appareil" à la p. 48).

8. Activation de l'application (cf.la page 49) sur l'appareil mobile.

SCHEMA DE DEPLOIEMENT DE L'APPLICATION POUR DES APPAREILS TOURNANT SOUS IOS

Les moyens iOS MDM sont utilisés pour délivrer le logiciel Kaspersky Security sur les appareils. La gestion centralisée des paramètres du logiciel est effectuée à l'aide des politiques concernant les groupes des appareils gérés. Pour plus d'information, adressez-vous au *Guide d'administrateur Kaspersky Security Center*.

Le déploiement du logiciel sur les appareils mobiles sous le système d'exploitation iOS est effectué via le serveur iOS MDM par les étapes suivantes :

1. Configuration de l'administration des appareils mobiles via Kaspersky Security Center. A cette étape, vous avez la possibilité de connecter les appareils mobiles au Serveur d'administration.

2. Déploiement du Serveur des appareils mobiles iOS MDM et connexion aux appareils des utilisateurs. A cette étape, vous avez la possibilité de connecter les appareils mobiles sous la gestion iOS au Serveur d'administration. Pour plus d'information, adressez-vous au *Guide de la mise en œuvre Kaspersky Security Center.*

3. Installation du module externe d'administration de Kaspersky Security 10 for Mobile.

4. La création des groupes de la gestion centralisée des paramètres du logiciel installé sur les appareils mobiles d'utilisateurs.

5. La création de la règle du déplacement automatique dans un groupe des appareils mobiles détectés lors de la synchronisation.

6. Création de stratégies pour la gestion des paramètres de Kaspersky Security 10 for mobile.

7. La vérification des comptes utilisateur sur la présence d'une adresse électronique ou d'un numéro de téléphone pour y envoyer un message texte.

8. La création du profil iOS MDM pour gérer l'appareil à l'aide Kaspersky Security Center et la transmission du profil sur les appareils d'utilisateurs (cf. partie "Création et installation du profil iOS" à la page 46).

9. L'installation du profil iOS MDM sur les appareils d'utilisateurs (cf. partie "Création et installation du profil iOS" à la page 46).

10. L'installation du logiciel (cf. partie "Création et installation du profil iOS" à la page 47) sur les appareils mobiles d'utilisateurs. Cette étape permet à l'utilisateur de lancer l'installation de l'application sur l'appareil mobile.

11. La configuration initiale du logiciel (cf. partie "La préparation au fonctionnement du logiciel" à la page 48) sur les appareils d'utilisateurs. Sur cette étape, l'utilisateur indique la configuration de la connexion vers le Serveur d'administration.

12. Activation de l'application (cf.la page 49) sur les appareils mobiles des utilisateurs.

SCHEMA DE DEPLOIEMENT DE L'APPLICATION POUR DES APPAREILS TOURNANT SOUS BLACKBERRY, SYMBIAN, WINDOWS MOBILE

La distribution de Kaspersky Security 10 for Mobile (cf. section "Distribution" à la page 12) contient les distributions de l'application pour plusieurs systèmes d'exploitation. La plateforme BlackBerry, Symbian et Windows Mobile comprend les distributions de Kaspersky Endpoint Security 8.0 for Smartphone.

Le module externe d'administration de Kaspersky Security 10 for mobile installé dans le système d'administration distant peut gérer les appareils équipés de Kaspersky Endpoint Security 8.0 for Smartphone.

Le schéma de déploiement de l'application pour les appareils tournant sous les systèmes d'exploitation BlackBerry, Symbian et Windows Mobile comprend les étapes suivantes :

1. Configuration de l'administration des appareils mobiles via Kaspersky Security Center. Cette étape permet de connecter les appareils mobiles au serveur d'administration (cf. section "Préparation de l'installation de l'application" à la p. 21).

2. Installation du module externe d'administration de Kaspersky Security 10 for Mobile.

3. Création des groupes pour les appareils mobiles faisant partie des ordinateurs administrés dans le système Kaspersky Security Center.

   Les appareils équipés de Kaspersky Security 10 for Mobile seront placés ajoutés à ces groupes manuellement ou selon des règles du transfert automatique.

4. Création des règles de déplacement automatique des appareils mobiles dans le groupe.

5. Création de stratégies pour la gestion des paramètres de Kaspersky Security 10 for mobile.

6. Création du paquet d'installation pour l'installation à distance de Kaspersky Security 10 for mobile.

7. Configuration des paramètres du paquet d'installation pour l'installation à distance de Kaspersky Security 10 for mobile.

8. La création de l'installation à distance permet de répartir la distribution de l'application Kaspersky Endpoint Security 8.0 for Smartphone sur les postes de travail des utilisateurs et d'installer l'utilitaire de livraison de la distribution sur les appareils mobiles.

9. Téléchargement de la distribution de l'application sur l'appareil mobile. Cette étape permet, à l'aide de l'utilitaire kmlisten.exe, à l'utilisateur de copier la distribution de l'application sur l'appareil mobile.

10. Installation de l'application sur l'appareil mobile. Cette étape permet à l'utilisateur de lancer l'installation de l'application sur l'appareil mobile.

11. Activation de l'application (cf.la page 49) sur les appareils mobiles des utilisateurs.

PREPARATION DE L'INSTALLATION DE L'APPLICATION

Avant de procéder au déploiement de l'application Kaspersky Security, vous devez configurer la gestion des appareils mobiles à l'aide de Kaspersky Security Center. Pour ce faire, procédez comme suit :

1. Installez ou vérifiez l'installation dans le réseau d'entreprise des composants de Kaspersky Security Center : le Serveur d'administration et la Console de gestion (cf. *Guide du déploiement de Kaspersky Security Center*).

2. Assurez-vous que les composants installés sont conformes aux configurations logicielles (cf. section "Configurations logicielles et matérielles " à la page 14) de l'installation de l'application Kaspersky Security 10 for Mobile.

   Lors de l'installation du Serveur d'administration (cf. section " Installation du Serveur d'administration " à la page 22), vous devez installer le composant Prise en charge des appareils mobiles qui assure la gestion de la protection des appareils mobiles à l'aide de Kaspersky Security Center. Si ce composant n'a pas été installé ou la version du Serveur d'administration n'est pas conforme aux configurations logicielles de l'installation de Kaspersky Security 10 for Mobile l'administrateur doit supprimer la version ancienne du composant et installer la version spécifiée dans la configuration logicielle après avoir effectué une copie de sauvegarde de données du Serveur d'administration.

3. Configurer la prise en charge des appareils mobiles dans les paramètres du Serveur d'administration (cf. section " Configuration de paramètres du Serveur d'administration" à la page 23).

4. Installer sur le poste de travail de l'administrateur le module externe d'administration (cf. section " Installation du module externe d'administration de Kaspersky Security pour les appareils mobiles " à la page 23) de l'application Kaspersky Security 10 for Mobile.

5. Si nécessaire, déployer le Serveur des appareils mobiles iOS MDM (cf. section " Déploiement du Serveur des appareils mobiles iOS MDM et la connexion au Serveur des appareils d'utilisateurs " à la page 24).

6. Créer un groupe d'administration distinct (cf. section " Création du groupe " à la page 26) pour les appareils mobiles.

7. Configurer les paramètres du transfert automatique (cf. section " Création de la règle de transfert automatique des appareils dans le groupe d'administration " à la page 27) vers ce groupe pour tous les appareils sur lesquels sera installée l'application.

8. Créer une stratégie de groupe (cf. section " Création d'une stratégie de groupe pour Kaspersky Security 10 for Mobile " à la page 28) pour Kaspersky Security applicable à tous les appareils mobiles placés dans le groupe d'administration approprié.

9. Si nécessaire, configurer les paramètres de diffusion des messages électroniques (cf. section " Configuration de la diffusion des messages électroniques " à la page 24) aux utilisateurs (cf. *Guide d'administrateur de Kaspersky Security Center*).

10. Si nécessaire, configurer les paramètres de diffusion des messages texte (cf. section "Configuration du mode de livraison des messages textes" à la page 25) aux utilisateurs (cf. *Guide d'administrateur de Kaspersky Security Center*).

DANS CETTE SECTION

INSTALLATION DU SERVEUR D'ADMINISTRATION

La procédure d'installation du Serveur d'administration est décrite dans le *Guide du déploiement de Kaspersky Security Center*. Pour assurer la gestion de la protection des appareils mobiles à l'aide de Kaspersky Security Center à l'étape **Sélection des composants**, vous devez cocher la case **Prise en charge des appareils mobiles**.

Lors de l'installation du composant Prise en charge des appareils mobiles, un *certificat du Serveur d'administration pour les appareils mobiles* est créé. Il sert à l'authentification des appareils mobiles lors de l'échange de données avec le Serveur d'administration. L'échange d'informations se fait à l'aide du protocole SSL (Secure Socket Layer). En l'absence d'un certificat pour les appareils mobiles sur le Serveur d'administration, toute connexion entre le Serveur d'administration et les appareils mobiles est impossible.

Le certificat pour les appareils mobiles est stocké dans le dossier d'installation de l'application Kaspersky Security Center dans le sous-dossier Cert. A la première synchronisation de l'appareil mobile avec le Serveur d'administration, une copie du certificat sera envoyée vers l'appareil pour être stockée dans un dossier local.

MISE A JOUR DU COMPOSANT SERVEUR D'ADMINISTRATION

Si lors de l'installation du Serveur d'administration la case **Prise en charge des appareils mobiles** n'a pas été cochée ou une ancienne version de Kaspersky Security Center qui ne prend pas en charge Kaspersky Security 10 for Mobile a été installée, vous devez mettre à jour la version installée du composant Serveur d'administration.

Pour mettre à jour la version installée du composant Serveur d'administration, procédez comme suit :

1. Faites une copie de sauvegarde des données du Serveur d'administration (cf. *Guide d'administrateur de Kaspersky Security Center*).

2. Installez la version du Serveur d'administration spécifiée dans les configurations logicielles de l'installation de Kaspersky Security 10 for Mobile (cf. section " Configurations logicielles et matérielles " à la page 14).

3. A l'étape **Sélection des composants**, cochez la case **Prise en charge des appareils mobiles**.

Si le Serveur d'administration ne prend pas en charge les appareils mobiles, vous ne pouvez pas gérer la protection des appareils mobiles à l'aide de Kaspersky Security Center.

4. Restaurez les données du Serveur d'administration depuis la copie de sauvegarde (cf. *Guide d'administrateur de Kaspersky Security Center*).

CONFIGURATION DES PARAMETRES DU SERVEUR D'ADMINISTRATION

Pour assurer la synchronisation des appareils mobiles au Serveur d'administration avant l'installation de Kaspersky Security 10 for Mobile, vous devez configurer les paramètres de connexion des appareils mobiles dans les propriétés du Serveur d'administration.

- *Pour configurer les paramètres de connexion des appareils mobiles dans les propriétés du Serveur d'administration, procédez comme suit :*

1. Sélectionnez dans l'arbre de la console le Serveur d'administration pour connecter les appareils mobiles.
2. Ouvrez le menu contextuel et sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.
3. Ouvrez la section **Paramètres**.
4. Cochez la case **Ouvrir le port pour les appareils mobiles** dans le groupe **Paramètres de connexion au Serveur d'administration**.
5. Dans le champ **Port pour les appareils mobiles**, spécifiez le port que le Serveur d'administration va utiliser pour la connexion des appareils mobiles.

   Le numéro de port par défaut est 13292. Si la case est décochée ou le port n'a pas été spécifié correctement, les appareils ne pourront pas se connecter au serveur ni transmettre ou télécharger les informations.

INSTALLATION DU MODULE EXTERNE D'ADMINISTRATION DE KASPERSKY SECURITY FOR MOBILE

Pour obtenir l'accès à l'interface de gestion de l'application à l'aide de Kaspersky Security Center sur le poste de travail de l'administrateur, vous devez installer le module externe d'administration de l'application Kaspersky Security 10 for Mobile.

- *Pour installer le module externe d'administration de l'application Kaspersky Security 10 for Mobile,*

  copiez depuis la distribution de l'application le fichier d'installation du module externe klcfinst.exe et lancez-le depuis le poste de travail de l'administrateur.

  L'installation est assurée par l'assistant et ne nécessite aucune configuration de paramètres.

Pour vérifier l'installation du module externe pour l'application Kaspersky Security 10 for Mobile, il suffit de consulter la liste des modules externes d'administration des programmes installés qui est affichée dans le volet **Avancée** de la fenêtre des propriétés du Serveur d'administration. Pour plus d'information, adressez-vous au *Guide d'administrateur de Kaspersky Security Center*.

DEPLOIEMENT DU SERVEUR DES APPAREILS MOBILES IOS MDM ET CONNEXION AUX APPAREILS DES UTILISATEURS

Pour l'installation de Kaspersky Security sur les appareils mobiles des utilisateurs tournant sous iOS, il faut que le serveur des appareils mobiles iOS MDM soit déployé dans Kaspersky Security Center et les appareils mobiles des utilisateurs y soient connectés. Le serveur d'administration gère les appareils mobiles iOS MDM à l'aide du serveur des appareils mobiles iOS MDM. Les appareils mobiles iOS gérés par le serveur d'administration sont des *appareils mobiles iOS MDM*

Pour connecter les appareils mobiles iOS MDM, procédez comme suit :

1. Installez sur l'ordinateur avec le serveur d'administration les appareils mobiles iOS MDM inclus dans les paquets d'installation du serveur d'administration par défaut.

   A ce moment-là, l'installation locale est supportée, mais pas l'installation à distance.

2. Vous pouvez obtenir le certificat Apple Push Notification Service (cf. section " Demande électronique de signature d'un certificat APN " à la page 57) (certificat APN) à l'aide du service Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

   Pour plus d'information sur les certificats APN, adressez-vous au *Guide d'administrateur de Kaspersky Security Center*.

3. Installez le certificat APN sur le serveur d'administration.

   Il est impossible d'établir le profil MDM correct sans le certificat APN, et pour sa création, les données du certificat APN sont nécessaires. Uniquement après l'installation du certificat APN, vous pourrez vous assurer de la livraison adéquate des commandes sur l'appareil.

