KASPERSKY lab

Kaspersky Security 10 for Mobile

Manuel d'implantation

Version de l'application : 10.0 Service Pack 1 Maintenance Release 3

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 aux questions que vous pourriez vous poser sur notre produit.

Ce document peut être modifié sans préavis. La dernière version de ce document est disponible sur le site de " Kaspersky Lab " à l'adresse http://www.kaspersky.com/fr/docs.

Date de rédaction du document : 18/11/2015

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

Contenu

A propos de ce document

Le Manuel d'implantation de la solution globale Kaspersky Security 10 for Mobile Service Pack 1 Maintenance Release 3 (plus loin "Kaspersky Security for Mobile") s'adresse aux spécialistes qui installent et administrent l'application. Il s'adresse également aux spécialistes qui fournissent un support technique aux organisations utilisant Kaspersky Security for Mobile.

Les informations reprises dans ce manuel peuvent être utiles dans l'exécution des tâches suivantes :

- planification de l'installation des modules de Kaspersky Security for Mobile (y compris principes de fonctionnement de l'application, configuration requise, schémas types de déploiement, particularités d'intégration de Kaspersky Security for Mobile avec d'autres applications) ;
- préparation de l'installation, installation et activation des applications mobiles Kaspersky Endpoint Security et Kaspersky Safe Browser ;
- configuration des applications mobiles Kaspersky Endpoint Security et Kaspersky Safe Browser après l'installation.

Ce manuel cite également les sources d'informations sur la solution globale et les méthodes d'obtention du support technique.

Dans cette section

Dans ce document

Ce document contient les sections suivantes.

Sources d'informations sur l'application (cf. page 9)

Cette section présente les différentes sources d'informations sur l'application.

Kaspersky Security for Mobile (cf. page 12)

Cette section décrit les fonctions et les modules de Kaspersky Security for Mobile.

Configuration matérielle et logicielle (cf. page 20)

Cette section contient la configuration matérielle et logicielle requise.

Architecture de la solution complète (cf. page 21)

Cette section décrit les modules de Kaspersky Security for Mobile et leurs interactions.

Schémas types de déploiement de la solution complète (cf. page 23)

Cette section décrit les schémas standard de déploiement de Kaspersky Security for Mobile sur le réseau de l'organisation.

Déploiement de la solution complète (cf. page 28)

Cette section décrit les processus de déploiement de Kaspersky Security for Mobile sur le réseau de l'organisation.

Installation du plug-in d'administration (cf. page 65)

Cette section décrit l'installation du plug-in d'administration de la solution complète Kaspersky Security for Mobile sur le poste de travail de l'administrateur.

Glossaire (cf. page 72)

Cette section contient une liste des termes qui apparaissent dans ce document et leur définition.

Kaspersky Lab AO (cf. page 72)

Cette section contient des informations sur Kaspersky Lab AO.

Information sur le code tiers (cf. page 79)

Cette section contient des informations sur le code tiers utilisé dans l'application.

Avis de marques déposées (cf. page 80)

Cette section énumère les marques des titulaires de droits tiers, utilisés dans le document.

Index (cf. page 81)

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

Conventions

Le présent document respecte des conventions (cf. tableau ci-dessous).

Tableau 1. Conventions

Exemple de texte	Description de la convention
Veuillez noter que...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent des informations sur les actions pouvant avoir des conséquences indésirables.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques contiennent des informations complémentaires ou d'aide.
Exemple :	Les exemples sont présentés sur un fond bleu sous le titre "Exemple".
La *mise à jour*, c'est... L'événement *Bases périmées* survient.	Les éléments de texte suivants sont en italique : • nouveaux termes; • noms des statuts et des événements de l'application.
Appuyez sur la touche **ENTER**. Appuyez en même temps sur les touches **ALT**+**F4**.	Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules. Des noms de touche unis par le caractère + (plus) représentent une combinaison de touches. Ces touches doivent être enfoncées simultanément.
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 et les boutons, sont en caractères mi-gras.

Exemple de texte	Description de la convention
► *Pour planifier une tâche, procédez comme suit :*	Les phrases de saisie des instructions sont en italique et présentent l'icône "flèche".
Dans la ligne de commande, saisissez le texte `help` Le message suivant s'affiche: `Indiquez la date au format JJ:MM:AA.`	Les types de texte suivants apparaissent dans un style spécial : • texte de la ligne de commande; • texte des messages affichés sur l'écran par l'application; • données à saisir à l'aide du clavier.
<Nom d'utilisateur>	Les variables sont écrites entre chevrons. A la place de la variable, il convient d'indiquer la valeur correspondante en enlevant les chevrons.

Sources d'informations sur l'application

Cette section présente les différentes sources d'informations sur l'application.

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

Dans cette section

Sources d'informations pour la recherche autonome

Vous pouvez utiliser les sources suivantes pour la recherche autonome d'informations à propos de Kaspersky Security Center :

- page Kaspersky Security for Mobile sur le site Internet de Kaspersky Lab ;
- page Kaspersky Security for Mobile sur le site Internet du Service de Support Technique (Base de connaissances) ;
- aide électronique ;
- documentation.

Si vous ne trouvez pas la réponse à votre question, il est recommandé de contacter le Support Technique de Kaspersky Lab.

Page Kaspersky Security for Mobile sur le site Internet de Kaspersky Lab

La page de Kaspersky Security for Mobile (http://www.kaspersky.fr/business-security/mobile#tab=frame-1) fournit des informations générales sur l'application, ses fonctionnalités et ses particularités de fonctionnement.

La page Kaspersky Security for Mobile contient un lien vers la boutique en ligne. Ce lien permet d'acheter l'application ou de prolonger le droit d'utilisation de l'application.

Page Kaspersky Security for Mobile dans la Base de connaissances

La *base de connaissances* est une rubrique du site du Support Technique.

La page de Kaspersky Security for Mobile dans la Base de connaissances (http://support.kaspersky.com/fr/ks10mob) permet de trouver des 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 de la Base de connaissances peuvent répondre à des questions en rapport non seulement avec Kaspersky Security for Mobile, mais également avec d'autres applications de Kaspersky Lab. Les articles de la base de connaissances peuvent également contenir des informations du Support technique.

Aide électronique

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

L'aide contextuelle pour le plug-in d'administration de Kaspersky Security for Mobile permet d'obtenir des informations sur les fenêtres de Kaspersky Security Center : description des paramètres de l'application et liens vers la description des tâches dans lesquelles ces paramètres sont utilisés.

L'aide complète des applications Kaspersky Endpoint Security et Kaspersky Safe Browser permet de trouver des informations sur la configuration et l'utilisation des applications mobiles.

Documentation

La distribution de la solution complète contient des documents grâce auxquels vous pouvez installer et activer les applications sur les périphériques mobiles d'entreprise des utilisateurs, configurer leurs paramètres d'utilisation, et obtenir des informations sur leur fonctionnement général.

Discussion sur les applications de Kaspersky Lab sur 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 ou créer une nouvelle discussion.

Kaspersky Security for Mobile

Kaspersky Security for Mobile est une solution complète dédiée à la protection et à l'administration des périphériques mobiles d'entreprise, ainsi que des périphériques personnels des employés utilisés dans un but professionnel. Kaspersky Security for Mobile contient les modules suivants :

- Paquet des applications mobiles pour les systèmes d'exploitation Android™, iOS et Windows Phone®.

  Les applications mobiles assurent la sécurité des appareils mobiles et des données qui s'y trouvent, et permettent de connecter ces appareils au Serveur d'administration de Kaspersky Security Center.

- Plug-in d'administration de Kaspersky Endpoint Security 10.0 Service Pack 1, Maintenance Release 3 (plus loin "plug-in d'administration de Kaspersky Endpoint Security").

  Le plug-in d'administration de Kaspersky Endpoint Security permet de connecter les appareils sur lesquels sont installées les applications mobiles Kaspersky Endpoint Security ou Kaspersky Safe Browser au Serveur d'administration de Kaspersky Security Center, et de configurer les paramètres de protection des appareils à l'aide de stratégies.

- Plug-in d'administration de Kaspersky Mobile Device Management 10.0 Service Pack 1, Maintenance Release 3 (plus loin "plug-in d'administration de Kaspersky Mobile Device Management").

  Le plug-in d'administration de Kaspersky Mobile Device Management permet de configurer les paramètres de configuration des périphériques connectés au serveur d'administration de Kaspersky Security Center selon le protocole iOS MDM et Exchange ActiveSync® sans passer par iPhone Configuration Utility ou par le profil d'administration Exchange ActiveSync.

Les plug-ins d'administration s'intègrent au *système d'administration à distance Kaspersky Security Center*. Grâce à la Console d'administration unique du Kaspersky Security Center, l'administrateur peut gérer l'ensemble des périphériques mobiles de l'entreprise, des ordinateurs clients et des systèmes virtuels. Les périphériques mobiles peuvent être administrés dès qu'ils ont été connectés au Serveur d'administration. L'administrateur peut commander à distance les périphériques administrés.

Dans cette section

A propos de Kaspersky Endpoint Security for Android

L'application mobile Kaspersky Endpoint Security for Android (plus loin "Kaspersky Endpoint Security") assure la protection des appareils mobiles équipés du système d'exploitation Android (plus loin "appareils Android") contre les virus et autres applications présentant une menace, les appels et SMS indésirables, ainsi que les menaces Internet.

Kaspersky Endpoint Security inclut les modules suivants :

- Anti-Virus. Ce module permet de détecter et de neutraliser les menaces sur l'appareil mobile à l'aide des bases antivirus de l'application et des services en nuage du Kaspersky Security Network. L'Anti-Virus présente les composants suivants :
  - Protection. La protection permet de découvrir les menaces dans les fichiers ouverts, d'analyser les nouvelles applications et de prévenir l'infection du périphérique en temps réel.
  - Vérification. L'analyse est lancée sur demande pour tout le système de fichiers, la mémoire vive ou un dossier. L'analyse complète permet de rechercher la présence éventuelle d'objets malveillants dans tout le système de fichiers du périphérique 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 et non ouverts, ainsi que les menaces dans les fichiers qui sont ouverts à ce moment-là. L'analyse de la mémoire permet de détecter les menaces uniquement dans les fichiers ouverts à ce moment-là.
  - Mise à jour. La mise à jour permet de télécharger les nouvelles bases antivirus de l'application.