4. Envoyez à l'utilisateur de l'appareil mobile iOS le lien pour télécharger le profil iOS MDM.

   L'utilisateur établit le profil iOS MDM sur l'appareil mobile iOS.

   L'appareil mobile est connecté au serveur des appareils mobiles iOS MDM via le canal Internet accessible. Les appareils mobiles iOS MDM connectés apparaissent dans le dossier **Appareils mobiles iOS MDM** enregistrés sous le dossier **Appareils mobiles.**

CONFIGURATION DE LA DIFFUSION DES MESSAGES ELECTRONIQUES

Si vous pensez utiliser la diffusion des messages électroniques vers les adresses de messagerie d'entreprise lors du déploiement de l'application, à savoir :

- utiliser le schéma de déploiement à l'aide de la diffusion des messages électroniques (cf. section " Schéma de déploiement via la diffusion des messages électroniques " à la page 16) pour les appareils mobiles tournant sous Android ;

- envoyer le profil iOS MDM (cf. section " Création et installation du profil iOS MDM " à la page 46) aux adresses de messagerie d'entreprise d'utilisateurs lors de la connexion de leurs appareils au Serveur d'administration (cf. section " Schéma de déploiement de l'application pour les appareils tournant sous iOS " à la page 19);

vous devez vérifier que les paramètres de la diffusion des messages électroniques depuis le Serveur d'administration sont corrects.

Pour configurer l'envoi des notifications par courrier électronique, procédez comme suit :

1. Sélectionnez dans l'arbre de la console le Serveur d'administration auquel vous souhaitez connecter les appareils portables.

2. Ouvrez la fenêtre des propriétés du dossier **Rapports et notifications** d'une des manières suivantes :

   - Dans le menu contextuel du dossier de l'arbre de la console **Rapports et notifications**, sélectionnez l'option **Propriétés**.

   - Dans l'espace de travail du dossier **Rapports et notifications** sous l'onglet **Notifications**, ouvrez la fenêtre en cliquant sur le lien **Modifier les paramètres de livraison des notifications**.

3. Dans le volet **Notifications**, sélectionnez comme type de notification **Courrier électronique**.

4. Dans le champ **Serveur SMTP**, spécifiez l'adresse du serveur de messagerie.

   Vous pouvez utiliser comme adresse l'adresse IP ou le nom de l'ordinateur dans le réseau Windows (nom NetBIOS).

5. Dans le champ **Port du serveur SMTP**, spécifiez le numéro du port de communication du serveur SMTP.

   Le port 25 est le port choisi par défaut.

6. Cliquez sur **Appliquer** pour actualiser les paramètres.

CONFIGURATION DU MODE DE LIVRAISON DES MESSAGES TEXTES

Si vous pensez utiliser la diffusion des messages textes vers les numéros des téléphones d'utilisateurs lors du déploiement de l'application, à savoir :

- utiliser le schéma de déploiement à l'aide de la diffusion des messages texte (cf. section " Schéma de déploiement via l'envoi de notifications électroniques " à la page 16) pour les appareils mobiles tournant sous Android ;

- envoyer le profil iOS MDM (cf. section " Création et installation du profil iOS MDM " à la page 46) aux utilisateurs à l'aide des SMS vers les numéros de téléphone d'entreprise lors de la connexion de leurs appareils au Serveur d'administration (cf. section "Schéma de déploiement de l'application pour les appareils tournant sous iOS" à la page 19) ;

vous devez vérifier que les paramètres de la diffusion des messages texte depuis le Serveur d'administration sont corrects.

Vous avez deux options de diffusion en masse des messages texte aux utilisateurs à l'aide de Kaspersky Security Center :

- Via la passerelle de messagerie. Pour ce faire, il suffit de spécifier dans les paramètres de Kaspersky Security Center le serveur SMTP et le port.

  Pour plus d'information sur les options de diffusion des notifications aux utilisateurs qui existent dans Kaspersky Security Center, adressez-vous au *Guide d'administrateur de Kaspersky Security Center*.

- Via l'appareil mobile sélectionné tournant sous Android qui sera l'expéditeur des SMS avec des notifications sur les événements survenus lors du fonctionnement de Kaspersky Security Center.

Pour pouvoir utiliser l'appareil mobile comme expéditeur de tous les messages texte en provenance de Kaspersky Security Center, vous devez installer sur l'appareil l'utilitaire Kaspersky SMS Broadcasting. L'utilitaire Kaspersky SMS Broadcasting est installé sur l'appareil mobile en tant qu'application standard Android. Après son installation, l'utilitaire Kaspersky SMS Broadcasting demande l'adresse et le port du Serveur d'administration de Kaspersky Security Center. A l'issue de la synchronisation, l'appareil sera affiché dans le volet **Expéditeurs des SMS** de la fenêtre des propriétés du dossier **Rapports et notifications** en tant qu'un appareil destinataire potentiel dans la liste d'appareils destinataires potentiels. Il est conseillé d'utiliser l'appareil mobile avec l'utilitaire Kaspersky SMS Broadcasting en tant qu'expéditeur des SMS, notamment si vous souhaitez recevoir des rapports sur la livraison des messages texte.

Pour configurer l'option de diffusion des messages texte, procédez comme suit :

1. Sélectionnez dans l'arbre de la console le Serveur d'administration auquel les appareils portables seront branchés.

2. Ouvrez la fenêtre des propriétés du dossier **Rapports et notifications** d'une des manières suivantes :

   - Dans le menu contextuel du dossier de l'arbre de la console **Rapports et notifications**, sélectionnez l'option **Propriétés**.

   - Dans l'espace de travail du dossier **Rapports et notifications** sous l'onglet **Notifications**, ouvrez la fenêtre en cliquant sur le lien **Modifier les paramètres de livraison des notifications**.

3. Dans le volet **Notifications**, sélectionnez **SMS** comme type de notification.

4. Spécifiez l'option de diffusion des messages texte préférée :

   - sélectionnez **Envoyer les SMS via la passerelle de messagerie** et indiquez ses paramètres si vous souhaitez diffuser les messages via le centre SMS ;

   - sélectionnez **Envoyer les SMS à l'aide de l'utilitaire Kaspersky SMS Broadcasting** et sélectionnez l'appareil mobile expéditeur dans le volet **Expéditeurs des SMS** si vous souhaitez diffuser les messages texte aux utilisateurs depuis l'appareil mobile équipé de l'utilitaire Kaspersky SMS Broadcasting.

Pour plus d'information sur les options de diffusion des notifications aux utilisateurs qui existent dans Kaspersky Security Center, adressez-vous au *Guide d'administrateur de Kaspersky Security Center*.

CREATION DU GROUPE

La configuration centralisée des paramètres de l'application Kaspersky Security installée sur les appareils mobiles d'utilisateurs est effectuée via l'application des stratégies de groupe à ces appareils.

Pour pouvoir appliquer une stratégie au groupe d'appareils, il est conseillé de créer avant l'installation de Kaspersky Security sur les appareils d'utilisateurs un groupe dédié à ces appareils dans le dossier **Ordinateurs administrés**.

Ensuite, vous devez configurer le déplacement automatique vers ce groupe des appareils sur lesquels (cf. section " Création d'une règle de transfert automatique des appareils vers le groupe d'administration " à la page 27) vous souhaitez installer Kaspersky Security. Enfin, vous devez définir les paramètres communs pour tous les appareils à l'aide d'une stratégie de groupe (cf. section " Création d'une stratégie de groupe pour Kaspersky Security 10 for Mobile " à la page 28).

Pour créer un groupe, procédez comme suit :

1. Sélectionnez dans l'arbre de la console le Serveur d'administration auquel les appareils portables seront branchés.

2. Dans l'arbre de la console ouvrez le dossier **Ordinateurs administrés**.

3. Si vous souhaitez créer un sous-groupe dans un groupe existant, sélectionnez dans le dossier **Ordinateurs administrés** le sous-dossier dans lequel vous souhaitez créer un sous-groupe.

4. Vous avez deux options pour lancer la procédure de création du groupe :

   - à l'aide de la commande du menu contextuel **Créer → un Groupe** ;
   - sur le lien **Créer un sous-groupe** situé sur l'onglet dans la zone de travail de la fenêtre principale **Groupes**.

5. Dans la fenêtre **Nom de groupe** qui s'ouvre, saisissez le nom de groupe, puis cliquez sur le bouton **OK**.

   A l'issue de la procédure, un nouveau dossier du groupe d'administration au nom défini sera affiché dans l'arbre de la console.

Si lors de l'installation de Kaspersky Security vous utilisez la procédure d'installation de l'application sur les appareils mobiles via les stations de travail, vous pouvez créer sur le Serveur d'administration un groupe supplémentaire pour les stations de travail auxquelles les utilisateurs connectent leurs appareils mobiles. Ensuite, vous devez créer pour ce groupe une tâche de groupe pour installer l'application Kaspersky Security à distance. Cette opération vous permettra d'installer l'application simultanément via toutes les stations de travail faisant partie du groupe.

Pour plus d'information sur l'utilisation des groupes d'administration, adressez-vous au *Guide d'administrateur de Kaspersky Security Center*.

CREATION DE LA REGLE DU TRANSFERT AUTOMATIQUE DES APPAREILS VERS LE GROUPE D'ADMINISTRATION

La gestion centralisée des paramètres de l'application Kaspersky Security installée sur les appareils mobiles d'utilisateurs ne sera opérationnelle que si tous ces appareils appartiennent au groupe d'administration que vous avez créé au préalable (cf. section " Création du groupe " à la page 26) du nœud **Ordinateurs administrés** et qui a une stratégie distincte de groupe (cf. section " Création d'une stratégie de groupe pour Kaspersky Security 10 for Mobile " à la page 28).

Si la règle du déplacement automatique des appareils mobiles détectés dans le réseau n'a pas été définie, à la première synchronisation de l'appareil au Serveur d'administration cet appareil sera automatiquement transféré vers le sous-dossier **KSM10** du dossier **Domaines** qui se trouve dans le dossier **Ordinateurs non repartis**. La stratégie de groupe (cf. section " Création d'une stratégie de groupe pour Kaspersky Security 10 for Mobile " à la page 28) n'est pas applicable à cet appareil.

L'administrateur peut configurer le déplacement automatique des appareils mobiles depuis le dossier **Ordinateurs non repartis** vers le groupe sélectionné du dossier **Ordinateurs administrés**.

Pour créer une règle du transfert automatique des appareils mobiles vers le groupe, procédez comme suit :

1. Sélectionnez dans l'arbre de la console le Serveur d'administration auquel les appareils portables seront branchés.

2. Dans l'arbre de la console ouvrez le dossier **Ordinateurs non repartis**.

3. Ouvrez la fenêtre des propriétés du dossier **Ordinateurs non repartis** d'une des manières suivantes :

   - à l'aide de l'option du menu contextuel **Propriétés** de ce dossier.
   - en cliquant sur le lien **Configurer les règles de déplacement des ordinateurs vers les groupes d'administration** dans l'espace de travail du dossier.

   La fenêtre **Propriétés : Ordinateurs non repartis** s'ouvre.

4. Dans le volet **Déplacement d'ordinateurs**, cliquez sur le bouton **Ajouter** pour lancer la procédure de création d'une règle de déplacement automatique des appareils vers le groupe d'administration.

   La fenêtre **Nouvelle règle** s'ouvre.

5. Dans le volet **Général**, effectuez les actions suivantes :

   - Spécifiez le nom de la règle.
   - Indiquez le groupe où seront déplacés les appareils mobiles équipés de l'application Kaspersky Security. Pour ce faire, cliquez sur le bouton **Sélectionner** qui se trouve à droite du champ **Groupe destiné au déplacement d'ordinateurs** et sélectionnez le groupe dans la fenêtre qui s'ouvre.
   - Dans le groupe **Exécution de la règle**, sélectionnez l'option **Appliquer une seule fois pour chacun des ordinateurs**.
   - Cochez la case **Déplacer uniquement les ordinateurs qui n'appartiennent pas aux groupes d'administration** pour que les ordinateurs déjà repartis dans d'autres groupes d'administration ne soient pas déplacés vers le groupe sélectionné selon cette règle.
   - Cochez la case **Activer la règle** pour appliquer cette règle aux appareils nouvellement détectés.

6. Dans la section **Programmes**, sélectionnez un ou plusieurs types de systèmes d'exploitation qui seront déplacés vers le groupe indiqué, tels qu'Android, BlackBerry, iOS, Symbian ou Windows Mobile.

7. Cliquez sur le bouton **OK**.

   La règle est créée, activée et affichée dans la liste des règles de déplacement des appareils (cf. volet **Déplacement d'ordinateurs** dans la fenêtre des propriétés du dossier **Ordinateurs non repartis**).

Cette règle assure le déplacement des appareils conformes aux critères définis depuis le dossier **Ordinateurs non repartis** vers le dossier que vous avez indiqué. Les appareils mobiles déjà déplacés vers le dossier **Ordinateurs non repartis** peuvent être déplacés vers un dossier requis du nœud **Ordinateurs administrés** manuellement. Pour plus d'information sur la gestion des groupes d'administration et l'utilisation des appareils non repartis, adressez-vous au *Guide d'administrateur de Kaspersky Security Center*.

CREATION D'UNE STRATEGIE DE GROUPE POUR KASPERSKY SECURITY 10 FOR MOBILE.

Cette section décrit la procédure de création d'une stratégie pour les appareils équipés de Kaspersky Security 10 for Mobile.

Tous les paramètres de fonctionnement de Kaspersky Security sur les appareils y compris les données nécessaires à l'activation de l'application, la planification de la mise à jour des bases de l'application, la planification de l'analyse de l'appareil et les paramètres de filtrage sont définis via la stratégie de groupe applicable ou via les paramètres locaux de l'application installée sur l'appareil. Les stratégies permettent de définir de façon centralisée les mêmes valeurs des paramètres de fonctionnement de l'application pour tous les appareils mobiles faisant partie du groupe d'administration. Pour plus d'information sur les stratégies et les groupes, adressez-vous au *Guide d'administrateur de Kaspersky Security Center*.

Le "cadenas"  détermine l'interdiction de modifier les valeurs des paramètres locaux de l'application via la Console d'administration et via l'interface de l'application sur l'appareil mobile. Si le "cadenas" ressemble à , il est possible de modifier les valeurs dans les paramètres locaux de l'application.

Les informations sur les paramètres de l'application définis dans les stratégies sont stockées sur le Serveur d'administration et transférées vers les appareils mobiles pendant la synchronisation. L'utilisateur peut apporter des modifications dans les paramètres définis par la stratégie sur l'appareil mobile si cette fonction est autorisée par la stratégie. Après la suppression de la stratégie ou son expiration, l'application continue à utiliser les paramètres définis par la stratégie. Par la suite, l'utilisateur peut modifier ces paramètres manuellement.

Les stratégies créées pour les appareils dans le groupe d'administration sont affichées dans l'espace de travail du groupe sous l'onglet **Stratégies**. A côté du nom de chacune des stratégies est affichée l'icône qui reflète son état. Vous pouvez créer plusieurs stratégies pour l'application Kaspersky Security 10 for Mobile pour d'autres programmes dans un même groupe, mais une seule stratégie peut être active. Si vous créez une nouvelle stratégie active, la stratégie active précédente devient inactive.

Lors de la création de la stratégie, vous pouvez configurer un jeu minimal de paramètres indispensables au fonctionnement de l'application. Toutes les autres valeurs des paramètres sont définies par défaut et correspondent aux valeurs par défaut lors de l'installation locale de l'application. Vous pouvez modifier la stratégie après sa création.

Pour créer une stratégie pour l'application Kaspersky Security 10 for Mobile, procédez comme suit :

1. Sélectionnez dans l'arbre de la console le groupe d'administration pour lequel vous souhaitez créer une stratégie.

2. Dans la zone de travail du groupe choisissez l'onglet **Politiques** et lancez l'assistant de la création de la politique sur le lien **Créer la politique**.

   Au final, l'assistant de la création de la politique va se lancer. Il faut suivre ses indications.

Définissez les valeurs des paramètres aux étapes suivantes :

- A l'étape **Sélection de l'application pour créer une stratégie du groupe**, sélectionnez Kaspersky Security 10 for Mobile comme application objet de la stratégie créée.

  Si l'application Kaspersky Security 10 for Mobile n'est pas sur la liste, cela veut dire que le module externe d'administration de cette application n'a pas été installé.

- A l'étape **Analyse de l'appareil**, spécifiez les paramètres suivants de l'analyse à la demande applicables aux appareils tournant sous les systèmes d'exploitation Android, Symbian et Windows Mobile :

  - activez / désactivez l'analyse uniquement des fichiers exécutables aux formats suivants : EXE, DLL, MDL, APP, APK, RDL, PRT, PXT, LDD, PDD, CLASS, SO, ELF.

  - activez / désactivez l'analyse des fichiers dans les archives ;

  - activez / désactivez la réparation automatique des objets malveillants détectés ;

  - créez une planification pour lancer l'analyse complète du système de fichiers de l'appareil.

- A l'étape **Protection**, définissez les paramètres de protection applicables pour les appareils tournant sous les systèmes d'exploitation Android, Symbian et Windows Mobile :

  - activez / désactivez la protection :

    - Pour les appareils tournant sous Windows Mobile et Symbian : La protection qui est une analyse automatique de toutes les applications en exécution et des fichiers que l'utilisateur ouvre et enregistre sur l'appareil ;

    - Pour les appareils tournant sous Android : l'analyse automatique des nouvelles applications tout de suite après leur installation. l'analyse automatique des nouvelles applications tout de suite après leur installation.

  - activez/désactivez le mode de protection élargi – l'analyse des applications tout de suite après leur installation, ainsi que tous les fichiers lors de toute action de l'utilisateur sur ceux-ci (uniquement pour les périphériques Android) ;

  - activez / désactivez l'analyse complémentaire de nouvelles applications avant leur première exécution à l'aide du service nuage Kaspersky Security Network (uniquement pour les appareils tournant sous Android) ;

  - activez / désactivez la détection des logiciels publicitaires et des programmes légaux que les individus malintentionnés peuvent utiliser pour nuire à l'appareil et aux données de l'utilisateur (uniquement pour les appareils tournant sous Android) ;

- activez / désactivez l'analyse uniquement des fichiers exécutables aux formats suivants : EXE, DLL, MDL, APP, APK, RDL, PRT, PXT, LDD, PDD, CLASS, SO, ELF.

- sélectionnez l'action qui sera exécutée à la détection d'un objet malveillant lorsque sa réparation est impossible.

- A l'étape **Mise à jour**, définissez les paramètres suivants de la mise à jour des bases de l'application applicables aux appareils tournant sous les systèmes d'exploitation Android, Symbian et Windows Mobile :

  - spécifiez si la mise à jour planifiée sera exécutée lorsque l'appareil est en itinérance ;

  - sélectionnez le serveur depuis lequel l'application va télécharger les mises à jour sur les appareils mobiles d'utilisateurs ;

  - créez une planification pour télécharger les mises à jour.

- A l'étape **Antivol** spécifier les paramètres de la protection des données sur l'appareil mobile en cas de perte ou de vol, applicables aux appareils tournant sous les systèmes d'exploitation Android, BlackBerry, Symbian et Windows Mobile:

  - **Activer la suppression des données** : activez / désactivez la fonction de suppression à distance des données personnelles, des données d'entreprise ou toutes les données de l'appareil. Les données sont supprimées à la réception de l'instruction de l'administrateur. Aucune restauration n'est possible.

  - **Activer le blocage** : activez / désactivez la fonction de blocage à distance de l'appareil mobile de l'utilisateur à la réception de l'instruction de l'administrateur.

  - **Activer la surveillance SIM** : activez / désactivez la fonction de blocage à distance de l'appareil mobile en cas de remplacement de la carte SIM ou de mise sous tension sans cette carte à la réception de l'instruction de l'administrateur.

  - **Activer la géolocalisation** : activez / désactivez la fonction de l'obtention à distance des coordonnées géographiques de l'appareil et de leur réception par SMS ou à l'adresse de messagerie indiquée à la réception de l'instruction de l'administrateur.

- A l'étape **Réseau**, définissez les paramètres de synchronisation des appareils mobiles au Serveur d'administration et les paramètres de filtrage des connexions entrantes et sortantes.

  - spécifiez la périodicité de la synchronisation : la fréquence de connexion des appareils mobiles au Serveur d'administration via le protocole HTTP ;

  - autorisez / interdisez la synchronisation automatique si l'appareil est en itinérance (inaccessible pour les périphériques) ;

    Pour les appareils tournant sous Windows Mobile et Symbian :

    - sélectionnez le mode de fonctionnement du Pare-feu que l'application va utiliser pour autoriser ou interdire les connexions entrantes et sortantes et spécifiez les paramètres de notification de l'utilisateur sur le blocage de la connexion.

    Pour les appareils tournant sous Android et iOS :

    - activez / désactivez le Pare-feu : la fonction du blocage d'accès utilisateur aux sites Web des catégories indésirables et sélectionnez ces catégories.

- A l'étape **Contrôle des Applications**, spécifiez pour les appareils tournant sous Android les paramètres de lancement d'applications installées sur l'appareil et créez une liste d'applications autorisées, interdites et obligatoires :

  - activez le mode de restriction d'accès des applications sur l'appareil de l'utilisateur. Pour ce faire, sélectionnez **Application interdite** pour permettre aux utilisateurs de lancer toutes les applications sauf celles classées **Interdites** dans la Liste d'applications ou sélectionnez **Applications autorisées** pour

permettre aux utilisateurs de lancer uniquement les applications classées **Autorisées** dans la liste d'applications.

- activez/désactivez la formation du rapport sur le lancement des applications interdites sur le périphérique mobile de l'utilisateur.

- créez une liste qui contient les applications dont l'exécution sur l'appareil mobile est autorisée ou interdite ainsi que les applications obligatoires (c'est-à-dire les applications recommandées à l'utilisateur pour une installation autonome sur l'appareil mobile). Pour ce faire, spécifiez les packages des applications mobiles créés au préalable (y compris les conteneurs) qui sont stockés sur le Serveur Web de Kaspersky Security Center ou le chemin d'accès aux fichiers avec l'extension apk sur un autre serveur HTTP.

- sélectionnez l'action que l'application exécutera en cas de détection de l'accès avec les privilèges d'administrateur au système du périphérique de l'utilisateur.

- activez/désactivez la formation du rapport sur les applications installées sur le périphérique mobile de l'utilisateur.

- A l'étape **Gestion de l'appareil**, spécifiez les paramètres et les restrictions applicables uniquement aux appareils tournant sous Android :

  - activez / désactivez l'obligation d'utiliser un mot de passe et spécifiez sa longueur minimale ;

  - autorisez / interdisez l'utilisation du Wi-Fi, de la caméra et du Bluetooth ;

  - configurez les paramètres du client de messagerie TouchDown pour permettre aux utilisateurs d'accéder à la messagerie d'entreprise depuis leurs appareils.

- A l'étape **Paramètres avancés**, spécifiez les paramètres des composants Chiffrement et Filtre des appels et SMS, ainsi que les paramètres de suppression de l'application.

  Pour les appareils tournant sous Android, BlackBerry, Symbian et Windows Mobile :

  - activez / désactivez l'utilisation du composant Filtre des appels et SMS qui bloque la réception des appels et des messages texte indésirables en fonction de la liste de contacts autorisés ou interdits créée par l'utilisateur.

  Pour les appareils tournant sous Symbian et Windows Mobile :

  - activez / désactivez la fonction qui permet aux utilisateurs d'utiliser et de configurer le composant Contacts personnels qui masque les informations confidentielles pour les contacts sélectionnés.

  - spécifiez l'intervalle de temps après le passage de l'appareil en mode économie d'énergie à l'issue duquel l'accès aux dossiers chiffrés sera interdit. Pour restaurer l'accès, l'utilisateur devra saisir le code secret de l'application spécifié lors du premier lancement.

  - créez des listes de dossiers pour le chiffrement.

  Pour les appareils tournant sous Android :

  - activez / désactivez la fonction qui permet aux utilisateurs de supprimer l'application Kaspersky Security 10 for Mobile de leurs appareils ;

  - cochez la case à côté de **Supprimer Kaspersky Security 10 for Mobile de l'appareil** pour supprimer l'installation sans l'intervention des utilisateurs de tous les appareils du groupe couvert par la stratégie que vous êtes en train de créer.

- A l'étape **Gestion des licences**, indiquez les paramètres d'activation de l'application (cf.la page 49) sur les appareils d'utilisateurs. Vous pouvez sélectionnez la clé de la liste des clés placées dans le stockage de Kaspersky Security Center. A l'aide de cette clé, les informations sur la licence de l'application seront transmises sur les périphériques des utilisateurs.

  Pour activer l'application sur les appareils mobiles, vous devez interdire toute modification des paramètres relatifs à l'activation.

- A l'étape finale, sélectionnez l'état **Stratégie active** si vous souhaitez appliquer cette stratégie au groupe.

  Par la suite, vous pouvez modifier l'état de la stratégie dans les propriétés.

LA MISE A JOUR DE LA VERSION PRECEDENTE DU LOGICIEL

Lors de la mise à jour de la version précédente du logiciel, il est indispensable de prendre en compte que Kaspersky Security est livré en commun avec le plugin de gestion du logiciel Kaspersky Security via Kaspersky Security Center.

Avant l'installation du plugin de gestion Kaspersky Security 10 il est nécessaire de supprimer la version précédente du présent plugin. Dans ce cas, les groupes déjà existants sont sauvegardés dans le dossier **Ordinateurs gérés**, créés pour la gestion centralisée des paramètres Kaspersky Security, ainsi que les règles du déplacement des appareils depuis le dossier **Ordinateurs non repartis** dans ces groupes. Les politiques de groupes, créées pour la version précédente du logiciel, sont aussi sauvegardées. Les nouveaux paramètres des politiques réalisant une nouvelle fonctionnalité de Kaspersky Security 10 vont apparaitre dans les politiques déjà existantes, ils vont avoir la valeur par défaut.

Vous pouvez installer Kaspersky Security 10 sur l'appareil mobile sous Kaspersky Endpoint Security 8 for Smartphone installé auparavant. L'utilisateur sera invité de supprimer la version précédente lors du premier lancement du logiciel Kaspersky Security 10. Il est recommandé de supprimer la version précédente du logiciel.

Il est à noter, pour les plates-formes BlackBerry, Symbian et Windows Mobile la distribution du logiciel Kaspersky Security 10 contient les fichiers de la précédente version ; la nouvelle fonctionnalité pour ces plates-formes n'est pas soutenue.

L'INSTALLATION SUR LES APPAREILS TOURNANT SOUS ANDROID

Dans cette section vous verrez les possibilités d'installation de Kaspersky Security 10 for Mobile sur les appareils tournant sous Android.

DANS CETTE SECTION

L'INSTALLATION DU LOGICIEL VIA L'ENVOI DES MESSAGES ELECTRONIQUES

Afin d'installer Kaspersky Security via l'envoi des messages aux courriers électroniques, il faut créer un package d'installation pour ce programme et y configurer la connexion au Serveur d'administration. Ensuite, à partir du package d'installation, vous devez créer un package d'installation autonome et le faire distribuer parmi les utilisateurs des appareils mobiles à l'aide de l'envoi des e-mails contenant soit le package lui-même, soit un lien sur le serveur Web Kaspersky Security Center, et aussi un dossier d'administrateur partagé, ou une autre ressource où vous voulez mettre le package autonome de l'installation.

L'utilisateur doit télécharger lui-même la distribution du logiciel sur son appareil portable. Après le téléchargement, l'assistant de l'installation va se mettre en route. Suivant les indications de l'assistant, l'utilisateur effectue l'installation de Kaspersky Security 10 for Mobile sur son appareil.