- Antivol. Ce composant protège les informations du périphérique contre tout accès non autorisé en cas de perte ou de vol du périphérique. Le module permet de bloquer l'appareil, de le localiser ou de supprimer à distance les données qui s'y trouvent à l'aide de commandes.
- Filtre des appels et SMS. En fonction du mode de fonctionnement Filtre des appels et SMS sélectionné, celui-ci permet de bloquer les appels et SMS entrants non sollicités. Le filtrage des SMS et des appels entrants s'effectue à l'aide des listes de contacts autorisés et interdits. Filtre des appels et SMS permet de bloquer ou de transmettre les SMS et les appels entrants provenant des contacts interdits ou autorisés. Selon le mode sélectionné, Filtre des appels et SMS permet également de transmettre les appels et SMS entrants provenant de tous les numéros du répertoire du périphérique (Contacts) ou de bloquer les appels et SMS entrants de tous les numéros comportant des lettres.
- Protection Internet. Permet de bloquer les sites Internet malveillants dont le but est de diffuser un code nuisible. Ce Filtre des appels et SMS bloque également les sites Internet de phishing qui servent à voler des données confidentielles des utilisateurs (mots de passe des banques en lignes ou des systèmes de paiement, par exemple) pour obtenir un accès à leurs comptes bancaires. Filtre des appels et SMS analyse les sites Internet avant leur ouverture à l'aide du service en nuage du Kaspersky Security Network. Selon les résultats de l'analyse, la Protection Internet autorise le chargement des sites Internet identifiés comme fiables et bloque les sites Internet identifiés comme malveillants. La Protection Internet prend également en charge le filtrage des sites Internet par catégorie, selon les catégories définies dans le service dans le nuage du Kaspersky Security Network. Cela permet à l'administrateur de limiter l'accès des utilisateurs à certaines catégories (les pages Internet des catégories " Jeux de hasard, loteries, tirages au sort " ou " Médias de communication Internet ", par exemple).
- Synchronisation. Assure la connexion de l'appareil mobile au Serveur d'administration. La synchronisation offre la possibilité de configurer à distance les paramètres de l'application, et de l'appareil mobile à l'aide de stratégies de groupe définies dans la Console d'administration Kaspersky Security Center.
- Quarantaine. Place dans un stockage spécial et isolé les fichiers qui ont été détectés lors de l'analyse du périphérique ou au cours du fonctionnement normal de la protection. La quarantaine compacte les fichiers avant leur isolement afin de protéger votre appareil. Ce module " Quarantaine " permet de supprimer ou de restaurer les fichiers placés en quarantaine.
- Rapports. Permet de recevoir des informations sur le fonctionnement de l'Anti-Virus, du Filtre des appels et SMS et de la Protection Internet sur le périphérique mobile de l'utilisateur. Ce module regroupe les rapports dès leur création. Le rapport peut contenir jusqu'à 200 entrées sur les événements. Lorsque le nombre d'entrées dépasse 200, le module remplace les entrées les plus anciennes par les entrées les plus récentes.

A propos de Kaspersky Safe Browser for iOS

L'application mobile Kaspersky Safe Browser for iOS (plus loin "Kaspersky Safe Browser") est un navigateur Web sécurisé.

Kaspersky Safe Browser inclut les modules suivants :

- Protection Internet. Permet de bloquer les sites Internet malveillants dont le but est de diffuser un code nuisible. Ce Filtre des appels et SMS bloque également les sites Internet de phishing qui servent à voler des données confidentielles des utilisateurs (mots de passe des banques en lignes ou des systèmes de paiement, par exemple) pour obtenir un accès à leurs comptes bancaires. Filtre des appels et SMS analyse les sites Internet avant leur ouverture à l'aide du service en nuage du Kaspersky Security Network. Selon les résultats de l'analyse, la Protection Internet autorise le chargement des sites Internet identifiés comme fiables et bloque les sites Internet identifiés comme malveillants. La Protection Internet prend également en charge le filtrage des sites Internet par catégorie, selon les catégories définies dans le service dans le nuage du Kaspersky Security Network. Cela permet à l'administrateur de limiter l'accès des utilisateurs à certaines catégories (les pages Internet des catégories " Jeux de hasard, loteries, tirages au sort " ou " Médias de communication Internet ", par exemple).

- Antivol. A l'aide d'une commande, le module permet de localiser l'appareil mobile en cas de perte ou de vol.

- Synchronisation. Assure la connexion de l'appareil mobile au Serveur d'administration. La synchronisation offre la possibilité de configurer à distance les paramètres de l'application, et de l'appareil mobile à l'aide de stratégies de groupe définies dans la Console d'administration Kaspersky Security Center.

Pour en savoir plus sur Kaspersky Safe Browser for iOS, consultez le *Manuel de l'utilisateur de Kaspersky Safe Browser*.

A propos de Kaspersky Safe Browser for Windows Phone

L'application mobile Kaspersky Safe Browser for Windows Phone (plus loin "Kaspersky Safe Browser") est un navigateur Web sécurisé.

Kaspersky Safe Browser inclut les modules suivants :

- Protection Internet. Permet de bloquer les sites Internet malveillants dont le but est de diffuser un code nuisible. Ce Filtre des appels et SMS bloque également les sites Internet de phishing qui servent à voler des données confidentielles des utilisateurs (mots de passe des banques en lignes ou des systèmes de paiement, par exemple) pour obtenir un accès à leurs comptes bancaires. Filtre des appels et SMS analyse les sites Internet avant leur ouverture à l'aide du service en nuage du Kaspersky Security Network. Selon les résultats de l'analyse, la Protection Internet autorise le chargement des sites Internet identifiés comme fiables et bloque les sites Internet identifiés comme malveillants. La Protection Internet prend également en charge le filtrage des sites Internet par catégorie, selon les catégories définies dans le service dans le nuage du Kaspersky Security Network. Cela permet à l'administrateur de limiter l'accès des utilisateurs à certaines catégories (les pages Internet des catégories " Jeux de hasard, loteries, tirages au sort " ou " Médias de communication Internet ", par exemple).

- Antivol. A l'aide d'une commande, le module permet de localiser l'appareil mobile en cas de perte ou de vol.

- Synchronisation. Assure la connexion de l'appareil mobile au Serveur d'administration. La synchronisation offre la possibilité de configurer à distance les paramètres de l'application, et de l'appareil mobile à l'aide de stratégies de groupe définies dans la Console d'administration Kaspersky Security Center.

Pour en savoir plus sur Kaspersky Safe Browser for Windows Phone, consultez le *Manuel de l'utilisateur de Kaspersky Safe Browser*.

Présentation du plug-in d'administration de Kaspersky Endpoint Security

Le plug-in d'administration de Kaspersky Endpoint Security assure l'administration par interface des périphériques mobiles et de leurs applications via la Console d'administration du Kaspersky Security Center. Le plug-in d'administration de Kaspersky Endpoint Security vous permet d'exécuter les actions suivantes :

- créer une stratégie de sécurité de groupe pour les périphériques mobiles ;
- configurer à distance les applications de Kaspersky Endpoint Security sur les périphériques mobiles des utilisateurs ;
- créer des paquets d'installation et des paquets autonomes d'applications mobiles dans le Kaspersky Security Center ;
- recevoir les rapports et les statistiques concernant le fonctionnement des applications de Kaspersky Endpoint Security sur les appareils mobiles des utilisateurs.

Présentation du plug-in d'administration de Kaspersky Mobile Device Management

Le plug-in d'administration de Kaspersky Mobile Device Management constitue l'interface d'administration des appareils mobiles connectés via les protocoles iOS MDM et Exchange Active Sync sur la Console d'administration Kaspersky Security Center. Le plug-in d'administration de Kaspersky Mobile Device Management vous permet d'exécuter les actions suivantes :

- définir à distance les paramètres de configuration des périphériques connectés au Serveur des périphériques mobiles Exchange ActiveSync via le protocole Exchange ActiveSync (ci-après, les "périphériques EAS").
- définir à distance les paramètres de configuration des périphériques connectés au Serveur des périphériques mobiles iOS MDM via le protocole iOS MDM (ci-après, les "périphériques iOS MDM").
- recevoir les rapports et les statistiques concernant le fonctionnement des périphériques mobiles des utilisateurs.

Configurations logicielles et matérielles

Cette section contient les configurations matérielle et logicielle de l'ordinateur de l'administrateur utilisé pour le déploiement des applications sur les appareils mobiles, ainsi que la liste des systèmes d'exploitation d'appareils mobiles prenant en charge Kaspersky Security for Mobile.

Configuration matérielle et logicielle de l'ordinateur de l'administrateur

Pour pouvoir déployer la solution Kaspersky Security for Mobile, l'ordinateur de l'administrateur doit répondre à la configuration matérielle requise pour Kaspersky Security Center. Pour en savoir plus sur la configuration matérielle de Kaspersky Security Center, consultez le *Manuel de l'administrateur du Kaspersky Security Center*.

Pour le déploiement du plug-in d'administration de Kaspersky Endpoint Security, la Console d'administration Kaspersky Security Center 10.0 doit être installée sur l'ordinateur de l'administrateur.

Pour le déploiement du plug-in d'administration de Kaspersky Mobile Device Management, l'ordinateur de l'administrateur doit satisfaire aux prérequis logiciels suivants :

- Console d'administration Kaspersky Security Center 10 Service Pack 1 ;
- Serveur de gestion des périphériques mobiles Exchange ActiveSync ;
- Serveur de gestion des périphériques mobiles iOS MDM ;
- Ensemble d'instructions SSE2 ou d'une version plus récente.

Pour le déploiement de l'application mobile Kaspersky Endpoint Security for Android via le Serveur d'administration, l'ordinateur de l'administrateur doit répondre à la configuration logicielle suivante :

- Kaspersky Security Center 10.0 ;
- utilitaire Kaspersky SMS Broadcasting.

Pour le déploiement de l'application mobile Kaspersky Safe Browser for iOS via le Serveur des périphériques mobiles iOS MDM, l'ordinateur de l'administrateur doit répondre à la configuration logicielle suivante :

- Kaspersky Security Center 10.0 ;
- Serveur de gestion des périphériques mobiles iOS MDM.
- utilitaire Kaspersky SMS Broadcasting.

Pour le déploiement des applications mobiles Kaspersky Endpoint Security for Android, Kaspersky Safe Browser for iOS, Kaspersky Safe Browser for Windows Phone à partir des boutiques en ligne correspondantes, la configuration requise pour l'ordinateur de l'administrateur n'est pas précisée.

Configurations matérielle et logicielle requises sur l'appareil mobile de l'utilisateur pour Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android requiert les configurations matérielle et logicielle suivantes :

- smartphone ou tablette avec résolution d'écran de 320 x 480 pixels ;
- 65 Mo d'espace libre dans la mémoire principale de l'appareil ;
- système d'exploitation Android 4.0 à 6.0 ;
- architecture du processeur Intel® Atom™ x86, ARM5, ARM6 ou ARM7.