DANS CETTE SECTION

LA CREATION DU PACKAGE D'INSTALLATION

Le package d'installation Kaspersky Security 10 for Mobile est un archive auto-décompactable sc_package.exe qui contient les fichiers pour l'installation du logiciel sur les appareils mobiles :

- `endpoint_8_0_0_37_fr.cab` – fichier d'installation pour le système d'exploitation Windows Mobile ;
- `endpoint8_mobile_8_1_44_fr.sisx` – fichier d'installation pour le système d'exploitation Symbian ;
- `endpoint8_Mobile_8_1_29_fr.zip` – fichier d'installation pour le système d'exploitation BlackBerry ;
- `KSM_10_1_75_fr.apk` – fichier d'installation pour le système d'exploitation Android ;
- `installer.ini` – fichier de configuration contenant les paramètres de connexion au Serveur d'administration ;
- `kmlisten.ini` – fichier de configuration contenant les paramètres pour l'utilitaire de la livraison du package d'installation ;
- `kmlisten.kpd` – fichier contenant la description du logiciel ;
- AdbWinUsbApi.dll, AdbWinApi.dll, adb.exe – kit des fichiers de l'installation du logiciel sur les appareils sous le système d'exploitation Android ;
- `kmlisten.exe` – utilitaire de la livraison de la distribution du logiciel sur l'appareil mobile via le poste terminale.

Pour créer le package d'installation Kaspersky Security 10 for Mobile, procédez comme suit :

1. Sélectionnez dans l'arbre de la console le Serveur d'administration auquel les appareils portables seront branchés.

2. Dans l'arbre du console, au dossier **Installation à distance** sélectionnez le sous-dossier **Packages d'installation**.

3. Lancez la création du package d'installation par l'un des procédés suivants :

   - dans le menu contextuel du dossier **Packages d'installation** sélectionnez **Créer → un package d'installation** ;

   - dans le menu contextuel de la liste des packages d'installation sélectionnez **Créer → un package d'installation** ;

   - sur le lien **Créer un package d'installation** dans le bloc de gestion de la liste des package d'installation.

   Au final, l'assistant de la création du package d'installation va se lancer. Il faut suivre ses indications.

   Faites attention à la configuration suivantes :

   - Dans la fenêtre de l'assistant **Sélectionnez le type du package d'installation** appuyez sur le bouton **Créer le package d'installation "Kaspersky Lab"**.

   - Dans la fenêtre de l'assistant **Sélection de la distribution du logiciel à installer** à l'aide du bouton **Sélectionner** ouvrez le fichier où vous avez placé la distribution du logiciel et sélectionnez l'archive auto-décompactable sc_package.exe. Si l'archive a été décompactée avant, vous pouvez sélectionner un fichier faisant partie de l'archive avec la description du programme kmlisten.kpd. Finalement le nom du logiciel ainsi que le numéro de la version vont apparaitre dans le champ de saisie.

   Après la fin du travail de l'assistant, le package d'installation ainsi créé va s'afficher dans la zone de travail du dossier **Packages d'installation**. Les packages d'installation sont stockés dans un dossier défini partagé dans le dossier de service Packages du Serveur d'administration.

Avant d'utiliser le package d'installation ainsi créé, il faut configurer les paramètres du package d'installation (cf. section "Configuration des paramètres du package d'installation" à la page 34).

LA CONFIGURATION DU PACKAGE D'INSTALLATION

La configuration du package d'installation du logiciel Kaspersky Security 10 for Mobile est nécessaire pour que l'appareil mobile puisse utiliser les paramètres correctes de la connexion au Serveur d'administration.

Pour configurer les paramètres du package d'installation, procédez comme suit :

1. Sélectionnez dans l'arbre de la console le Serveur d'administration auquel vous souhaitez connecter les appareils portables.

2. Dans l'arbre du console, au dossier **Installation à distance** sélectionnez le sous-dossier **Packages d'installation**.

3. Dans le menu contextuel du package d'installation du logiciel Kaspersky Security, sélectionnez **Propriétés**.

4. Sur l'onglette **Paramètres** indiquez les paramètres de connexion des appareils portables au Serveur d'administration et le nom du groupe où les appareils portables seront ajoutés après la première synchronisation avec le Serveur d'administration. Pour ce faire, procédez comme suit :

- Dans le bloc **Connexion avec le Serveur d'administration** dans le champ **Adresse de serveur** saisissez le nom du Serveur d'administration pour connecter les appareils mobiles dans le même format qui a été spécifié lors de l'installation du composant **Support des appareils mobiles** pendant le déploiement du Serveur d'administration.

  C'est à dire, selon le format du nom de Serveur d'administration pour le composant **Support des appareils mobiles** indiquez le nom DNS ou IP-adresse du Serveur d'administration. Dans le champ **Numéro du port SSL** indiquez le numéro du port qui est ouvert sur le Serveur d'administration pour connecter les appareils mobiles. Le numéro de port par défaut est 13292.

- Dans le bloc **Répartition des ordinateurs selon les groupes** dans le champ **Nom du groupe** saisissez le nom du groupe où les appareils portables seront ajoutés après la première synchronisation avec le Serveur d'administration (par défaut KSM10).

  Le groupe sélectionné sera automatiquement crée dans le dossier **Ordinateurs non-repartis**.

- Dans le bloc **Actions à l'entreprendre lors de l'installation** cochez la case **Demander l'adresse du courrier électronique** pour que lors du premier lancement le logiciel demande à l'utilisateur son adresse e-mail de fonction.

  L'adresse e-mail de l'utilisateur est utilisée pour créer le nom des appareils mobiles lorsqu'ils sont ajoutés à un groupe d'administration. Le nom de l'appareil mobile sous Android est formé selon la règle <adresse e-mail de l'utilisateur (modèle de l'appareil mobile – device ID)>.

5. Pour appliquer les paramètres sélectionnez appuyez sur **Appliquer**.

LA CREATION DU PACKAGE AUTONOME D'INSTALLATION

Pour créer un package autonome d'installation, procédez comme suit :

1. Sélectionnez dans l'arbre de la console le Serveur d'administration auquel les appareils portables seront branchés.

2. Dans l'arbre du console, dans le champ **Installation à distance** spécifiez le sous-dossier **Packages d'installation**.

3. Spécifiez le package d'installation pour le logiciel Kaspersky Security 10 pour les appareils mobiles.

4. Lancez le procédé de la création du package autonome par l'un des moyens ci-dessous :

   - dans le menu contextuel du dossier **Packages d'installation** choisissez **Créer un package autonome** ;

   - dans le menu contextuel de la liste des packages d'installation choisissez **Créer un package autonome** ;

   - sur le lien **Créer un package autonome** dans le bloc de gestion des packages d'installation.

Comme résultat, l'assistant de la création du package autonome d'installation va se lancer. Il faut suivre ses indications.

Notez bien que lorsque vous créez un package autonome, il ne faut pas spécifier qu'un package est créé pour installer l'Agent d'administration.

Après la fin du travail de l'assistant, si la case **Ouvrir la liste des packages autonomes** est cochée pendant la dernière étape, la fenêtre avec la liste de tous les packages disponibles va s'ouvrir. Lors de la sélection d'un package, le logiciel affiche l'emplacement du fichier sur le serveur Web Kaspersky Security Center (champ **URL**) et dans le dossier partagé de l'administrateur (champ **Destination**).

Sur cette étape, le fichier d'installation du logiciel Kaspersky Security 10 pour les appareils mobiles est prêt pour l'envoi aux utilisateurs. Lors de l'envoi par e-mail, vous pouvez indiquer comme source du téléchargement du fichier d'installation sois l'adresse du champ **URL** (adresse du package autonome sur le site Web Kaspersky Security Center), sois l'adresse indiquée comme **Destination** (accès de réseau vers le dossier partagé).

Il est recommandé de copier l'adresse d'un package autonome dans le presse-papiers pour ajouter ensuite le lien sur le téléchargement d'un fichier d'installation souhaité dans le message électronique destiné aux utilisateurs.

L'ENVOI DES MESSAGES ELECTRONIQUES AUX UTILISATEURS

Pour envoyer aux utilisateurs un courrier électronique contenant le lien sur le package autonome d'installation du logiciel Kaspersky Security 10 pour les appareils mobiles, procédez comme suit :

1. Sélectionnez dans l'arbre de la console le Serveur d'administration auquel les appareils portables seront branchés.
2. Dans l'arbre de la console sélectionnez le dossier **Comptes utilisateurs**.
3. Sélectionnez un ou plusieurs utilisateurs.
4. Dans le menu contextuel, sélectionnez l'option **Envoyer par courrier électronique**.

   La fenêtre e-mail va s'ouvrir.
5. Indiquez les paramètres suivants :
   - Saisissez le sujet du message.
   - Saisissez le texte du message en mettant le lien sur l'emplacement du package autonome d'installation du site Web Kaspersky Security Center ou son trajet dans votre dossier partagé.
   - Cochez les cases **Utiliser l'adresse e-mail principale** et **Utiliser l'adresse e-mail supplémentaire** lorsqu'il faut utiliser les adresses principale et supplémentaire respectivement.
   - Lorsqu'il faut créer les codes QR pour les liens, cochez la case **Créer les codes QR graphiques pour les URL et les envoyer dans un message mail**.
6. Appuyez **OK** pour l'envoi.

L'INSTALLATION DU LOGICIEL SUR L'APPAREIL MOBILE APRES LA RECEPTION DU MESSAGE PAR E-MAIL

Après avoir reçu un message mail contenant le lien sur le package autonome, l'utilisateur peut télécharger le fichier de distribution sur son appareil portable par des moyens accessibles. Le package autonome contient le fichier d'installation pour le système d'exploitation Android avec la configuration présélectionnée de connexion au Serveur d'administration.

Le téléchargement terminé, l'utilisateur ouvre le fichier d'installation sur son appareil, l'assistant de l'installation du logiciel se lance automatiquement. L'utilisateur doit suivre les indications de l'assistant de l'installation.

Si tous les paramètres de la connexion au Serveur d'administration ont été indiqués lors de la création du package d'installation, alors la configuration initiale du logiciel (cf.la section "La préparation du logiciel au fonctionnement" à la page 48) n'est pas nécessaire.

Par défaut, le système d'exploitation Android interdit toute installation d'application hors Google Play. Si le système ne procède pas à l'installation, l'utilisateur doit autoriser l'installation des applications depuis une source externe dans les paramètres de son appareil tournant sous Android.

L'INSTALLATION DU LOGICIEL VIA L'ENVOI DES MESSAGES TEXTE

Afin d'installer Kaspersky Security via la diffusion des messages texte (SMS), il faut créer un package d'installation pour ce programme et y configurer la connexion au Serveur d'administration. Ensuite, vous devez créer à partir du package d'installation un package d'installation autonome et le faire distribuer parmi les utilisateurs des appareils mobiles via la diffusion des messages texte avec un lien sur le serveur Web Kaspersky Security Center ou sur une autre ressource où vous souhaitez mettre le package autonome de l'installation.

L'utilisateur télécharge la distribution de l'application sur l'appareil mobile à partir de la ressource réseau spécifiée dans la diffusion. Après le téléchargement, l'assistant de l'installation va se mettre en route. Suivant les indications de l'assistant, l'utilisateur effectue l'installation de Kaspersky Security 10 for Mobile sur son appareil.

DANS CETTE SECTION

LA CREATION DU PACKAGE D'INSTALLATION

Le package d'installation Kaspersky Security 10 for Mobile est un archive auto-décompactable sc_package.exe qui contient les fichiers pour l'installation du logiciel sur les appareils mobiles :

- `endpoint_8_0_0_37_fr.cab` – fichier d'installation pour le système d'exploitation Windows Mobile ;
- `endpoint8_mobile_8_1_44_fr.sisx` – fichier d'installation pour le système d'exploitation Symbian ;
- `endpoint8_Mobile_8_1_29_fr.zip` – fichier d'installation pour le système d'exploitation BlackBerry ;
- `KSM_10_1_75_fr.apk` – fichier d'installation pour le système d'exploitation Android ;
- `installer.ini` – fichier de configuration contenant les paramètres de connexion au Serveur d'administration ;
- `kmlisten.ini` – fichier de configuration contenant les paramètres pour l'utilitaire de la livraison du package d'installation ;
- `kmlisten.kpd` – fichier contenant la description du logiciel ;
- `AdbWinUsbApi.dll, AdbWinApi.dll, adb.exe` – kit des fichiers de l'installation du logiciel sur les appareils sous le système d'exploitation Android ;
- `kmlisten.exe` – utilitaire de la livraison de la distribution du logiciel sur l'appareil mobile via le poste terminale.

Pour créer le package d'installation Kaspersky Security 10 for Mobile, procédez comme suit :

1. Sélectionnez dans l'arbre de la console le Serveur d'administration auquel les appareils portables seront branchés.

2. Dans l'arbre du console, au dossier **Installation à distance** sélectionnez le sous-dossier **Packages d'installation**.

3. Lancez la création du package d'installation par l'un des procédés suivants :

   - dans le menu contextuel du dossier **Packages d'installation** sélectionnez **Créer → un package d'installation** ;

   - dans le menu contextuel de la liste des packages d'installation sélectionnez **Créer → un package d'installation** ;

   - sur le lien **Créer un package d'installation** dans le bloc de gestion de la liste des package d'installation.

   Au final, l'assistant de la création du package d'installation va se lancer. Il faut suivre ses indications.

   Faites attention à la configuration suivantes :

   - Dans la fenêtre de l'assistant **Sélectionnez le type du package d'installation** appuyez sur le bouton **Créer le package d'installation "Kaspersky Lab"**.

   - Dans la fenêtre de l'assistant **Sélection de la distribution du logiciel à installer** à l'aide du bouton **Sélectionner** ouvrez le fichier où vous avez placé la distribution du logiciel et sélectionnez l'archive auto-décompactable sc_package.exe. Si l'archive a été décompactée avant, vous pouvez sélectionner un fichier faisant partie de l'archive avec la description du programme kmlisten.kpd. Finalement le nom du logiciel ainsi que le numéro de la version vont apparaitre dans le champ de saisie.

   Après la fin du travail de l'assistant, le package d'installation ainsi créé va s'afficher dans la zone de travail du dossier **Packages d'installation**. Les packages d'installation sont stockés dans un dossier défini partagé dans le dossier de service Packages du Serveur d'administration.

Avant d'utiliser le package d'installation ainsi créé, il faut configurer les paramètres du package d'installation (cf. section "Configuration des paramètres du package d'installation" à la page 38).