L'application ne peut être installée que dans la mémoire principale de l'appareil.

Pour l'utilisation des fonctions Filtre des appels et SMS et Surveillance SIM, une carte SIM doit être installée sur l'appareil.

Configurations matérielle et logicielle requises sur l'appareil mobile de l'utilisateur pour Kaspersky Safe Browser for iOS

Les configurations logicielles et matérielles suivantes sont requises pour Kaspersky Safe Browser for iOS :

- type d'appareil : iPhone 4 ou modèle plus récent, iPad 2 ou modèle plus récent ;
- 35 Mo d'espace libre dans la mémoire principale de l'appareil ;
- système d'exploitation iOS 7, iOS 8 et iOS 9 ;
- connexion à Internet ;
- accès à la géolocalisation et à l'appareil photo de l'appareil.

Configurations matérielle et logicielle requises sur l'appareil mobile de l'utilisateur pour Kaspersky Safe Browser for Windows Phone

Les configurations logicielles et matérielles suivantes sont requises pour Kaspersky Safe Browser for Windows Phone :

- type d'appareil : smartphone ou tablette ;
- résolution de l'écran de 320 x 480 pixels minimum ;
- 30 Mo d'espace libre dans la mémoire principale de l'appareil ;
- système d'exploitation Windows Phone 8.1 ou Windows 10 Mobile ;
- connexion à Internet ;
- accès à la géolocalisation de l'appareil.

Architecture de la solution complète

Kaspersky Security for Mobile comprend les modules suivants :

- Application mobile Kaspersky Endpoint Security for Android.

  Assure la protection des appareils mobiles équipés du système d'exploitation Android (plus loin "appareils Android"). Gère les interactions entre les appareils mobiles et le Serveur d'administration.

- Application mobile Kaspersky Safe Browser for iOS.

  Permet d'assurer un accès sécurisé à Internet pour les appareils mobiles équipés du système d'exploitation iOS (plus loin "appareils iOS"). Gère les interactions entre les appareils mobiles et le Serveur d'administration.

- Application mobile Kaspersky Safe Browser for Windows Phone.

  Permet d'assurer un accès sécurisé à Internet pour les appareils mobiles équipés du système d'exploitation Windows Phone (plus loin "appareils Windows Phone"). Gère les interactions entre les appareils mobiles et le Serveur d'administration.

- Plug-in d'administration de Kaspersky Endpoint Security.

  Constitue l'interface d'administration des appareils mobiles sur lesquels sont installées les applications mobiles Kaspersky Endpoint Security ou Kaspersky Safe Browser via la Console d'administration Kaspersky Security Center.

- Plug-in d'administration Kaspersky Mobile Device Management.

  Constitue l'interface d'administration des appareils mobiles prenant en charge les protocoles Exchange ActiveSync et iOS Mobile Device Management via la Console d'administration Kaspersky Security Center.

L'architecture de la solution complète Kaspersky Security for Mobile est représentée sur l'illustration ci-dessous.

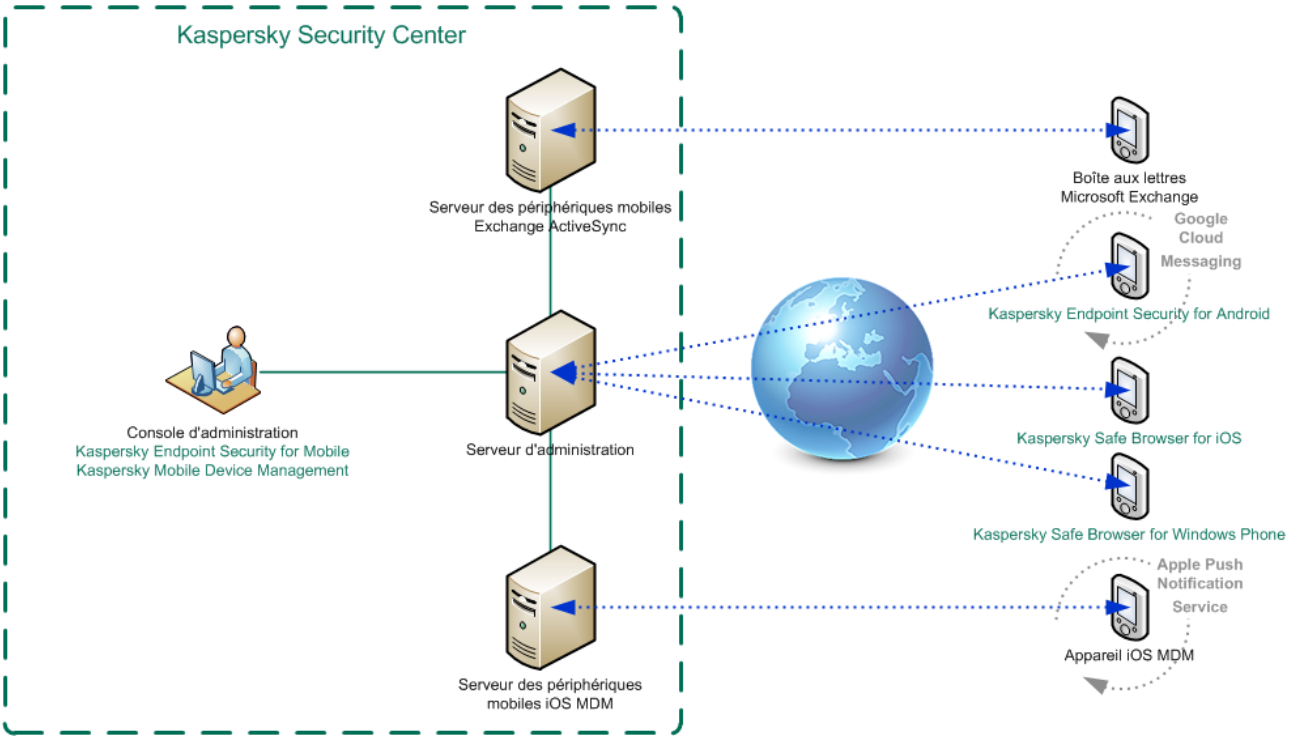

Illustration 1. Architecture de Kaspersky Security for Mobile

Pour en savoir plus sur la Console d'administration, le Serveur d'administration, le Serveur des périphériques mobiles Exchange ActiveSync et le Serveur des périphériques mobiles iOS MDM, consultez le *Manuel d'implantation de Kaspersky Security Center*.

Schémas types de déploiement de la solution complète

Cette section décrit les schémas types de déploiement de la solution complète Kaspersky Security for Mobile.

Le déploiement de la solution complète sur les appareils Android, iOS et Windows Phone s'effectue selon des schémas différents. Si l'organisation utilise des appareils mobiles équipés de différents systèmes d'exploitation, il faut installer l'application pour chaque système d'exploitation séparément, conformément au schéma de déploiement correspondant.

Dans cette section

Schéma de déploiement de Kaspersky Endpoint Security for Android

Il existe plusieurs moyens de déployer Kaspersky Endpoint Security sur les appareils Android du réseau de l'organisation. Vous pouvez sélectionner la méthode de déploiement qui convient le mieux à votre organisation, et utiliser plusieurs méthodes de déploiement simultanément.

Déploiement de Kaspersky Endpoint Security via l'envoi de messages SMS ou de messages électroniques

Le déploiement de Kaspersky Endpoint Security via l'envoi de messages implique les actions suivantes de l'administrateur :

1. Création du paquet d'installation de l'application.
2. Configuration du paquet d'installation.

3. Création d'un paquet autonome d'installation.

4. Envoi d'un message contenant un lien pour télécharger le paquet autonome d'installation aux utilisateurs d'appareils Android.

L'installation de Kaspersky Endpoint Security sur l'appareil mobile est effectuée par l'utilisateur une fois qu'il a reçu le message contenant le lien permettant de télécharger le fichier de distribution sur le serveur Web de Kaspersky Security Center. Aucune autre préparation de l'application n'est nécessaire à son fonctionnement.

Déploiement de Kaspersky Endpoint Security via une station de travail

Le déploiement de Kaspersky Endpoint Security via une station de travail implique les actions suivantes de l'administrateur :

1. Création du paquet d'installation de l'application.

2. Configuration du paquet d'installation.

3. Création de la tâche d'installation à distance.

L'installation de Kaspersky Endpoint Security s'effectue automatiquement lors de la connexion de l'appareil mobile de l'utilisateur à la station de travail. Aucune autre préparation de l'application n'est nécessaire à son fonctionnement.

Déploiement de Kaspersky Endpoint Security via Self Service Portal

Self Service Portal est un portail Web qui permet à l'administrateur de transférer aux utilisateurs une partie des opérations d'administration de leurs appareils mobiles. Pour en savoir plus sur Self Service Portal, consultez le *Manuel d'implantation de Kaspersky Security Center* et le *Manuel de l'administrateur de Kaspersky Security Center*.

L'utilisateur installe lui-même Kaspersky Endpoint Security sur son appareil mobile. Lors de l'ajout de son appareil mobile au Self Service Portal, l'utilisateur télécharge le fichier de distribution de l'application mobile et l'installe. Aucune autre préparation de l'application n'est nécessaire à son fonctionnement. Pour installer l'application via Self Service Portal, l'utilisateur doit être autorisé à utiliser le portail.

Déploiement de Kaspersky Endpoint Security à partir de Google Play

Les utilisateurs installent eux-mêmes Kaspersky Endpoint Security sur leur appareil mobile. L'utilisateur télécharge le fichier de distribution de l'application mobile sur Google Play et l'installe sur son appareil. Après l'installation de l'application sur l'appareil mobile, il faut la préparer pour qu'elle puisse fonctionner : il est nécessaire de configurer les paramètres de connexion au Serveur d'administration et d'installer un certificat commun.

Cette option de déploiement est recommandée lorsqu'il est impossible d'effectuer une installation à distance.

Schéma de déploiement de Kaspersky Safe Browser for iOS

Il existe plusieurs moyens de déployer Kaspersky Endpoint Security sur les appareils iOS du réseau de l'organisation. Vous pouvez sélectionner la méthode de déploiement qui convient le mieux à votre organisation, et utiliser plusieurs méthodes de déploiement simultanément.