LA CONFIGURATION DU PACKAGE D'INSTALLATION

La configuration du package d'installation du logiciel Kaspersky Security 10 for Mobile est nécessaire pour que l'appareil mobile puisse utiliser les paramètres correctes de la connexion au Serveur d'administration.

Pour configurer les paramètres du package d'installation, procédez comme suit :

1. Sélectionnez dans l'arbre de la console le Serveur d'administration auquel vous souhaitez connecter les appareils portables.

2. Dans l'arbre du console, au dossier **Installation à distance** sélectionnez le sous-dossier **Packages d'installation**.

3. Dans le menu contextuel du package d'installation du logiciel Kaspersky Security, sélectionnez **Propriétés**.

4. Sur l'onglette **Paramètres** indiquez les paramètres de connexion des appareils portables au Serveur d'administration et le nom du groupe où les appareils portables seront ajoutés après la première synchronisation avec le Serveur d'administration. Pour ce faire, procédez comme suit :

- Dans le bloc **Connexion avec le Serveur d'administration** dans le champ **Adresse de serveur** saisissez le nom du Serveur d'administration pour connecter les appareils mobiles dans le même format qui a été spécifié lors de l'installation du composant **Support des appareils mobiles** pendant le déploiement du Serveur d'administration.

  C'est à dire, selon le format du nom de Serveur d'administration pour le composant **Support des appareils mobiles** indiquez le nom DNS ou IP-adresse du Serveur d'administration. Dans le champ **Numéro du port SSL** indiquez le numéro du port qui est ouvert sur le Serveur d'administration pour connecter les appareils mobiles. Le numéro de port par défaut est 13292.

- Dans le bloc **Répartition des ordinateurs selon les groupes** dans le champ **Nom du groupe** saisissez le nom du groupe où les appareils portables seront ajoutés après la première synchronisation avec le Serveur d'administration (par défaut KSM10).

  Le groupe sélectionné sera automatiquement crée dans le dossier **Ordinateurs non-repartis**.

- Dans le bloc **Actions à l'entreprendre lors de l'installation** cochez la case **Demander l'adresse du courrier électronique** pour que lors du premier lancement le logiciel demande à l'utilisateur son adresse e-mail de fonction.

  L'adresse e-mail de l'utilisateur est utilisée pour créer le nom des appareils mobiles lorsqu'ils sont ajoutés à un groupe d'administration. Le nom de l'appareil mobile sous Android est formé selon la règle <adresse e-mail de l'utilisateur (modèle de l'appareil mobile – device ID)>.

5. Pour appliquer les paramètres sélectionnez appuyez sur **Appliquer**.

LA CREATION DU PACKAGE AUTONOME D'INSTALLATION

Pour créer un package autonome d'installation, procédez comme suit :

1. Sélectionnez dans l'arbre de la console le Serveur d'administration auquel les appareils portables seront branchés.

2. Dans l'arbre du console, dans le champ **Installation à distance** spécifiez le sous-dossier **Packages d'installation**.

3. Spécifiez le package d'installation pour le logiciel Kaspersky Security 10 pour les appareils mobiles.

4. Lancez le procédé de la création du package autonome par l'un des moyens ci-dessous :

   - dans le menu contextuel du dossier **Packages d'installation** choisissez **Créer un package autonome** ;

   - dans le menu contextuel de la liste des packages d'installation choisissez **Créer un package autonome** ;

   - sur le lien **Créer un package autonome** dans le bloc de gestion des packages d'installation.

Comme résultat, l'assistant de la création du package autonome d'installation va se lancer. Il faut suivre ses indications.

Notez bien que lorsque vous créez un package autonome, il ne faut pas spécifier qu'un package est créé pour installer l'Agent d'administration.

Après la fin du travail de l'assistant, si la case **Ouvrir la liste des packages autonomes** est cochée pendant la dernière étape, la fenêtre avec la liste de tous les packages disponibles va s'ouvrir. Lors de la sélection d'un package, le logiciel affiche l'emplacement du fichier sur le serveur Web Kaspersky Security Center (champ **URL**) et dans le dossier partagé de l'administrateur (champ **Destination**).

A cette étape, le fichier d'installation de l'application <PRODUCT_NAME> est prêt à la diffusion parmi les utilisateurs. Lors de la diffusion des messages texte (SMS) aux utilisateurs, vous devez spécifier le lien pour le téléchargement qui se trouve dans le champ **URL** (adresse du package autonome sur le serveur Web de Kaspersky Security Center).

Il est recommandé de copier l'adresse d'un package autonome dans le presse-papiers pour ajouter ensuite le lien sur le téléchargement d'un fichier d'installation souhaité dans le message texte (SMS) destiné aux utilisateurs.

LA DIFFUSION DES MESSAGES TEXTE AUX UTILISATEURS

Pour envoyer aux utilisateurs un message texte contenant le lien sur le package autonome d'installation du logiciel Kaspersky Security 10, procédez comme suit :

1. Sélectionnez dans l'arbre de la console le Serveur d'administration auquel les appareils portables seront branchés.
2. Dans l'arbre de la console sélectionnez le dossier **Comptes utilisateurs**.
3. Sélectionnez un ou plusieurs utilisateurs.
4. Dans le menu contextuel, sélectionnez l'option **Envoyer un SMS**.

   La fenêtre de création des SMS s'ouvre.
5. Sélectionnez le type du numéro de téléphone de l'utilisateur vers lequel vous souhaitez envoyer le message en cochant une ou plusieurs cases à côté de **Utiliser le numéro de mobile**, **Utiliser le numéro de téléphone complémentaire** ou **Utiliser le numéro de téléphone principal**.
6. Saisissez le texte du message en insérant le lien sur le package autonome d'installation stocké sur le serveur Web. Le message sera envoyé aux utilisateurs sélectionnés.
7. Appuyez **OK** pour l'envoi.

INSTALLATION DE L'APPLICATION SUR L'APPAREIL MOBILE A LA RECEPTION DU MESSAGE TEXTE

Après avoir reçu un message texte contenant le lien sur le package autonome, l'utilisateur peut télécharger le fichier de distribution sur son appareil portable par des moyens accessibles. Le package autonome contient le fichier d'installation pour le système d'exploitation Android avec la configuration présélectionnée de connexion au Serveur d'administration.

Le téléchargement terminé, l'utilisateur ouvre le fichier d'installation sur son appareil, l'assistant de l'installation du logiciel se lance automatiquement. L'utilisateur doit suivre les indications de l'assistant de l'installation.

Si tous les paramètres de la connexion au Serveur d'administration ont été indiqués lors de la création du package d'installation, alors la configuration initiale du logiciel (cf.la section "La préparation du logiciel au fonctionnement" à la page 48) n'est pas nécessaire.

Par défaut, le système d'exploitation Android interdit toute installation d'application hors Google Play. Si le système ne procède pas à l'installation, l'utilisateur doit autoriser l'installation des applications depuis une source externe dans les paramètres de son appareil tournant sous Android.

L'INSTALLATION DU LOGICIEL VIA POSTE TERMINAL

Pour installer Kaspersky Security depuis une station de travail, vous devez créer un package d'installation et configurer ses paramètres. Ensuite, vous devez créer et lancer la tâche d'installation à distance pour les stations de travail auxquelles les appareils mobiles d'utilisateurs sont connectés. Pour créer la tâche, l'administrateur peut utiliser plusieurs options prévues dans Kaspersky Security Center :

- créer une tâche d'installation à distance de groupe si les stations de travail font partie d'un seul groupe ;
- créer une tâche pour un jeu d'ordinateurs si les stations de travail font partie de groupes différents ou du groupe **Ordinateurs non repartis** ;
- utiliser l'assistant d'installation à distance.

L'exécution de la tâche d'installation à distance consiste à envoyer vers les stations de travail des utilisateurs le package d'installation avec la distribution de l'application Kaspersky Security 10 for Mobile, à installer et à lancer l'utilitaire de livraison de la distribution de l'application sur les appareils mobiles kmlisten.exe. Cet utilitaire contrôle la connexion des appareils mobiles à l'ordinateur. Dès que l'utilisateur connecte à la station de travail un appareil dont la configuration système permet d'installer Kaspersky Security 10 for Mobile l'utilitaire affiche sur l'écran un message qui propose d'installer l'application sur l'appareil mobile connecté. Si l'utilisateur autorise l'installation, l'utilitaire télécharge la distribution de l'application sur l'appareil. Après le téléchargement, l'assistant de l'installation va se mettre en route. Suivant les indications de l'assistant, l'utilisateur effectue lui-même l'installation de Kaspersky Security 10 for Mobile sur son appareil.

DANS CETTE SECTION

LA CREATION DU PACKAGE D'INSTALLATION

Le package d'installation Kaspersky Security 10 for Mobile est un archive auto-décompactable sc_package.exe qui contient les fichiers pour l'installation du logiciel sur les appareils mobiles :

- `endpoint_8_0_0_37_fr.cab` – fichier d'installation pour le système d'exploitation Windows Mobile ;
- `endpoint8_mobile_8_1_44_fr.sisx` – fichier d'installation pour le système d'exploitation Symbian ;
- `endpoint8_Mobile_8_1_29_fr.zip` – fichier d'installation pour le système d'exploitation BlackBerry ;
- `KSM_10_1_75_fr.apk` – fichier d'installation pour le système d'exploitation Android ;
- `installer.ini` – fichier de configuration contenant les paramètres de connexion au Serveur d'administration ;
- `kmlisten.ini` – fichier de configuration contenant les paramètres pour l'utilitaire de la livraison du package d'installation ;
- `kmlisten.kpd` – fichier contenant la description du logiciel ;

- `AdbWinUsbApi.dll, AdbWinApi.dll, adb.exe` – kit des fichiers de l'installation du logiciel sur les appareils sous le système d'exploitation Android ;

- `kmlisten.exe` – utilitaire de la livraison de la distribution du logiciel sur l'appareil mobile via le poste terminale.

Pour créer le package d'installation Kaspersky Security 10 for Mobile, procédez comme suit :

1. Sélectionnez dans l'arbre de la console le Serveur d'administration auquel les appareils portables seront branchés.

2. Dans l'arbre du console, au dossier **Installation à distance** sélectionnez le sous-dossier **Packages d'installation**.

3. Lancez la création du package d'installation par l'un des procédés suivants :

   - dans le menu contextuel du dossier **Packages d'installation** sélectionnez **Créer → un package d'installation** ;

   - dans le menu contextuel de la liste des packages d'installation sélectionnez **Créer → un package d'installation** ;

   - sur le lien **Créer un package d'installation** dans le bloc de gestion de la liste des package d'installation.

   Au final, l'assistant de la création du package d'installation va se lancer. Il faut suivre ses indications.

   Faites attention à la configuration suivantes :

   - Dans la fenêtre de l'assistant **Sélectionnez le type du package d'installation** appuyez sur le bouton **Créer le package d'installation "Kaspersky Lab"**.

   - Dans la fenêtre de l'assistant **Sélection de la distribution du logiciel à installer** à l'aide du bouton **Sélectionner** ouvrez le fichier où vous avez placé la distribution du logiciel et sélectionnez l'archive auto-décompactable sc_package.exe. Si l'archive a été décompactée avant, vous pouvez sélectionner un fichier faisant partie de l'archive avec la description du programme kmlisten.kpd. Finalement le nom du logiciel ainsi que le numéro de la version vont apparaitre dans le champ de saisie.

   Après la fin du travail de l'assistant, le package d'installation ainsi créé va s'afficher dans la zone de travail du dossier **Packages d'installation**. Les packages d'installation sont stockés dans un dossier défini partagé dans le dossier de service Packages du Serveur d'administration.

Avant d'utiliser le package d'installation ainsi créé, il faut configurer les paramètres du package d'installation (cf. section "Configuration des paramètres du package d'installation" à la page 42).

LA CONFIGURATION DU PACKAGE D'INSTALLATION

La configuration du package d'installation du logiciel Kaspersky Security 10 for Mobile est nécessaire pour que l'appareil mobile puisse utiliser les paramètres correctes de la connexion au Serveur d'administration.

Pour configurer les paramètres du package d'installation, procédez comme suit :

1. Sélectionnez dans l'arbre de la console le Serveur d'administration auquel vous souhaitez connecter les appareils portables.

2. Dans l'arbre du console, au dossier **Installation à distance** sélectionnez le sous-dossier **Packages d'installation**.

3. Dans le menu contextuel du package d'installation du logiciel Kaspersky Security, sélectionnez **Propriétés**.

4. Sur l'onglette **Paramètres** indiquez les paramètres de connexion des appareils portables au Serveur d'administration et le nom du groupe où les appareils portables seront ajoutés après la première synchronisation avec le Serveur d'administration. Pour ce faire, procédez comme suit :

   - Dans le bloc **Connexion avec le Serveur d'administration** dans le champ **Adresse de serveur** saisissez le nom du Serveur d'administration pour connecter les appareils mobiles dans le même format qui a été spécifié lors de l'installation du composant **Support des appareils mobiles** pendant le déploiement du Serveur d'administration.

     C'est à dire, selon le format du nom de Serveur d'administration pour le composant **Support des appareils mobiles** indiquez le nom DNS ou IP-adresse du Serveur d'administration. Dans le champ **Numéro du port SSL** indiquez le numéro du port qui est ouvert sur le Serveur d'administration pour connecter les appareils mobiles. Le numéro de port par défaut est 13292.

   - Dans le bloc **Répartition des ordinateurs selon les groupes** dans le champ **Nom du groupe** saisissez le nom du groupe où les appareils portables seront ajoutés après la première synchronisation avec le Serveur d'administration (par défaut KSM10).

     Le groupe sélectionné sera automatiquement crée dans le dossier **Ordinateurs non-repartis**.

   - Dans le bloc **Actions à l'entreprendre lors de l'installation** cochez la case **Demander l'adresse du courrier électronique** pour que lors du premier lancement le logiciel demande à l'utilisateur son adresse e-mail de fonction.

     L'adresse e-mail de l'utilisateur est utilisée pour créer le nom des appareils mobiles lorsqu'ils sont ajoutés à un groupe d'administration. Le nom de l'appareil mobile sous Android est formé selon la règle <adresse e-mail de l'utilisateur (modèle de l'appareil mobile – device ID)>.