Déploiement de Kaspersky Safe Browser via le Serveur des périphériques mobiles iOS MDM

L'installation de Kaspersky Safe Browser sur les appareils mobiles des utilisateurs s'effectue automatiquement via Kaspersky Security Center. Après l'installation de l'application sur l'appareil mobile, il faut la préparer pour qu'elle puisse fonctionner : il est nécessaire de configurer les paramètres de connexion au Serveur d'administration et d'installer un certificat commun. Pour que Kaspersky Safe Browser puisse être installé, les appareils mobiles doivent être connectés au Serveur des périphériques mobiles iOS MDM.

Le déploiement de Kaspersky Safe Browser via le Serveur des périphériques mobiles iOS MDM implique les actions suivantes de l'administrateur :

1. Ajout de l'application sur le Serveur des périphériques mobiles iOS MDM.
2. Installation de Kaspersky Safe Browser sur l'appareil mobile.

Le schéma de déploiement de Kaspersky Safe Browser sur appareil mobile est représenté sur l'illustration ci-dessous.

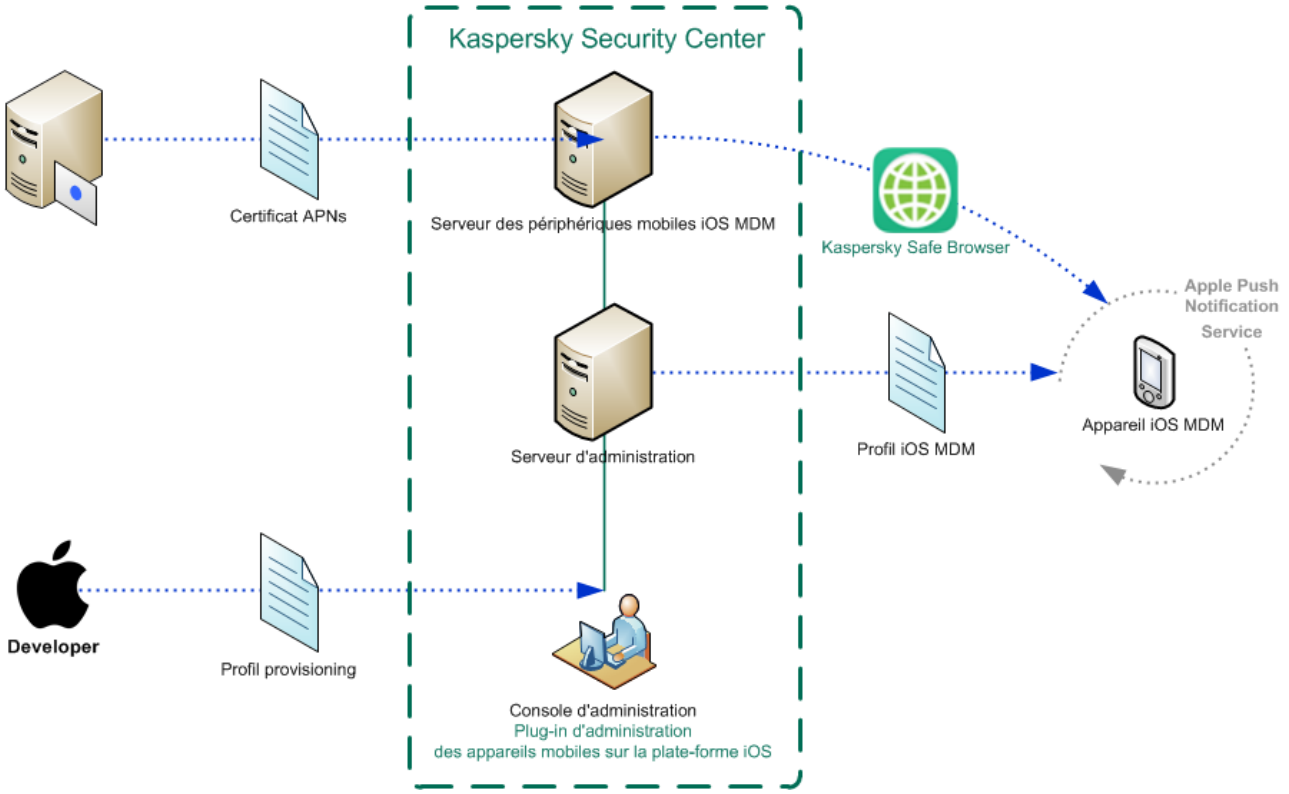

Illustration 2. Schéma de déploiement de Kaspersky Safe Browser for iOS via le Serveur des périphériques mobiles iOS MDM

Déploiement de Kaspersky Safe Browser à partir de l'App Store

Les utilisateurs installent eux-mêmes Kaspersky Safe Browser sur leur appareil mobile. L'utilisateur télécharge le fichier de distribution de l'application mobile sur l'App Store et l'installe sur son appareil. Après l'installation de l'application sur l'appareil mobile, il faut la préparer pour qu'elle puisse fonctionner : il est nécessaire de configurer les paramètres de connexion au Serveur d'administration et d'installer un certificat commun.

Cette option de déploiement est recommandée lorsqu'il est impossible d'effectuer une installation à distance.

Schéma de déploiement de Kaspersky Safe Browser for Windows Phone

Les utilisateurs installent eux-mêmes Kaspersky Safe Browser sur leur appareil mobile. L'utilisateur télécharge le fichier de distribution de l'application mobile sur la boutique Windows Phone et l'installe sur son appareil. Après l'installation de l'application sur l'appareil mobile, il faut la préparer pour qu'elle puisse fonctionner : il est nécessaire de configurer les paramètres de connexion au Serveur d'administration et d'installer un certificat commun.

Déploiement de la solution complète

Cette section décrit les processus de déploiement de Kaspersky Security for Mobile sur le réseau de l'organisation.

Dans cette section

Préparation de la Console d'administration au déploiement de la solution complète

Cette section contient des instructions concernant la préparation de la Console d'administration au déploiement de la solution complète.

Dans cette section

Configuration du Serveur d'administration pour la connexion des périphériques mobiles

Pour que les appareils mobiles puissent se connecter au Serveur d'administration, il est nécessaire de configurer les paramètres de connexion des appareils mobiles dans les propriétés du Serveur d'administration, avant l'installation des applications mobiles Kaspersky Endpoint Security et Kaspersky Safe Browser.

► *Pour configurer les paramètres du Serveur d'administration pour la connexion des appareils mobiles, procédez comme suit :*

1. Dans le menu contextuel Serveur d'administration, choisissez l'option **Propriétés**.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sélectionnez la section **Paramètres**.

3. Dans le groupe **Paramètres de connexion au Serveur d'administration**, cochez la case **Ouvrir le port pour les périphériques mobiles**.

4. Dans le champ **Port pour les périphériques mobiles**, spécifiez le port que les périphériques mobiles utiliseront pour se connecter au Serveur d'administration.

   Le numéro de port par défaut est 13292. Si la case **Ouvrir le port pour les périphériques mobiles** est décochée ou qu'un port invalide a été indiqué pour la connexion, les périphériques mobiles ne pourront pas se connecter au Serveur d'administration.

5. Cliquez sur le bouton **OK**.

Affichage du dossier Gestion des appareils mobiles dans la Console d'administration

L'affichage du dossier **Gestion des appareils mobiles** dans la Console d'administration permet de consulter la liste des périphériques mobiles gérés par le Serveur d'administration, de définir les paramètres d'administration des appareils mobiles et d'installer les certificats sur les appareils mobiles des utilisateurs.

► *Pour activer l'affichage du dossier **Gestion des appareils mobiles** dans la Console d'administration, procédez comme suit :*

1. Dans le menu contextuel du Serveur d'administration sélectionnez l'option **Affichage** → **Configuration de l'interface**.

2. Dans la fenêtre qui s'ouvre, cochez la case **Afficher la gestion des appareils mobiles**.

3. Cliquez sur le bouton **OK**.

Le dossier **Gestion des appareils mobiles** s'affichera dans l'arborescence de la Console d'administration après son redémarrage.

Création d'un groupe d'administration

La configuration centralisée des paramètres des applications Kaspersky Endpoint Security et Kaspersky Safe Browser installés sur les périphériques mobiles des 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 un groupe d'administration dédié à ces appareils dans le dossier **Ordinateurs administrés** avant l'installation des applications mobiles sur les périphériques des utilisateurs.

Après la création du groupe d'administration, il est recommandé de configurer le déplacement automatique vers le groupe de périphériques où vous souhaitez installer les applications (cf. section "Création des règles du transfert automatique des périphériques dans le groupe d'administration" à la page 31) . Il faut ensuite définir les paramètres communs à l'ensemble des périphériques à l'aide d'une stratégie de groupe. Pour en savoir plus sur la configuration des paramètres à l'aide des stratégies de groupe, consultez le*Manuel de l'administrateur de Kaspersky Security for Mobile*.

► *Pour créer un groupe d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Ordinateurs administrés**.

2. Dans l'espace de travail du dossier **Ordinateurs administrés** ou dans un sous-dossier, sélectionnez l'onglet **Groupes**.

3. En cliquant sur le lien **Créer un sous-groupe**, ouvrez la fenêtre de création d'un nouveau groupe.

4. Dans la fenêtre **Nom du groupe** qui s'ouvre, saisissez le nom du 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.

Pour plus d'informations sur l'utilisation des groupes d'administration, cf. *Manuel d'administrateur de Kaspersky Security Center*.

Création des règles du transfert automatique des périphériques dans le groupe d'administration

L'administration centralisée des paramètres des applications Kaspersky Endpoint Security et Kaspersky Safe Browser installées sur des périphériques mobiles n'est possible que si ces périphériques se trouvent dans un groupe d'administration déjà existant, et pour lequel une stratégie de groupe a été définie (cf. section "Création d'un groupe d'administration" à la page 30).

Si la règle du déplacement automatique des périphériques mobiles détectés dans le réseau vers le groupe d'administration n'a pas été définie, à la première synchronisation du périphérique au Serveur d'administration, cet appareil sera automatiquement transféré vers le sous-dossier **KSM10** du dossier **Domaines** qui se trouve dans le dossier **Périphériques non définis** de la Console d'administration. La stratégie de groupe n'est pas appliquée à cet appareil.

► *Pour créer une règle de transfert automatique des périphériques mobiles vers le groupe d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Périphériques non définis**.

2. Dans le menu contextuel du dossier **Périphériques non définis**, choisissez l'option **Propriétés**.

   La fenêtre **Propriétés : Périphériques non définis** s'ouvre.

3. Dans la section **Déplacement d'ordinateurs**, cliquez sur le bouton **Ajouter** pour lancer la procédure de création des règles de déplacement automatique des périphériques vers le groupe d'administration.

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

4. Ouvrez la section **Général**, et effectuez les actions suivantes :

   a. Spécifiez le nom de la règle.

   b. Indiquez le groupe d'administration vers lequel seront déplacés les périphériques mobiles une fois que l'application mobile Kaspersky Endpoint Security ou Kaspersky Safe Browser y aura été installée. 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.

   c. Dans le groupe **Exécution de la règle**, sélectionnez l'option **Appliquer une fois pour chacun des ordinateurs**.

   d. Cochez la case **Déplacer uniquement les ordinateurs qui n'appartiennent pas aux groupes d'administration** pour que les périphériques mobiles déjà répartis dans d'autres groupes d'administration ne soient pas déplacés vers le groupe sélectionné lors de l'application de cette règle.

   e. Cochez la case **Activer la règle** pour appliquer cette règle aux appareils nouvellement détectés.

5. Ouvrez la section **Applications**, et effectuez les actions suivantes :

   a. Cochez la case **Version du système d'exploitation**.

   b. Sélectionnez un ou plusieurs types de systèmes d'exploitation qui seront déplacés vers le groupe indiqué : Android, iOS, ou Windows Phone.

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

La règle créée s'affiche dans la liste des règles de transfert des périphériques dans la section **Déplacement d'ordinateurs** de la fenêtre des propriétés du dossier **Périphériques non définis**.

Grâce à cette règle, Kaspersky Security Center transfère tous les périphériques conformes aux critères définis depuis le dossier **Périphériques non définis** vers le groupe d'administration que vous avez indiqué. Les périphériques mobiles déjà répartis dans le dossier **Périphériques non définis** peuvent être déplacés manuellement vers le groupe d'administration requis du dossier **Ordinateurs administrés**. Pour plus d'informations sur la gestion des groupes d'administration et l'utilisation des périphériques non repartis, cf. *Manuel d'administrateur de Kaspersky Security Center*.

Création d'un certificat commun

Afin d'identifier l'utilisateur d'un appareil mobile, il faut créer un certificat commun dans la Console d'administration.

► *Pour créer un certificat commun, procédez comme suit :*

1. Dans l'arborescence de la console, dans le dossier **Gestion des appareils mobiles**, sélectionnez le sous-dossier **Certificats**.

2. Dans la zone de travail du dossier **Certificats**, cliquez sur le lien **Ajouter un certificat** pour lancer l'assistant d'installation de certificats.

3. Dans la fenêtre **Sélection de l'utilisateur** de l'assistant, indiquez les utilisateurs pour lesquels vous souhaitez créer un certificat commun.

4. Dans la fenêtre **Type de certificat** de l'assistant, sélectionnez l'option **Certificat commun**.

5. Dans la fenêtre **Source du certificat** de l'assistant, indiquez le mode de création du certificat commun.

   - Pour créer un certificat commun automatiquement à l'aide des outils du Serveur d'administration, sélectionnez l'option **Créer le certificat à l'aide des outils du Serveur d'administration**.
   - Pour indiquer à l'utilisateur le certificat créé précédemment, sélectionnez l'option **Indiquer le fichier du certificat**. Cliquez sur le bouton **Indiquer** pour ouvrir la fenêtre **Certificat** et y indiquer le fichier du certificat.
     Décochez la case **Publier le certificat** si vous ne souhaitez pas indiquer le type d'appareil mobile et le mode de notification de l'utilisateur concernant la création du certificat.

6. Dans la fenêtre **Type d'appareil** de l'assistant, sélectionnez le type d'appareil mobile de l'utilisateur pour lequel vous souhaitez établir un certificat commun :

   - Pour ajouter un certificat au profil iOS MDM, sélectionnez l'option **Dans le profil iOS MDM**.

     L'ajout d'un certificat au profil iOS MDM n'est disponible que pour les appareils iOS MDM.

     À l'étape suivante de l'Assistant d'installation du certificat, vous devez sélectionner Serveur des périphériques mobiles iOS MDM.

   - Pour ajouter un certificat au paquet d'installation, sélectionnez l'option **Dans le paquet de l'application mobile**.

     L'ajout d'un certificat au paquet d'installation n'est accessible que pour l'application Kaspersky Endpoint Security for Android.

     À l'étape suivante de l'Assistant d'installation du certificat, vous devez sélectionner le paquet d'installation pour installer Kaspersky Endpoint Security for Android.

   - Afin de créer un certificat pour l'utilisation sur un appareil mobile sur lequel l'application Kaspersky Endpoint Security ou Kaspersky Safe Browser est déjà installée, sélectionnez l'option **Pour utilisation par une application mobile installée**.

7. Dans la fenêtre **Mode de notification des utilisateurs** de l'assistant, configurez les paramètres de la notification, par SMS ou courrier électronique, de l'utilisateur d'un périphérique mobile à propos de la création du certificat.

8. Dans la fenêtre **Informations sur le certificat** de l'assistant, cliquez sur le bouton **Terminer** pour fermer l'assistant d'installation de certificats.

Au terme de l'exécution de l'assistant d'installation de certificats, un certificat commun sera créé et pourra être installé par un utilisateur sur un périphérique mobile. Afin d'obtenir un certificat, il est nécessaire de lancer la synchronisation du périphérique mobile avec le Serveur d'administration.

Kaspersky Endpoint Security for Android

Cette section contient des informations concernant l'utilisation de Kaspersky Endpoint Security sur le système d'exploitation Android : instructions d'installation, préparation de l'application, activation et suppression de l'application.

Dans cette section

Mise à jour d'une version précédente de l'application

C'est l'utilisateur de l'appareil mobile qui met à jour Kaspersky Endpoint Security à l'aide de Google Play. La mise à jour s'effectue selon la méthode classique pour la plate-forme Android. L'utilisateur utilise son propre compte Google™ pour la mise à jour de l'application.

Installation via l'envoi de messages

Cette section contient des instructions sur la préparation à l'installation et l'installation de l'application sur les appareils mobiles des utilisateurs via l'envoi de messages (messages SMS ou messages électroniques).

L'installation de Kaspersky Endpoint Security via l'envoi de messages comprend les étapes suivantes :

1. Création du paquet d'installation.

   Un *Paquet d'installation* est un ensemble de fichiers qui assure l'installation à distance de l'application de Kaspersky Lab via Kaspersky Security Center.

2. Configuration du paquet d'installation.

3. Création d'un paquet autonome d'installation.

   Un *paquet autonome d'installation* est un fichier d'installation de l'application mobile contenant les paramètres de connexion de l'application au Serveur d'administration. Il est créé à partir du paquet d'installation pour Kaspersky Endpoint Security. Le paquet autonome d'installation constitue un cas particulier de paquet d'applications mobiles.

4. Configuration de l'envoi de messages : messages SMS ou messages électroniques.

5. Envoi de messages contenant un lien pour télécharger le paquet autonome d'installation aux appareils mobiles des utilisateurs.

Dans cette section

Création du paquet d'installation

Le paquet d'installation de Kaspersky Endpoint Security se présente sous la forme d'une archive auto-extractible ak_package.exe. L'archive contient les fichiers nécessaires à l'installation de l'application mobile sur l'appareil :

- adb.exe, AdbWinApi.dll, AdbWinUsbApi.dll : fichiers nécessaires à l'installation de l'application mobile Kaspersky Endpoint Security for Android ;
- installer.ini – fichier de configuration contenant les paramètres de connexion au Serveur d'administration ;
- KSM_10_5_11_xxx_fr.apk : fichier d'installation de l'application mobile Kaspersky Endpoint Security for Android ;
- kmlisten.exe : utilitaire de distribution du paquet d'installation sur un périphérique mobile via une station de travail ;
- kmlisten.ini – fichier de configuration contenant les paramètres pour l'utilitaire de distribution du paquet d'installation ;
- kmlisten.kpd – fichier contenant la description de l'application.

► *Pour créer le paquet d'installation de Kaspersky Endpoint Security, procédez comme suit :*

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.
2. Dans le menu contextuel du dossier **Paquets d'installation**, sélectionnez **Créer** → **Paquet d'installation**.

   L'Assistant de création du paquet d'installation se lance. Il faut suivre ses indications.
3. Dans la fenêtre de l'assistant, **Sélectionnez le type de paquet d'installation**, appuyez sur le bouton **Créer le paquet d'installation pour l'application Kaspersky Lab**.
4. Dans la fenêtre **Sélection de la distribution de l'application à installer**, sélectionnez l'archive auto-extractible ak_package.exe incluse dans la distribution.

   Si l'archive a été décompressée auparavant, vous pouvez sélectionner un fichier faisant partie de l'archive avec la description de l'application kmlisten.kpd. Le nom de l'application ainsi que le numéro de la version vont apparaitre dans le champ de saisie.

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

Configuration du paquet d'installation

► *Pour configurer les paramètres du paquet d'installation, procédez comme suit :*

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.

2. Dans le menu contextuel du paquet d'installation de l'application Kaspersky Endpoint Security, sélectionnez **Propriétés**.

3. Sous l'onglet **Paramètres**, indiquez les paramètres de connexion des périphériques mobiles au Serveur d'administration et le nom du groupe d'administration où les périphériques mobiles seront automatiquement ajoutés après la première synchronisation avec le Serveur d'administration. Pour ce faire, procédez comme suit :

   - Dans le bloc **Connexion au Serveur d'administration**, dans le champ **Adresse du serveur** saisissez le nom du Serveur d'administration pour connecter les périphériques mobiles dans le format qui a été spécifié lors de l'installation du composant **Prise en charge des périphériques mobiles** pendant le déploiement du Serveur d'administration.

     Selon le format du nom du Serveur d'administration pour le module **Prise en charge des périphériques mobiles,** indiquez le nom DNS ou l'adresse IP 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 groupe **Répartition des ordinateurs selon les groupes** dans le champ **Nom du groupe**, saisissez le nom du groupe où les appareils mobiles seront ajoutés après la première synchronisation avec le Serveur d'administration (par défaut **KSM10**).

     Le groupe sélectionné sera automatiquement créé dans le dossier **Ordinateurs non répartis**.

- Dans le bloc **Actions lors de l'installation** cochez la case **Demander l'adresse email** pour que, lors du premier lancement, l'application demande à l'utilisateur son adresse de messagerie d'entreprise.