5. Pour appliquer les paramètres sélectionnez appuyez sur **Appliquer**.

LA CREATION DE LA TACHE DE L'INSTALLATION A DISTANCE

Il est nécessaire de créer la tâche de l'installation à distance pour l'installation à distance du logiciel à l'aide de Kaspersky Security Center La tâche prescrite de l'installation à distance sera lancée conformément à son horaire.

Pour plus des renseignements sur l'installation à distance, adressez-vous au *Guide de la mise en œuvre Kaspersky Security Center*.

La tâche d'installation à distance pour Kaspersky Security for Mobile pour le groupe sélectionné de l'administration peut être créée de plusieurs manières :

- à l'aide *de l'assistant de la création de tâche de l'installation à distance*

  - sur les ordinateurs d'utilisateur auxquels les appareils mobiles seront connectés ;

  - sur les ordinateurs du groupe d'administration auxquels les appareils mobiles seront connectés ;

- à l'aide *de l'assistant de l'installation à distance*.

Selon les modes d'installation choisies, le fonctionnement de l'assistant et les paramètres à configurer peuvent varier. Faites attention à la configuration suivantes :

- Sélection du type de la tâche. Sur cette étape, spécifiez que la tâche de l'installation à distance va être créée pour le logiciel Kaspersky Security Center, et le type de cette tâche est **L'installation à distance du logiciel**.

- La sélection d'un package d'installation. Sur cette étape, sélectionnez un package d'installation déjà prêt qui contient le fichier de distribution Kaspersky Security 10 for Mobile ainsi que les configurations de la connexion des appareils mobiles au Serveur d'administration avec le logiciel installé. Vous pouvez créer le package d'installation sur cette étape même, mais dans ce cas il ne contient pas les configurations de connexion, les utilisateurs devront faire la configuration initiale du logiciel à la main. Lors de la création du package d'installation, sélectionnez l'archive auto-décompactable sc_package.exe. Si l'archive a été décompactée

auparavant, vous pouvez sélectionner le fichier avec la description du logiciel kmlisten.kpd faisant partie de l'archive.

- Sélection du type d'installation. L'installation à distance du logiciel aux postes terminales du Kaspersky Security Center se produit par l'un des deux procédés : par un procédé de l'installation forcée et par un procédé de l'installation à l'aide d'un scénario d'entrée. Le procédé de l'installation forcée permet d'effectuer l'installation à distance du logiciel sur les postes terminales déterminées. Le procédé d'installation à distance à l'aide d'un scénario d'entrée permet d'associer le lancement d'une tâche d'installation à distance à un compte utilisateur particulier (ou à plusieurs comptes).

  Cette étape est absente lors du fonctionnement de l'assistant d'installation à distance et de l'assistant de la création d'une tâche de groupe car ici se produit l'installation sur les postes terminales déterminées et le procédé de l'installation forcée est utilisé. Pour installer le Kaspersky Security 10 for Mobile à l'aide d'une tâche spécifique pour le groupe d'ordinateurs, l'administrateur peut utiliser n'importe quel procédé.

  Plus d'information sur l'installation élongée des logiciel vous pouvez voir au *Guide d'administrateur Kaspersky Security Center*.

- La sélection des ordinateurs pour l'installation. A cette étape il vous sera proposé de former la liste des postes terminales à travers lesquels le logiciel sera installé sur les appareils mobiles. Vous pouvez sélectionner l'une des options suivantes :

  - **Installation sur le groupe des ordinateurs administrés**. Utilisez cette option si vous avez créé lors de la préparation d'installation un groupe d'administration dans le dossier **Ordinateurs administrés** où vous avez déplacé les ordinateurs avec les appareils mobiles connectés.

  - **Sélectionner les ordinateurs pour l'installation**. Vous pouvez sélectionner cette option si le groupe n'a pas été créé. A l'étape suivante l'assistant va vous proposer de former la liste des ordinateurs pour installer le logiciel.

- La sélection du moyen de téléchargement du package d'installation. A cette étape il vous sera proposé de configurer les paramètres de livraison du package d'installation vers les postes terminal. La livraison du package d'installation vers les postes terminal peut être effectuée par deux moyens :

  - **A l'aide de l'Agent d'administration**. Choisissez ce moyen si sur les postes terminaux, à travers lesquels le Kaspersky Security 10 for Mobile est installé, l'Agent d'administration est installé et connecté au Serveur d'administration.

    Si l'Agent de l'administration n'est pas installé et vous souhaitez l'installer, vous pouvez utiliser l'installation conjointe qui vous sera proposée à l'étape suivante du fonctionnement de l'assistant.

  - **A l'aide des moyens Microsoft Windows à partir du dossier partagé**. Choisissez cette option si l'Agent d'administration n'est pas installé sur les postes terminaux ou il est branché à l'autre Serveur d'administration. Ici la transmission des fichiers d'installation s'effectue à l'aide des moyens Microsoft Windows à partir des dossiers partagés.

- Le choix du package d'installation supplémentaire. A cette étape il vous sera proposé d'installer l'Agent d'administration sur les postes terminaux. Utilisez l'installation conjointe si l'option A l'aide de l'Agent d'administration a été choisie à l'étape précédente mais **l'Agent d'administration** n'est pas encore installé sur les postes terminaux. Dans ce cas, on installe d'abord l'Agent d'administration sur les postes terminaux, et après le package d'installation du logiciel est délivré à l'aide de l'Agent d'administration.

  L'installation conjointe n'est pas nécessaire si la livraison de la distribution vers les postes terminaux est effectuée par les moyens du Microsoft Windows ou la version de l'Agent d'administration répondante aux exigences de la configuration pour l'installation Kaspersky Security 10 for Mobile est déjà installée.

LA LIVRAISON DU FICHIER DE DISTRIBUTION SUR L'APPAREIL MOBILE VIA LE POSTE TERMINALE

La livraison du fichier de distribution sur l'appareil mobile Kaspersky Security est effectuée par le programme utilitaire kmlisten.exe installé sur le terminal au cours de l'exécution de la tâche d'installation à distance. Lorsque vous connectez l'appareil répondant aux exigences d'appareillage et de logiciel à un ordinateur, l'utilitaire demande à l'utilisateur d'installer Kaspersky Security 10 for Mobile sur l'appareil mobile connecté.

Afin de copier le fichier de distribution Kaspersky Security 10 for Mobile à partir du poste terminal sur l'appareil mobile, il faut procéder comme suit :

1. Connecter l'appareil au poste terminal.

   Si l'appareil réponde aux exigences de système pour l'installation du logiciel, la fenêtre de l'utilitaire kmlisten.exe va s'ouvrir automatiquement.

2. Dans la liste des appareils détectés vous choisissez un ou plusieurs appareils où il faut installer le logiciel.

3. Appuyer sur le bouton **Installer**.

   L'utilitaire va copier le fichier de distribution sur les appareils choisi et va afficher les résultats du fonctionnement. L'installation de Kaspersky Security va se lancer automatiquement sur l'appareil mobile après le téléchargement correct de la distribution.

   La fenêtre **KSM 10** de l'utilitaire kmlisten.exe s'ouvre et propose d'installer le logiciel à chaque connexion de l'appareil mobile vers l'ordinateur.

4. Là où il faut désactiver l'affichage de la fenêtre **KSM10** de l'utilitaire kmlisten.exe avec la proposition d'installer le logiciel, cochez la case dans cette fenêtre **Arrêter le lancement automatique du logiciel d'installation Kaspersky Security 10 for Mobile**.

L'INSTALLATION DE L'APPLICATION SUR L'APPAREIL MOBILE DEPUIS UNE STATION DE TRAVAIL

Une fois le téléchargement du package d'installation sur l'appareil mobile terminé, l'application est automatiquement installée sur l'appareil sans l'intervention de l'utilisateur. L'utilisateur doit suivre les indications de l'assistant de l'installation.

Si tous les paramètres de la connexion au Serveur d'administration ont été indiqués lors de la création du package d'installation, alors la configuration initiale du logiciel (cf.la section "La préparation du logiciel au fonctionnement" à la page 48) n'est pas nécessaire.

Par défaut, le système d'exploitation Android interdit toute installation d'application hors Google Play. Si le système ne procède pas à l'installation, l'utilisateur doit autoriser l'installation des applications depuis une source externe dans les paramètres de son appareil tournant sous Android.

L'INSTALLATION DU LOGICIEL SANS L'ADMINISTRATEUR

Le téléchargement immédiat du fichier d'installation sur l'appareil est utilisé lorsque les utilisateurs sont en mesure d'installer seuls l'application, par exemple en téléchargeant le fichier d'installation sur Google Play.

Dans ce cas, ne préparez pas la distribution de l'application, l'utilisateur indiquera lui-même les paramètres de connexion au serveur d'administration (cf. section "Préparation de l'application au fonctionnement sur l'appareil " à la p. 48) lors du lancement initial de l'application.

Par défaut, le système d'exploitation Android interdit toute installation d'application hors Google Play. Si le système ne procède pas à l'installation, l'utilisateur doit autoriser l'installation des applications depuis une source externe dans les paramètres de son appareil tournant sous Android.

INSTALLATION SUR DES APPAREILS TOURNANT SOUS IOS

Cette section décrit la procédure d'installation de Kaspersky Security 10 for mobile sur des appareils tournant sous le système d'exploitation iOS.

DANS CETTE SECTION

CONFIGURATION DE L'INTERFACE DE KASPERSKY SECURITY CENTER POUR LA GESTION DES APPAREILS MOBILES

Pour configurer l'interface de Kaspersky Security Center pour la gestion des appareils mobiles, procédez comme suit :

1. Sélectionnez dans l'arbre de la console le Serveur d'administration auquel les appareils portables seront branchés.
2. Dans le menu contextuel, les dossiers **Serveur d'administration** sélectionnez l'option **Affichage → Configuration de l'interface**.
3. Dans la fenêtre **Configuration de l'interface** cochez la case **Afficher la gestion des appareils mobiles**.
4. Cliquez sur le bouton **OK**.
5. Pour que les modifications soient prises en compte, redémarrez la console d'administration.

CREATION ET L'ENVOI DU PROFIL IOS MDM

Le profil iOS MDM permet de distribuer les profils iOS configurés en arrière-plan à l'aide du serveur MDM et recevoir des informations de diagnostics complètes sur les appareils mobiles. Le profil iOS MDM doit être diffusé pour que le serveur d'administration puisse détecter les appareils mobiles tournant sous iOS.

Pour créer le profil iOS MDM et l'envoyer sur un appareil mobile, procédez comme suit :

1. Dans l'arborescence, sélectionnez le dossier **Comptes utilisateur**.
2. Sélectionnez le compte utilisateur avec lequel vous voulez installer le profil iOS MDM sur l'appareil mobile.

3. Dans le menu contextuel du compte utilisateur de l'appareil mobile, sélectionnez l'option **Installer le profil iOS MDM sur l'appareil mobile de l'utilisateur.**

   La fenêtre **Installation du profil iOS MD** s'ouvre.

   Le profil iOS MDM est automatiquement créé lors de la requête via l'onglet **Comptes utilisateur**.

4. Dans la fenêtre **Installation du profil iOS MDM** dans le champ **Liste des serveurs disponibles des appareils mobiles iOS MDM** sélectionnez **Serveur des appareils mobiles iOS MDM** pour lesquels la création du profil iOS MDM est nécessaire.

5. Dans la fenêtre **Installation du profil iOS MDM**, indiquez le mode d'envoi de notification à l'utilisateur sur l'installation du profil iOS MDM sur l'appareil mobile :

   - **Par SMS**. Cochez la case pour envoyer à l'utilisateur le message texte avec le lien pour télécharger le profil MDM. Dans le champ **Texte SMS**, saisissez le message destiné à l'utilisateur ou utilisez la notification par défaut. Dans la liste déroulante, à côté du champ de saisie **Texte SMS**, sélectionnez l'option **Mot de passe à usage unique** et indiquez le mot de passe de l'utilisateur.

     La diffusion du profil iOS MDM par SMS est uniquement possible sur des appareils équipés du module GSM.

   - **Par courrier électronique**. Cochez la case pour envoyer à l'utilisateur une notification par courrier électronique contenant le lien pour télécharger le profil MDM et le code QR spécialement créé pour cette notification. Dans le champ **Objet**, indiquez l'objet de la notification. Dans le champ **Texte de la notification**, saisissez la notification pour l'utilisateur. Dans la liste déroulante, à côté du champ **Texte de la notification**, sélectionnez l'option **Mot de passe à usage unique** et indiquez le mot de passe de l'utilisateur.

6. Cliquez sur le bouton **OK**.

L'utilisateur de l'appareil mobile reçoit la notification avec le lien pour télécharger le profil iOS MDM à partir du portail web. L'utilisateur se dirige de lui-même vers le lien reçu ou le code QP en téléchargeant le profil iOS MDM sur son appareil iOS.

Après avoir téléchargé le profil iOS MDM et synchronisé avec le serveur d'administration, l'appareil tournant sous iOS apparaîtra dans le dossier **Appareils mobiles** dans le sous-dossier **Appareils mobiles iOS MDM**.

INSTALLATION DE L'APPLICATION SUR UN APPAREIL MOBILE IOS

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

1. Sélectionnez dans l'arbre de la console le Serveur d'administration auquel les appareils portables seront branchés.

2. Ouvrez le sous-dossier **Appareils mobiles iOS MDM** dans le dossier **Appareils mobiles**.

3. Sélectionnez un ou plusieurs appareils de la liste.

4. Lancez l'installation de l'application sur l'appareil en choisissant une des méthodes suivantes :

   - Dans le menu contextuel, sélectionnez l'option **Installer l'application sur l'appareil** et choisissez dans la liste de Kaspersky Security.

   - Le lien **Installer l'application sur l'appareil** dans le groupe des appareils sélectionnés.

   L'utilisateur doit confirmer la commande d'installation de l'application sur l'appareil.

Dès que l'appareil mobile de l'utilisateur est synchronisé avec le serveur d'administration, l'utilisateur reçoit une requête pour installer l'application. Après avoir reçu l'acception pour l'installation sur l'appareil mobile, l'application est automatiquement téléchargée et installée sur l'appareil sans l'intervention de l'utilisateur. L'icône de l'application apparaît sur l'appareil qui indique la progression de son téléchargement. Ensuite, l'utilisateur doit effectuer la configuration initiale de l'application (cf. section "Préparation du logiciel pour le fonctionnement sur l'appareil" à la page 48) sur l'appareil. Pour cela, l'utilisateur indique les paramètres de connexion au serveur d'administration reçus par l'administrateur par courrier électronique ainsi que l'adresse de sa messagerie électronique.

INSTALLATION DEPUIS DES STATIONS DE TRAVAIL SUR LES APPAREILS TOURNANT SOUS BLACKBERRY, SYMBIAN ET WINDOWS MOBILE

Paquet de livraison de Kaspersky Security 10 for mobile (cf. section " Paquet de livraison " à la p. 12) contient la distribution de l'application des systèmes d'exploitation. La plateforme BlackBerry, Symbian et Windows Mobile comprend les distributions de Kaspersky Endpoint Security 8.0 for Smartphone.

Le module externe d'administration de Kaspersky Security 10 pour Kaspersky Security Center prend en charge l'administration des appareils équipés de Kaspersky Endpoint Security 8.0 for Smartphone.

La procédure d'installation de l'application sur les appareils tournant sous les systèmes d'exploitation BlackBerry, Symbian et Windows Mobile est identique à la procédure d'installation sur les appareils tournant sous Android depuis les stations de travail d'utilisateurs.

LA PREPARATION DU LOGICIEL POUR LE FONCTIONNEMENT SUR L'APPAREIL

Le paramétrage de configuration initiale de la connexion au serveur d'administration n'est pas requis dans les cas suivants :

- un package autonome ou un fichier d'installation préconfiguré est installé sur l'appareil mobile sous Android (par exemple, lors du déploiement à l'aide de l'envoi des messages texte ou électronique).
- le logiciel est installé sur l'appareil mobile après la connexion vers le poste terminal (lors du déploiement via les postes terminaux pour les systèmes d'exploitation Android, BlackBerry, Symbian, Windows Mobile).

Dans les autres cas il suffit de sélectionner une fois les paramètres de connexion au Serveur d'administration :

- **Adresse du serveur**

  Si l'adresse IP est indiquée dans les propriétés du Serveur d'administration, alors l'utilisateur sera obligé de saisir cette adresse IP. Si le nom DNS est indiqué dans les propriétés du Serveur d'administration, alors l'utilisateur sera obligé de saisir ce nom.

- **Numéro du port SSL**

  L'utilisateur doit saisir le numéro du port de Serveur d'administration destiné pour les appareils mobiles. Le numéro de port par défaut est 13292. Le numéro du port est indiqué dans les propriétés du Serveur d'administration, section Paramètres.

ACTIVATION DE L'APPLICATION

Dans Kaspersky Security Center, la licence peut couvrir différents groupes fonctionnels. Pour pouvoir utiliser toutes les fonctionnalités du module externe d'administration de Kaspersky Security 10 et de l'application Kaspersky Security sur les appareils mobiles, la licence pour Kaspersky Security Center acquise par l'entreprise doit couvrir la fonctionnalité Administration des appareils mobiles. La fonctionnalité Administration des appareils mobiles sert à connecter et à administrer des appareils mobiles via Exchange ActiveSync et iOS MDM, ainsi que l'administration des appareils mobiles équipés de l'application Kaspersky Security 10.

Pour plus d'information sur la licence pour Kaspersky Security Center et les options de la licence, adressez-vous au *Guide d'administrateur de Kaspersky Security Center*.

L'activation de l'application Kaspersky Security 10 for Mobile est une procédure particulière, car les informations sur la licence sont transmises sur l'appareil mobile avec la stratégie (cf. section " Création d'une stratégie de groupe pour Kaspersky Security 10 for Mobile " à la page 28) lors de la synchronisation de l'appareil au Serveur d'administration. Après l'installation de l'application, l'appareil se connecte au Serveur d'administration tous les trois heures. Après l'application de la stratégie, la fréquence de synchronisation de l'appareil au Serveur d'administration sera celle spécifiée dans les paramètres de réseau lors de la création de la stratégie. La fréquence de synchronisation par défaut est toutes les 6 heures.

Pour activer l'application sur l'appareil mobile, vous devez créer une stratégie pour le groupe (cf. section " Création d'une stratégie de groupe pour Kaspersky Security 10 for Mobile" à la page 28) dont l'appareil fait partie et spécifiez pour cette stratégie une clé qui se trouve dans le stockage du Serveur d'administration et qui a été ajoutée à l'aide d'un code d'activation ou d'un fichier de licence. Lors de la connexion suivant de l'appareil mobile au Serveur d'administration, les informations sur la licence seront téléchargées sur l'appareil avec la stratégie. Par conséquent, l'application Kaspersky Security 10 installée sur l'appareil sera activée.

Si l'application n'est pas activée dans les trois jours qui suivent l'installation de Kaspersky Security 10 sur l'appareil mobile, ses fonctionnalités seront automatiquement restreintes. La plupart de ses composants seront désactivés. Lorsque les fonctionnalités de l'application sont restreintes, elle ne pourra plus effectuer une synchronisation automatique au Serveur d'administration. Si l'application n'a pas été activée dans les trois jours qui suivent son installation, l'utilisateur doit effectuer la synchronisation avec le Serveur d'administration manuellement.

SUPPRESSION DE L'APPLICATION

Dans cette section vous trouverez l'information sur la suppression du logiciel Kaspersky Security 10 à partir des appareils mobiles d'utilisateurs.

Le moyen de suppression du Kaspersky Security dépend du système d'exploitation des appareils mobiles.

DANS CETTE SECTION

SUPPRESSION DE L'APPLICATION A PARTIR DES APPAREILS SOUS ANDROID

L'utilisateur peut lui-même supprimer l'application Kaspersky Security 10 depuis son appareil sous la gestion Android si c'est autorisé par la politique du groupe dont l'appareil fait partie.

Si la politique autorise la possibilité de suppression de l'application, alors l'utilisateur peut lui-même supprimer le Kaspersky Security depuis son appareil à l'aide de l'interface de l'application ou à l'aide du contrôle de l'appareil sous Android.

Si la politique interdit de supprimer le Kaspersky Security depuis l'appareil, dans ce cas il faut s'adresser à l'administrateur. L'administrateur peut éliminer le logiciel soit à distance à l'aide des moyens Kaspersky Security Center (cf. section "Suppression du logiciel sans utilisateur " à la page 51) sans utilisateur, soit par permission de supprimer permettre de supprimer le logiciel (cf. section "Permettre aux utilisateurs de supprimer le logiciel" à la page 50) depuis son appareil selon la politique appliqué.

PERMETTRE AUX UTILISATEURS DE SUPPRIMER LE LOGICIEL

Vous pouvez permettre aux utilisateurs de supprimer l'application Kaspersky Security 10 for Mobile à partir des appareils mobiles par la politique du groupe applicable. Si vous n'êtes pas contre la possibilité de suppression du programme pour tous les appareils du groupe, vous pouvez autoriser cette action dans les propriétés de la politique du groupe établie auparavant.

Si vous souhaitez autoriser la suppression du programme uniquement sur les certains appareils, vous devez configurer une politique de groupe spéciale et de l'appliquer pour les appareils appropriés. Au cours de la prochaine synchronisation des appareils mobiles avec le Serveur d'administration ce logiciel sera accessible pour l'auto-élimination.

Pour permettre aux utilisateurs de supprimer l'application Kaspersky Security à partir de ses appareils mobiles, procédez comme suit :

1. Sélectionnez dans l'arbre de la console le Serveur d'administration auquel les appareils portables seront branchés.
2. Dans l'arbre de la console ouvrez le dossier **Ordinateurs administrés**.
3. Dans le dossier **Ordinateurs administrés** choisissez le groupe où vous souhaitez autoriser la suppression du logiciel.
4. Vous pouvez créer un nouveau sous-groupe par l'un des moyens suivant :
   - à l'aide de la commande du menu contextuel **Créer → un Groupe** ;
   - sur le lien **Créer un sous-groupe** situé sur l'onglet dans la zone de travail de la fenêtre principale **Groupes**.
5. Dans la fenêtre **Nom de groupe** qui s'ouvre, saisissez le nom de groupe, puis cliquez sur le bouton **OK**.
6. Lancez la procédure de l'ajout des appareils pour lesquels vous souhaitez autoriser la suppression de l'application par l'un des procédés suivants :
   - sur le lien **Ajouter des ordinateurs dans le groupe** situé sur l'onglet dans la zone de travail de la fenêtre principale **Groupes** ;
   - sur le lien **Ajouter des ordinateurs** situé sur l'onglet dans la zone de travail de la fenêtre principale **Ordinateurs**.

   Comme résultat, l'assistant de l'ajout des ordinateurs va se lancer. Il faut suivre ses indications.

7. Dans la zone de travail du groupe créé sélectionnez l'onglet **Politiques** et lancer l'assistant de la création de la politique sur le lien **Créer la politique**.

   Suivez les indications de l'assistant. Modifiez les paramètres aux étapes suivantes :

   - à l'étape **Choix du logiciel** lors de la création de la politique de groupe choisissez Kaspersky Security pour les appareils mobiles.
   - à l'étape **Paramètres supplémentaires** du bloc **Gestion du logiciel** cochez la case **Permettre la suppression du Kaspersky Security 10 for Mobile**.
   - à l'étape **Création de la politique de groupe** pour le logiciel dans le bloc des paramètres **Etat de la politique** choisissez l'option **Politique active**.

   La politique ainsi créée sera active pour le groupe choisi lors de la prochaine synchronisation des appareils mobiles du groupe avec le Serveur d'administration, le logiciel Kaspersky Security sera accessible pour la suppression par les utilisateurs eux-mêmes.

LA SUPPRESSION DU LOGICIEL A PARTIR DE L'APPAREIL SANS LA PARTICIPATION DE L'UTILISATEUR

Vous pouvez effectuer la suppression à distance du Kaspersky Security 10 for Mobile à partir des appareils mobiles d'utilisateurs connectés au Serveur d'administration Kaspersky Security Center. Pour cet effet, vous devez créer la politique spéciale du groupe et l'appliquer aux appareils appropriés. Lors de la prochaine synchronisation des appareils portables avec le Serveur d'administration, ce logiciel sera automatiquement supprimé.

Afin de supprimer le logiciel Kaspersky Security à partir des appareils mobiles sans utilisateur, procédez comme suit :

1. Sélectionnez dans l'arbre de la console le Serveur d'administration auquel les appareils portables seront branchés.
2. Dans l'arbre de la console ouvrez le dossier **Ordinateurs administrés**.
3. Dans le dossier **Ordinateurs administrés** sélectionnez le groupe des appareils d'où vous souhaitez supprimer le logiciel.
4. Vous pouvez créer un nouveau sous-groupe par l'un des moyens suivant :
   - à l'aide de la commande du menu contextuel **Créer → un Groupe** ;
   - sur le lien **Créer un sous-groupe** situé sur l'onglet dans la zone de travail de la fenêtre principale **Groupes**.
5. Dans la fenêtre **Nom de groupe** qui s'ouvre, saisissez le nom de groupe, puis cliquez sur le bouton **OK**.
6. Lancez la procédure de l'ajout des appareils dans un groupe d'où vous voulez supprimer le logiciel par l'un des procédés suivants :
   - sur le lien **Ajouter des ordinateurs dans le groupe** situé sur l'onglet dans la zone de travail de la fenêtre principale **Groupes** ;
   - sur le lien **Ajouter des ordinateurs** situé sur l'onglet dans la zone de travail de la fenêtre principale **Ordinateurs**.

   Comme résultat, l'assistant de l'ajout des ordinateurs va se lancer. Il faut suivre ses indications.

7. Dans la zone de travail du groupe choisissez l'onglet **Politiques** et lancez l'assistant de la création de la politique sur le lien **Créer la politique**.

   Au final, l'assistant de la création de la politique va se lancer. Il faut suivre ses indications. Modifiez les paramètres de la politique de suppression aux étapes suivantes :

   - à l'étape **Sélection du logiciel pour la création de la politique de groupe** sélectionnez Kaspersky Security pour les appareils mobiles.

   - à l'étape **Paramètres supplémentaires** dans le bloc **Gestion du logiciel** cochez la case **Supprimer Kaspersky Security 10 for Mobile**.

     Un avertissement sur l'impossibilité d'annuler cette opération va apparaitre dans la fenêtre de dialogue. Confirmez la suppression.

   - à l'étape **Création de la politique de groupe pour le logiciel** dans le bloc des paramètres **État de la politique** choisissez l'option **Politique active**.

   La politique ainsi créée sera active pour le groupe choisi, et le logiciel Kaspersky Security sera supprimé lors de la prochaine synchronisation des appareils mobiles de ce groupe avec le Serveur d'administration.

SUPPRESSION DE L'APPLICATION A PARTIR DES APPAREILS SOUS BLACKBERRY, SYMBIAN ET WINDOWS MOBILE

La suppression de l'application depuis les appareils sous BlackBerry, Symbian et Windows Mobile Kaspersky Security 10 for Mobile est effectuée par les utilisateurs eux-mêmes à l'aide de la procédure standard pour la plate-forme appropriée.

Avant la suppression de l'application depuis les appareils sous Windows Mobile et Symbian le masquage de l'information confidentielle sera automatiquement désactivé et l'information chiffrée auparavant sera déchiffrée. L'utilisateur de l'appareil mobile sous BlackBerry doit désactiver à la main le masquage de l'information confidentielle avant de supprimer l'application.

Pour supprimer l'application sur les appareils sous Symbian et Windows Mobile, l'utilisateur doit saisir le code secret installé lors le premier lancement. Si l'utilisateur a oublié ce code, l'administrateur doit s'adresser au Service de maintenance technique afin recevoir le programme utilitaire spécial pour la suppression de l'application sans code secret.

La suppression définitive de l'application est effectuée après le redémarrage de l'appareil.

SUPPRESSION DE L'APPLICATION A PARTIR DES APPAREILS SOUS IOS

La suppression de l'application Kaspersky Security 10 est faite par l'utilisateur à la main conformément à la règle de la plate-forme iOS.