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

4. Pour appliquer les paramètres sélectionnés, appuyez sur le bouton **Appliquer**.

Création d'un paquet autonome d'installation

► *Pour créer un paquet autonome d'installation, procédez comme suit:*

1. Dans l'arborescence de la console, dans le champ **Installation à distance**, spécifiez le sous-dossier **Paquets d'installation**.
2. Spécifiez le paquet d'installation pour l'application Kaspersky Endpoint Security.
3. Dans le menu contextuel du paquet d'installation, choisissez **Créer un paquet autonome d'installation**.

   L'Assistant de création du paquet autonome d'installation se lance. Il faut suivre ses indications.

4. Dans la fenêtre **Choix du paquet d'installation de l'Agent d'administration pour une installation en parallèle** de l'Assistant, décochez la case **Installer l'Agent d'administration avec cette application**.

   La fenêtre **Résultat de la composition du paquet d'installation autonome** de l'Assistant affiche le chemin vers le dossier partagé comportant le paquet d'installation autonome créé. Il est possible d'ouvrir le dossier partagé en cliquant sur le lien **Ouvrir le dossier** dans la section **Actions suivantes**.

5. Configurez les méthodes de diffusion du paquet autonome :

   - Pour diffuser le chemin vers le paquet autonome d'installation aux utilisateurs par le biais d'un email : dans le groupe **Actions suivantes**, cliquez sur le lien **Envoyer le lien vers le paquet autonome d'installation par message électronique**.

Une fenêtre s'ouvre pour la rédaction d'un message dont le texte comprend le chemin vers le dossier partagé qui contient le paquet autonome d'installation.

- Pour publier le lien vers le paquet autonome d'installation créé sur le site Internet de votre entreprise, cliquez sur le lien **Exemple de code HTML pour la publication du lien sur le site Internet**.

  Le fichier .tmp contenant le lien HTML_RJL s'ouvre.

- Pour publier le paquet autonome d'installation créé sur le serveur Internet du Kaspersky Security Center et consulter toute la liste des paquets autonomes pour le paquet d'installation sélectionné, cochez la case **Ouvrir la liste des paquets autonomes** dans la fenêtre de l'Assistant **L'Assistant de création du paquet autonome d'installation s'est terminé avec succès**.

Une fois le travail de l'Assistant terminé, la fenêtre **Liste des paquets autonomes pour le paquet d'installation <Nom du paquet d'installation>** s'ouvre.

La fenêtre **Liste des paquets autonomes pour le paquet d'installation <Nom du paquet d'installation>** s'ouvre. Elle comporte les informations suivantes :

- liste des paquets autonomes d'installation ;
- chemin réseau vers le dossier partagé dans le champ **Chemin d'accès** ;
- adresse du paquet autonome sur le serveur Internet du Kaspersky Security Center, dans le champ **URL**.

Lors de l'envoi d'un message électronique, vous pouvez indiquer l'adresse du champ **URL** ou l'adresse du champ **Chemin** en tant que ressource que les utilisateurs peuvent exploiter pour le téléchargement du fichier d'installation de l'application. Lors de l'envoi de SMS, vous devez indiquer le lien du champ **URL** pour le téléchargement.

> Il est recommandé de copier l'adresse du paquet autonome préparé dans le presse-papiers pour ajouter ensuite le lien destiné au téléchargement du fichier d'installation souhaité dans le message électronique ou le SMS adressé aux utilisateurs.

Configuration de l'envoi de messages

► *Pour configurer l'envoi de messages, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Rapports et notifications**.
2. Sélectionnez **Propriétés** dans le menu contextuel du dossier.

   La fenêtre **Propriétés : comptes et notifications**.
3. Sélectionnez la section **Notification**.
4. Dans l'onglet **E-mail**, configurez l'envoi de messages électroniques :

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

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

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

1. Dans l'onglet **SMS**, configurez l'envoi de messages SMS :

   - Pour envoyer des SMS via la passerelle de messagerie, sélectionnez l'option **Envoyer les SMS via la passerelle de messagerie** et indiquez les paramètres du serveur SMTP.
   - Pour envoyer des messages SMS à l'aide de l'utilitaire Kaspersky SMS Broadcasting, sélectionnez l'option **Envoyer les SMS à l'aide de l'utilitaire Kaspersky SMS Broadcasting** et configurez les paramètres d'envoi.

     Pour en savoir plus sur l'utilisation de l'utilitaire Kaspersky SMS Broadcasting, consultez le *Manuel d'implantation de Kaspersky Security Center*.
2. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

Envoi de messages contenant le paquet autonome d'installation

► *Pour envoyer un message aux utilisateurs avec le lien vers le paquet autonome d'installation de Kaspersky Endpoint Security, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Comptes utilisateurs**.
2. Dans l'espace de travail du dossier, sélectionnez un ou plusieurs utilisateurs.

   Assurez-vous que les comptes des utilisateurs contiennent les coordonnées (adresse email et numéro de téléphone). En l'absence de coordonnées, ajoutez-les dans la fenêtre des propriétés du compte dans la section **Contacts**.

3. Dans le menu contextuel du compte utilisateur, sélectionnez la méthode d'envoi des messages :
   - **Envoyer par message électronique** ;
   - **Envoyer un message SMS**.
4. Dans la fenêtre qui s'ouvre, rédigez le texte du message destiné à l'utilisateur et ajoutez le lien vers le paquet autonome d'installation qui se trouve sur le serveur Internet du Kaspersky Security Center.

   Si vous envoyez des messages électroniques, vous pouvez indiquer le chemin d'accès au paquet autonome d'installation dans le dossier partagé.
5. Cliquez sur le bouton **OK** pour commencer l'envoi des messages.

Après avoir reçu un message contenant le lien vers le paquet autonome d'installation, l'utilisateur peut télécharger le fichier de distribution de Kaspersky Endpoint Security sur son appareil par les moyens à sa disposition.

A l'issue du téléchargement, l'utilisateur ouvre le fichier d'installation sur le périphérique. L'Assistant d'installation de l'application mobile se lance automatiquement. L'utilisateur doit suivre les indications de l'assistant de l'installation.

Afin d'installer Kaspersky Endpoint Security à l'aide de la distribution, l'installation d'applications provenant d'une autre source que Google Play doit être autorisée sur l'appareil mobile de l'utilisateur.

Installation via le poste de travail

Cette section contient des instructions sur la préparation à l'installation et l'installation de l'application sur les appareils mobiles des utilisateurs via le poste de travail.

L'installation de Kaspersky Endpoint Security via le poste de travail comprend les étapes suivantes :

1. Création du paquet d'installation.

   Un *Paquet d'installation* est un ensemble de fichiers qui assure l'installation à distance de l'application de Kaspersky Lab via Kaspersky Security Center.

2. Configuration du paquet d'installation.

3. Création de la tâche d'installation à distance de l'application.

4. Connexion de l'appareil mobile à la station de travail via USB.

Dans cette section

Création du paquet d'installation

Le paquet d'installation de Kaspersky Endpoint Security se présente sous la forme d'une archive auto-extractible ak_package.exe. L'archive contient les fichiers nécessaires à l'installation de l'application mobile sur l'appareil :

- adb.exe, AdbWinApi.dll, AdbWinUsbApi.dll : fichiers nécessaires à l'installation de l'application mobile Kaspersky Endpoint Security for Android ;

- installer.ini – fichier de configuration contenant les paramètres de connexion au Serveur d'administration ;
- KSM_10_5_11_xxx_fr.apk : fichier d'installation de l'application mobile Kaspersky Endpoint Security for Android ;
- kmlisten.exe : utilitaire de distribution du paquet d'installation sur un périphérique mobile via une station de travail ;
- kmlisten.ini – fichier de configuration contenant les paramètres pour l'utilitaire de distribution du paquet d'installation ;
- kmlisten.kpd – fichier contenant la description de l'application.

► *Pour créer le paquet d'installation de Kaspersky Endpoint Security, procédez comme suit :*

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.
2. Dans le menu contextuel du dossier **Paquets d'installation**, sélectionnez **Créer** → **Paquet d'installation**.

   L'Assistant de création du paquet d'installation se lance. Il faut suivre ses indications.
3. Dans la fenêtre de l'assistant, **Sélectionnez le type de paquet d'installation**, appuyez sur le bouton **Créer le paquet d'installation pour l'application Kaspersky Lab**.
4. Dans la fenêtre **Sélection de la distribution de l'application à installer**, sélectionnez l'archive auto-extractible ak_package.exe incluse dans la distribution.

   Si l'archive a été décompressée auparavant, vous pouvez sélectionner un fichier faisant partie de l'archive avec la description de l'application kmlisten.kpd. Le nom de l'application ainsi que le numéro de la version vont apparaitre dans le champ de saisie.

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

Configuration du paquet d'installation

► *Pour configurer les paramètres du paquet d'installation, procédez comme suit :*

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.
2. Dans le menu contextuel du paquet d'installation de l'application Kaspersky Endpoint Security, sélectionnez **Propriétés**.
3. Sous l'onglet **Paramètres**, indiquez les paramètres de connexion des périphériques mobiles au Serveur d'administration et le nom du groupe d'administration où les périphériques mobiles seront automatiquement ajoutés après la première synchronisation avec le Serveur d'administration. Pour ce faire, procédez comme suit :
   - Dans le bloc **Connexion au Serveur d'administration**, dans le champ **Adresse du serveur** saisissez le nom du Serveur d'administration pour connecter les périphériques mobiles dans le format qui a été spécifié lors de l'installation du composant **Prise en charge des périphériques mobiles** pendant le déploiement du Serveur d'administration.

     Selon le format du nom du Serveur d'administration pour le module **Prise en charge des périphériques mobiles,** indiquez le nom DNS ou l'adresse IP 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 groupe **Répartition des ordinateurs selon les groupes** dans le champ **Nom du groupe**, saisissez le nom du groupe où les appareils mobiles seront ajoutés après la première synchronisation avec le Serveur d'administration (par défaut **KSM10**).

     Le groupe sélectionné sera automatiquement créé dans le dossier **Ordinateurs non répartis**.

- Dans le bloc **Actions lors de l'installation** cochez la case **Demander l'adresse email** pour que, lors du premier lancement, l'application demande à l'utilisateur son adresse de messagerie d'entreprise.

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

4. Pour appliquer les paramètres sélectionnés, appuyez sur le bouton **Appliquer**.

Création de la tâche d'installation à distance

Il est nécessaire de créer la tâche d'installation à distance pour l'installation à distance de l'application à l'aide de Kaspersky Security Center. La tâche d'installation à distance créée sera lancée conformément à sa programmation.

Pour plus de renseignements sur l'installation à distance, cf. *Manuel de la mise en œuvre Kaspersky Security Center*.

► *Pour créer la tâche d'installation à distance de l'application pour les postes de travail, procédez comme suit :*

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, cliquez sur le lien **Lancer l'Assistant d'installation à distance** pour lancer l'Assistant d'installation à distance.
2. Dans la fenêtre **Sélection du paquet d'installation pour l'installation de l'application** de l'assistant, indiquez le paquet d'installation pour l'application Kaspersky Endpoint Security.
3. Dans la fenêtre de l'Assistant **Sélection des ordinateurs pour l'installation**, sélectionnez les postes de travail pour lesquels une tâche doit être créée :

   - Cliquez sur le bouton **Sélectionner les ordinateurs pour l'installation** afin de créer une tâche pour les ordinateurs non définis, pour plusieurs ordinateurs appartenant à un groupe d'administration, ou pour un ensemble d'ordinateurs appartenant à différents groupes d'administration.

     Cliquez sur le bouton **Installation sur le groupe des ordinateurs administrés** afin de créer une tâche pour tous les ordinateurs appartenant à un groupe d'administration.

     Suivez les indications de l'assistant.

A l'issue de la tâche d'installation à distance sur les postes de travail des utilisateurs, le paquet d'installation comprenant la distribution de l'application mobile Kaspersky Endpoint Security for Android est téléchargé. De même, l'utilitaire kmlisten.exe de téléchargement de la distribution de l'application mobile sur les périphériques est installé et lancé automatiquement.

Installation de l'application sur le périphérique mobile

Le téléchargement de la distribution de l'application Kaspersky Endpoint Security sur le périphérique mobile est assuré par l'utilitaire kmlisten.exe. Cet utilitaire est installé sur le poste de travail avec la tâche d'installation à distance. Dès que le poste de travail est connecté à un appareil mobile répondant aux configurations matérielles et logicielles requises de l'application, l'utilitaire propose à l'utilisateur d'y installer Kaspersky Endpoint Security.

► *Pour copier le fichier de distribution de l'application Kaspersky Endpoint Security à partir du poste de travail sur le périphérique mobile, l'utilisateur doit procéder comme suit :*

1. Connecter le périphérique au poste de travail.

   Si l'appareil répond aux pré-requis système pour l'installation de l'application mobile, la fenêtre de l'utilitaire kmlisten.exe s'ouvre automatiquement.

2. Dans la liste des périphériques détectés, choisir le périphérique où il est nécessaire d'installer l'application.

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

L'utilitaire va copier le fichier de distribution de l'application sur les périphériques choisis et va afficher les résultats du fonctionnement. L'installation de Kaspersky Endpoint Security démarrera automatiquement sur l'appareil lorsque le fichier de distribution aura bien été téléchargé.

> L'utilitaire kmlisten.exe propose d'installer l'application à chaque connexion de l'appareil mobile à l'ordinateur. Pour désactiver le lancement automatique de l'utilitaire kmlisten.exe à chaque connexion de l'appareil mobile, l'utilisateur doit cocher la case **Interrompre l'exécution automatique de l'application d'installation de Kaspersky Endpoint Security** dans la fenêtre de l'utilitaire **KSM10**.

Installation à partir de Self Service Portal

L'utilisateur de l'appareil installe manuellement Kaspersky Endpoint Security à partir de Self Service Portal. Lors de l'ajout de son appareil mobile au Self Service Portal, l'utilisateur télécharge le paquet d'installation de Kaspersky Endpoint Security. Le paquet d'installation contient le fichier de distribution de Kaspersky Endpoint Security, le certificat commun et les paramètres de connexion au Serveur d'administration. L'utilisateur utilise son propre compte sur Self Service Portal pour installer l'application.

Après l'installation de Kaspersky Endpoint Security sur l'appareil mobile, la préparation de l'application s'effectue automatiquement.

Pour en savoir plus sur l'ajout d'un appareil mobile sur Self Service Portal et sur la procédure d'installation de Kaspersky Endpoint Security, consultez le *Manuel d'implantation de Kaspersky Security Center*.

Installation à partir de Google Play

L'utilisateur de l'appareil installe manuellement Kaspersky Endpoint Security à partir de Google Play. L'installation s'effectue selon la méthode classique pour la plate-forme Android. L'utilisateur utilise son propre compte Google pour installer l'application.

Pour en savoir plus sur la procédure d'installation de Kaspersky Endpoint Security à partir de Google Play, consultez le site du support technique de Google http://support.google.com/googleplay/.

Préparation de l'application

Si l'application Kaspersky Endpoint Security a été installée sur l'appareil mobile de l'utilisateur via l'envoi de messages, via le poste de travail ou à partir de Self Service Portal, il n'est pas nécessaire de préparer l'application.

La préparation de l'application s'effectue après son installation sur l'appareil. La préparation de l'application comprend les étapes suivantes :

1. L'administrateur envoie à l'utilisateur les paramètres de synchronisation de l'appareil mobile avec le Serveur d'administration (adresse du serveur et port) en utilisant l'une des méthodes disponibles (par exemple par message électronique).

2. L'utilisateur configure les paramètres de synchronisation de l'appareil mobile avec le Serveur d'administration dans l'Assistant de configuration initiale ou dans les paramètres de Kaspersky Endpoint Security.

3. L'administrateur crée un certificat commun pour l'utilisateur de l'appareil mobile (cf. page 33).

4. L'utilisateur reçoit automatiquement une notification lui proposant d'installer le certificat commun. Lorsque l'utilisateur confirme, le certificat commun est installé sur l'appareil mobile.

Pour la synchronisation avec le Serveur d'administration, l'accès Internet doit être activé sur l'appareil mobile.

Pour en savoir plus sur la configuration des paramètres de synchronisation de l'appareil mobile avec le Serveur d'administration et sur l'obtention d'un certificat commun, consultez *l'aide de Kaspersky Endpoint Security*.

Au terme de la synchronisation suivante de l'appareil mobile avec le Serveur d'administration, l'appareil mobile sur lequel Kaspersky Endpoint Security est installé est placé dans le dossier **Périphériques non définis** dans le groupe d'administration indiqué lors de l'installation de l'application (par défaut, il s'agit du groupe **KSM 10**). Vous pouvez déplacer l'appareil mobile dans le dossier **Ordinateurs administrés** du groupe d'administration que vous avez créé, manuellement ou à l'aide de règles de déplacement automatique (cf. section "Création des règles du transfert automatique des périphériques dans le groupe d'administration" à la page 31).

Activation de l'application

Pour que la solution complète Kaspersky Security for Mobile fonctionne parfaitement, la licence acquise par l'organisation sur le Kaspersky Security Center doit s'étendre à la fonctionnalité **Gestion des appareils mobiles**. Pour en savoir plus sur la licence du Kaspersky Security Center et les options de licence, consultez le *Manuel de l'administrateur du Kaspersky Security Center*.

Pour activer l'application mobile, il faut créer une stratégie pour le groupe d'administration dans lequel se trouve l'appareil, et indiquer une clé du stockage de Kaspersky Security Center pour cette stratégie. L'activation de l'application mobile s'effectue après l'application de la stratégie de groupe lors de la synchronisation des appareils mobiles avec le Serveur d'administration. Suite à l'installation de l'application, le périphérique mobile tente de se synchroniser au Serveur d'administration toutes les trois heures. Après l'application d'une stratégie, la fréquence de synchronisation du périphérique avec le Serveur d'administration sera celle que vous aurez spécifiée lors de la création de cette stratégie. Par défaut, la synchronisation s'exécute toutes les six heures. Pour en savoir plus sur la création d'une stratégie de groupe, consultez le*Manuel de l'administrateur de Kaspersky Security for Mobile*.

Vous pouvez ajouter une clé au stockage de Kaspersky Security Center à l'aide d'un code d'activation ou d'un fichier clé. Pour en savoir plus sur l'ajout d'une clé au stockage de Kaspersky Security Center, consultez le *Manuel de l'administrateur du Kaspersky Security Center*. Lors de la connexion suivante du périphérique mobile au Serveur d'administration, les informations sur la licence seront téléchargées sur le périphérique avec la stratégie. L'application mobile installée sur l'appareil sera activée.

Si l'application n'est pas activée dans les trois jours qui suivent l'installation sur l'appareil mobile, ses fonctionnalités seront automatiquement restreintes. Lorsqu'elle fonctionne en mode restreint, l'application continue à effectuer la synchronisation avec le Serveur d'administration.

En mode restreint, dans Kaspersky Endpoint Security for Android, la recherche de virus est possible à partir des bases anti-virus installées avant la date d'expiration de la licence. La mise à jour des bases anti-virus n'est plus possible par la suite. En mode restreint, la protection contre les menaces Internet (Protection Internet), la protection de l'appareil contre la perte et le vol (Antivol), ainsi que la configuration à distance des paramètres de l'application et de l'appareil mobile ne sont pas disponibles.

Suppression de l'application

Les méthodes suivantes sont disponibles pour supprimer Kaspersky Endpoint Security :

1. Suppression de l'application par l'utilisateur.

   L'utilisateur supprime lui-même Kaspersky Endpoint Security via l'interface de l'application. Pour que cela soit possible, la suppression de l'application doit être autorisée dans la stratégie de groupe appliquée à l'appareil.

2. Suppression de l'application par l'administrateur.

   L'administrateur supprime à distance l'application via la Console d'administration Kaspersky Security Center. Il est possible de supprimer l'application sur un seul appareil ou sur plusieurs à la fois.

Dans cette section

Suppression de l'application à distance

Vous pouvez supprimer à distance Kaspersky Endpoint Security des appareils mobiles des utilisateurs en utilisant les méthodes suivantes :

- Création d'une stratégie de groupe. Cette méthode est pratique si vous souhaitez supprimer l'application de plusieurs appareils à la fois.
- Configuration des paramètres locaux de l'application. Cette méthode est pratique si vous souhaitez supprimer l'application d'un seul appareil.

► *Pour supprimer l'application en appliquant une stratégie de groupe, procédez comme suit :*

1. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, sélectionnez le groupe d'administration où se trouvent les appareils mobiles desquels vous souhaitez supprimer Kaspersky Endpoint Security.

2. Dans la zone de travail du groupe, choisissez l'onglet **Stratégies**.

3. Dans la liste des stratégies, sélectionnez la stratégie pour l'application Kaspersky Endpoint Security.

   Le cas échéant, vous pouvez créer une nouvelle stratégie de groupe. Pour en savoir plus sur la création et la configuration d'une stratégie de groupe, consultez le*Manuel de l'administrateur de Kaspersky Security for Mobile*.

4. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.