Pour supprimer l'application Kaspersky Security de l'appareil sous iOS

appuyez et maintenez l'icône de l'application jusqu'à ce qu'elle commence à se balancer, puis appuyez sur la croix.

L'ECHANGE DE L'INFORMATION AVEC KASPERSKY SECURITY NETWORK

Le service Cloud de Kaspersky Security Network est un service en ligne " Kaspersky Lab" qui contient l'information sur la fiabilité des fichiers, des logiciels et des ressources Internet. Kaspersky Security utilise le service Cloud de Kaspersky Security Network pendant le fonctionnement des éléments suivants :

- La vérification. L'application effectue la vérification supplémentaire des logiciels installés avant leur premier lancement. La vérification est effectuée aussi pour les nouvelles menaces dont les informations ne sont pas encore ajoutées dans les bases antivirus.

- Protection Internet. L'application fait la vérification complémentaire des sites Web avant leur ouverture.

Dans l'Accord de licence vous pouvez lire l'information sur les données qui sont transmises au "Kaspersky Lab" lors de l'utilisation du service Cloud pendant le fonctionnement du Kaspersky Security sur les appareils mobiles. En acceptant les termes de l'Accord de licence, vous consentez de transmettre l'information suivante :

- les sommes de contrôle des fichiers traités (MD5) ;

- le nombre de l'installation des logiciels ;

- l'adresse du site Web visité en ce moment pour définir sa réputation ;
- les données statistiques sur les menaces détectées.

Toute l'information transmise au service Cloud ne contient pas de données personnelles et d'autre information confidentielle de l'utilisateur. L'information obtenue par le service Cloud de Kaspersky Security Network est protégée par le "Kaspersky Lab" conformément à la législation en vigueur. Pour plus d'informations, visitez notre site Web http://support.kaspersky.fr.

CONTACTER LE SUPPORT TECHNIQUE

Cette section présente les différentes méthodes d'obtention de l'assistance technique et les conditions à remplir pour pouvoir bénéficier de l'aide du service d'assistance technique.

DANS CETTE SECTION

MODES D'OBTENTION DU SUPPORT TECHNIQUE

Si vous ne trouvez pas la solution à votre problème dans la documentation de l'application ou dans une des sources des informations relatives à l'application (cf. section "Sources d'informations sur l'application" à la page 8), contactez le service d'assistance technique de Kaspersky Lab. Les experts du service d'assistance technique répondront à vos questions sur l'installation et l'utilisation de l'application.

Avant de contacter le service d'assistance technique, veuillez lire les règles d'octroi de l'assistance technique (http://support.kaspersky.com/fr/support/rules).

Vous pouvez contacter les experts du service d'assistance technique d'une des manières suivantes :

- Via téléphone. Vous pouvez demander une consultation des experts du service d'assistance technique russe ou internationale.
- Envoyer la demande via le système Kaspersky CompanyAccount au site Web du Service d'assistance technique. Cette méthode permet de contacter les experts du service d'assistance technique via un formulaire.

ASSISTANCE TECHNIQUE PAR TELEPHONE

Si vous êtes confronté à un problème que vous ne parvenez pas à résoudre, vous pouvez contacter les experts du service d'assistance technique russe ou internationale (http://support.kaspersky.com/fr/support/international).

Avant de contacter le Service d'assistance technique, prenez connaissance des règles de la mise à disposition de l'assistance technique (http://support.kaspersky.com/support/details). Nos experts pourront ainsi vous venir en aide plus rapidement.

OBTENTION DE L'ASSISTANCE TECHNIQUE VIA KASPERSKY COMPANYACCOUNT

Kaspersky CompanyAccount est un service Web (https://companyaccount.kaspersky.com) qui assure l'envoi des demandes vers Kaspersky Lab et le suivi du traitement de ces demandes par les experts de Kaspersky Lab.

Pour pouvoir accéder au Kaspersky CompanyAccount, vous devez vous inscrire (https://support.kaspersky.com/companyaccount/register?LANG=fr). Pour ce faire, il faut saisir le code d'activation ou de télécharger le fichier de licence, votre adresse de messagerie et le nom de votre entreprise. Le service va créer pour

votre entreprise un compte CompanyAccount et y ajouter automatiquement les informations sur la licence que vous avez acquise. Par la suite, ces informations permettront d'ajouter au compte CompanyAccount de votre entreprise tous les employés de l'entreprise inscrits dans Kaspersky CompanyAccount.

Kaspersky CompanyAccount permet de réaliser les opérations suivantes :

- Traiter les demandes :
  - Envoyer les demandes au Service d'assistance technique (cf. section "Demande électronique au Service d'assistance technique" à la page 57).
  - Envoyer les demandes d'analyse de fichiers au Laboratoire d'étude des virus (cf. section " Demande électronique au Laboratoire d'étude des virus "à la page 57).
  - Envoyer les demandes de signature de certificats (par exemple, pour signer les certificats APN (cf. section " Demande électronique de signature d'un certificat APN " à la page 57).
  - Envoyer les questions et les commentaires sur le fonctionnement du service Web Kaspersky CompanyAccount.
  - Effectuer des échanges de messages avec le Service d'assistance technique.
  - Contrôler l'état de traitement des demandes et consulter l'historique des demandes.
- Gérer les clés et les codes d'activation de l'entreprise :
  - Télécharger d'autres fichiers de licence et indiquer d'autres codes d'activation pour le compte utilisateur CompanyAccount de votre entreprise.
  - Supprimer les clés et les codes d'activation (avec des privilèges d'administrateur de CompanyAccount uniquement).
  - Consulter la liste d'applications couvertes par la licence.
  - Obtenir une copie du fichier de licence en cas de perte ou de suppression de celui-ci.
- Administrer les comptes utilisateur CompanyAccount (avec des privilèges d'administrateur de CompanyAccount uniquement) :
  - Ajout et suppression des comptes utilisateur.
  - Réinitialisation de mot de passe des comptes utilisateur.
  - Consultation des demandes.
  - Gestion des privilèges des comptes utilisateur.
- Recevoir les notifications :
  - Sur l'état de traitement de la demande.
  - A propos de l'expiration de la licence.
  - Sur l'ajout de nouveaux comptes utilisateurs au CompanyAccount (avec des privilèges appropriés uniquement).
  - A propos de l'ajout d'une nouvelle clé ou d'un nouveau code d'activation (avec des privilèges appropriés uniquement).

Pour pouvoir administrer le compte CompanyAccount de votre entreprise, vous devez envoyer une demande électronique en utilisant le formulaire **Question relative au compte CompanyAccount**. Après avoir obtenu des privilèges d'administrateur du compte CompanyAccount, vous pouvez administrer les comptes utilisateurs de votre entreprise et recevoir les notifications, notamment, sur l'ajout de nouveaux utilisateurs au compte CompanyAccount de votre entreprise.

DEMANDE ADRESSEE PAR VOIE ELECTRONIQUE AU SERVICE D'ASSISTANCE TECHNIQUE

Vous pouvez envoyer une demande par voie électronique au service d'assistance technique en russe, en anglais et en d'autres langues.

Vous devez fournir les informations suivantes dans les champs du formulaire :

- Type de demande ;
- Nom et numéro de version de l'application ;
- texte de la demande.

Si nécessaire, vous pouvez également joindre des fichiers au formulaire de demande électronique.

L'expert du Service d'assistance technique répond via le système Kaspersky CompanyAccount à l'adresse de messagerie indiquée lors de l'inscription.

DEMANDE ELECTRONIQUE ADRESSEE AU LABORATOIRE ANTIVIRUS

Certaines demandes ne sont pas envoyées au service d'assistance technique, mais au laboratoire antivirus.

Vous pouvez envoyer au laboratoire antivirus les demandes des types suivants :

- *Programme malveillant inconnu* : vous soupçonnez le fichier de contenir un virus, mais Kaspersky Internet Security ne marque pas ce fichier comme infecté.

  Les experts du Laboratoire antivirus analysent le code malveillant envoyé et en cas de découverte d'un virus inconnu jusque-là ajoutent sa définition à la base des données accessible lors de la mise à jour des logiciels antivirus.

- *Faux positif du logiciel antivirus* : Kaspersky Security considère un certain fichier comme infecté, mais vous êtes convaincu que ce n'est pas le cas.

Vous pouvez également envoyer une demande au Laboratoire antivirus depuis la page avec le formulaire de demande (http://support.kaspersky.com/virlab/helpdesk.html?LANG=fr), sans vous inscrire au compte Kaspersky CompanyAccount. Dans ce cas, vous ne devez pas indiquer le code d'activation de l'application. La priorité des demandes créées à l'aide du formulaire approprié est inférieure à celle des demandes créées via le compte Kaspersky CompanyAccount.

DEMANDE ELECTRONIQUE DE SIGNATURE D'UN CERTIFICAT APN

Vous pouvez envoyer au Service d'assistance technique une demande électronique de signature d'un certificat APN.

Pour ce faire, vous devez indiquer dans le formulaire de la demande électronique le fichier de demande d'un certificat APN http://support.kaspersky.com/9245.

Lorsque votre demande électronique sera traitée automatiquement, vous recevrez un fichier de demande d'un certificat APN signé par Kaspersky Lab pour le transférer à Apple.

Vous pouvez consulter la demande traitée dans la liste de demandes inactives de votre compte utilisateur.

GLOSSAIRE

A

Agent d'administration

Le fichier d'installation de l'application Kaspersky Security pour le système d'exploitation Android qui contient les paramètres de connexion de l'application au Serveur d'administration. Ce fichier est créé depuis le package d'installation pour cette application et représente un cas particulier d'un package des applications mobiles.

Appareil mobile iOS MDM

Un appareil mobile tournant sous iOS et administré par le Serveur des appareils mobiles iOS MDM.

C

Certificat Apple Push Notification service (APNs)

Il s'agit d'un certificat signé par la société Apple qui permet de diffuser les profils de configuration iOS en arrière-plan à l'aide du serveur MDM d'iOS.

Conteneur

Une enveloppe spéciale pour des applications mobiles qui permet de contrôler les activités de l'application dans le conteneur afin de protéger les données personnelles et d'entreprise stockées dans l'appareil.

G

Groupe d'administration

L'ensemble des appareils administrés, notamment, des appareils mobiles réunis suivant leurs fonctionnalités et l'ensemble d'applications dont ils seront équipés. Les appareils administrés sont groupés pour pouvoir les administrer comme un tout unique. Par exemple, un groupe peut comprendre des appareils mobiles tournant sous un même système d'exploitation. Un groupe peut comprendre d'autres groupes. Vous pouvez créer des stratégies de groupe et des tâches de groupe pour les appareils qui font partie d'un groupe.

M

Module externe d'administration de l'application

Un composant spécialisé qui fournit une interface pour administrer l'application de Kaspersky Lab via la Console d'administration. Chaque application a un module externe dédié. Ce module fait partie de toutes les applications de Kaspersky Lab administrées à l'aide de Kaspersky Security Center.

P

Package d'installation

Un ensemble de fichiers qui assure l'installation à distance de l'application de Kaspersky Lab à l'aide du système d'administration à distance. Le package d'installation est créé à partir de fichiers spéciaux faisant partie de la distribution de l'application. Il contient les paramètres nécessaires à l'installation de l'application et assure le fonctionnement de l'application après son installation. Les valeurs des paramètres sont celles des paramètres de l'application par défaut.

Package des applications mobiles

Un fichier d'installation pour le système d'exploitation Android (fichier avec l'extension apk) téléchargé sur le Serveur d'administration. Les packages des applications mobiles sont stockés sur le serveur Web Kaspersky Security Center ou dans le dossier partagé d'administrateur de Kaspersky Security Center. Les packages des applications mobiles peuvent être créés pour les programmes tiers. Lors de la procédure de création, vous pouvez indiquer que l'application sera placée dans le conteneur.

PROFIL IOS MDM

Il permet de distribuer les profils iOS configurés en arrière-plan à l'aide du serveur MDM et recevoir des informations de diagnostics complètes sur les appareils mobiles. Vous devez envoyer le profil iOS MDM à l'utilisateur pour permettre au serveur d'administration de détecter et de connecter son appareil mobile tournant sous iOS.

S

SERVEUR D'ADMINISTRATION

Un composant de l'application Kaspersky Security Center qui assure le stockage centralisé des informations relatives aux applications de Kaspersky Lab installées dans le réseau d'entreprise et à l'administration de ces applications.

SERVEUR DES APPAREILS MOBILES IOS MDM

Un composant du système d'administration de Kaspersky Security Center qui assure la connexion des appareils mobiles tournant sous iOS au Serveur d'administration et la gestion de ces appareils à l'aide des profils iOS MDM.

STRATEGIE

L'ensemble des paramètres de fonctionnement de l'application pour le groupe d'administration lorsque l'application est administrée à l'aide des outils de Kaspersky Security Center. Les paramètres de fonctionnement de l'application peuvent varier en fonction du groupe. La stratégie comprend les paramètres de la configuration complète pour toutes les fonctionnalités de l'application.

T

TACHE DE GROUPE (KSM)

Une tâche définie pour un groupe d'administration et exécutée par tous les appareils administrés faisant partie du groupe.

KASPERSKY LAB ZAO

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

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

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

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

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

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

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

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

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

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

INFORMATIONS SUR LE CODE TIERS

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt situé dans le dossier d'installation de l'application.

Pour les appareils tournant sous Android, les informations du fichier legal_notices.txt sont affichées dans la fenêtre **Avancé** dans la section **A propos de ...**.

NOTIFICATION SUR LES MARQUES

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

Apple est une marque déposée d'Apple Inc.

Android sont des marques déposées de Google, Inc.

Microsoft, Windows sont des marques de Microsoft Corporation déposées aux Etats-Unis et dans d'autres pays.

Nokia, Series 60 sont des marques ou des marques déposées de Nokia Corporation.

La marque BlackBerry appartient à Research In Motion Limited. Elle a été déposée aux Etats-Unis et peut être soumise à la procédure de dépôt ou déjà déposée dans d'autres pays.

La marque verbale Bluetooth et le logo approprié appartiennent à Bluetooth SIG, Inc.

La marque déposée Symbian appartient à Symbian Foundation Ltd.

INDEX