5. Sélectionnez la section **Paramètres avancés**.

6. Dans la section **Administration de l'application**, cochez la case **Supprimer Kaspersky Endpoint Security for Android de l'appareil**.

7. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

Après la synchronisation avec le Serveur d'administration, l'application Kaspersky Endpoint Security sera supprimée des appareils mobiles. Les utilisateurs des appareils mobiles reçoivent une notification les informant de la suppression de l'application.

► *Pour supprimer l'application en configurant les paramètres locaux, procédez comme suit :*

1. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, sélectionnez le groupe d'administration où se trouve l'appareil mobile duquel vous souhaitez supprimer Kaspersky Endpoint Security.

2. Dans la zone de travail du groupe, sélectionnez l'onglet **Ordinateurs**.

3. Dans la liste des appareils, sélectionnez celui duquel vous souhaitez supprimer l'application.

4. Double-cliquez pour ouvrir la fenêtre des propriétés de l'appareil.

5. Sélectionnez la section **Applications** → **Kaspersky Endpoint Security**.

6. Double-cliquez pour ouvrir la fenêtre des propriétés de l'application Kaspersky Endpoint Security.

7. Sélectionnez la section **Paramètres avancés**.

8. Dans la section **Administration de l'application**, cochez la case **Supprimer Kaspersky Endpoint Security for Android de l'appareil**.

9. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

Après la synchronisation avec le Serveur d'administration, l'application Kaspersky Endpoint Security sera supprimée de l'appareil mobile. L'utilisateur de l'appareil reçoit une notification l'informant de la suppression de l'application.

Permettre aux utilisateurs de supprimer l'application

Vous pouvez autoriser les utilisateurs à supprimer Kaspersky Endpoint Security de leur appareil mobile à l'aide des méthodes suivantes :

- Création d'une stratégie de groupe. Cette méthode est pratique si vous souhaitez autoriser la suppression de l'application par les utilisateurs de plusieurs appareils à la fois.

- Configuration des paramètres locaux de l'application. Cette méthode est pratique si vous souhaitez autoriser la suppression de l'application par l'utilisateur d'un appareil.

► *Pour autoriser la suppression de l'application dans une stratégie de groupe, procédez comme suit :*

1. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, sélectionnez le groupe d'administration où se trouvent les appareils mobiles pour lesquels vous souhaitez autoriser la suppression de Kaspersky Endpoint Security.

2. Dans la zone de travail du groupe, choisissez l'onglet **Stratégies**.

3. Dans la liste des stratégies, sélectionnez la stratégie pour l'application Kaspersky Endpoint Security.

   Le cas échéant, vous pouvez créer une nouvelle stratégie de groupe. Pour en savoir plus sur la création et la configuration d'une stratégie de groupe, consultez le*Manuel de l'administrateur de Kaspersky Security for Mobile*.

4. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.

5. Sélectionnez la section **Paramètres avancés**.

6. Dans la section **Administration de l'application**, cochez la case **Autoriser la suppression de Kaspersky Endpoint Security for Android**.

7. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

Après la synchronisation avec le Serveur d'administration, la suppression de l'application par l'utilisateur sera autorisée sur les appareils mobiles. Le bouton de suppression de l'application sera accessible dans les paramètres de Kaspersky Endpoint Security.

► *Pour autoriser la suppression de l'application dans les paramètres locaux de l'application, procédez comme suit :*

1. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, sélectionnez le groupe d'administration où se trouvent les appareils mobiles pour lequel vous souhaitez autoriser la suppression de Kaspersky Endpoint Security.

2. Dans la zone de travail du groupe, sélectionnez l'onglet **Ordinateurs**.

3. Dans la liste des appareils, sélectionnez celui pour lequel vous souhaitez autoriser la suppression de l'application par l'utilisateur.

4. Double-cliquez pour ouvrir la fenêtre des propriétés de l'appareil.

5. Sélectionnez la section **Applications** → **Kaspersky Endpoint Security**.

6. Double-cliquez pour ouvrir la fenêtre des propriétés de l'application Kaspersky Endpoint Security.

7. Sélectionnez la section **Paramètres avancés**.

8. Dans la section **Administration de l'application**, cochez la case **Autoriser la suppression de Kaspersky Endpoint Security for Android**.
9. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

Après la synchronisation avec le Serveur d'administration, la suppression de l'application par l'utilisateur sera autorisée sur l'appareil mobile. Le bouton de suppression de l'application sera accessible dans les paramètres de Kaspersky Endpoint Security.

Suppression de l'application par l'utilisateur

► *Pour supprimer lui-même Kaspersky Endpoint Security de son appareil mobile, l'utilisateur doit procéder comme suit :*

1. Dans la fenêtre principale de Kaspersky Endpoint Security, ouvrir le volet de lancement rapide et cliquer sur **Paramètres** → **Paramètres avancés** → **Suppression de l'application**.

   Une demande de confirmation apparaît à l'écran.

2. Confirmer la suppression de Kaspersky Endpoint Security.

L'application Kaspersky Endpoint Security sera supprimée de l'appareil mobile de l'utilisateur.

Kaspersky Safe Browser for iOS

Cette section contient des informations concernant l'utilisation de Kaspersky Safe Browser sur le système d'exploitation iOS : instructions d'installation, préparation de l'application, activation et suppression de l'application.

Dans cette section

Mise à jour d'une version précédente de l'application

Il est possible de mettre à jour une version précédente de l'application via l'App Store. C'est l'utilisateur de l'appareil mobile qui met à jour Kaspersky Safe Browser à l'aide de l'App Store. La mise à jour s'effectue selon la méthode classique pour la plate-forme iOS. L'utilisateur met à jour l'application en utilisant son propre identifiant Apple.

Installation via le Serveur des périphériques mobiles iOS MDM

Pour que Kaspersky Safe Browser puisse être installé, les appareils mobiles doivent être connectés au Serveur des périphériques mobiles iOS MDM. Lors de la connexion de l'appareil au Serveur des périphériques mobiles iOS MDM, les actions suivantes doivent être effectuées :

1. Le plug-in d'administration des appareils mobiles sur la plate-forme iOS doit être installé sur le poste de travail de l'administrateur.

   Le plug-in d'administration des appareils mobiles sur la plate-forme iOS est inclus dans le paquet d'installation de Kaspersky Security Center.

2. Le certificat APN doit être installé sur le Serveur des périphériques mobiles iOS MDM.

   Le *certificat APN* est un certificat qui permet au Serveur d'administration de se connecter au service des APN pour l'envoi de notifications push sur les périphériques mobiles iOS MDM.

3. Le profil iOS MDM doit être installé sur les appareils mobiles des utilisateurs.

   Le *profil iOS MDM* est un profil qui contient l'ensemble des paramètres de connexion des appareils iOS MDM au Serveur d'administration.

4. Le poste de travail de l'administrateur doit disposer du profil provisioning.

   Le *profil provisioning* est utilisé pour l'administration des applications diffusées autrement que par l'App Store. Le profil provisioning comporte des informations sur la licence et est rattaché à une application en particulier.

Pour en savoir plus sur la connexion des appareils mobiles au Serveur des périphériques mobiles iOS MDM, consultez le *Manuel d'implantation du Kaspersky Security Center*.

L'installation de Kaspersky Safe Browser via le Serveur des périphériques mobiles iOS MDM passe par les étapes suivantes :

1. Ajout du fichier de distribution de Kaspersky Safe Browser via le Serveur des périphériques mobiles iOS MDM.
2. Installation de Kaspersky Safe Browser sur les appareils mobiles.

Dans cette section

Ajout de l'application sur le Serveur des périphériques mobiles iOS MDM

► *Pour ajouter Kaspersky Safe Browser for iOS sur le Serveur des périphériques mobiles iOS MDM, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Gestion des appareils mobiles**.
2. Dans l'espace de travail du dossier, sélectionnez le Serveur des périphériques mobiles iOS MDM.
3. Sélectionnez l'option **Propriétés** dans le menu contextuel du Serveur iOS MDM.

   La fenêtre **<Serveur iOS MDM>** s'ouvre.
4. Sélectionnez la section **Applications administrées**.
5. Cliquez sur le bouton **Ajouter**.

   La fenêtre **Ajout d'une application** s'ouvre.
6. Dans le champ **Nom de l'application**, saisissez le nom de l'application administrée.

7. Dans le champ **Apple ID ou lien vers l'application**, indiquez l'identifiant Apple de l'application Kaspersky Safe Browser dans l'App Store.

8. Configurez les paramètres avancés :

   - Cochez la case **Supprimer avec le profil iOS MDM** pour que le profil iOS MDM soit supprimé après la suppression de Kaspersky Safe Browser de l'appareil mobile de l'utilisateur.

   - Cochez la case **Interdire la création de copies de sauvegarde des données** pour interdire à l'utilisateur de créer des copies de sauvegarde des données, par exemple à l'aide du service iCloud.

9. Cliquez sur le bouton **OK**.

   L'application mobile Kaspersky Safe Browser for iOS sera ajoutée à la liste des applications administrées.

10. Cliquez sur le bouton **OK** pour enregistrer les modifications apportées.

Installation de l'application sur le périphérique mobile

► *Pour installer Kaspersky Safe Browser for iOS sur un périphérique mobile, procédez comme suit :*

1. Dans l'arborescence de la console, dans le dossier **Gestion des appareils mobiles**, sélectionnez le sous-dossier **Appareils mobiles**.

2. Dans l'espace de travail du dossier, sélectionnez les appareils iOS MDM en cliquant sur le lien **Afficher : iOS MDM**.

3. Choisissez l'appareil iOS MDM dans la liste.

4. Choisissez l'option **Installer l'application sur le périphérique** dans le menu contextuel.

5. La fenêtre **Sélection de l'application à installer** s'ouvre.

6. Choisissez Kaspersky Safe Browser dans la liste des applications administrées.

Kaspersky Safe Browser est automatiquement téléchargée sur l'appareil de l'utilisateur. L'application demande à l'utilisateur s'il accepte l'installation. Lorsque l'utilisateur accepte, Kaspersky Safe Browser installe l'application sur l'appareil.

Installation à partir de l'App Store

L'utilisateur de l'appareil effectue manuellement l'installation de Kaspersky Safe Browser à partir de l'App Store. L'installation s'effectue selon la méthode classique pour la plate-forme iOS. L'utilisateur installe l'application en utilisant son propre identifiant Apple.

Pour en savoir plus sur la procédure d'installation de Kaspersky Safe Browser à partir de l'App Store, consultez le *Manuel de l'utilisateur de Kaspersky Safe Browser*.

Préparation de l'application

La préparation de l'application s'effectue après son installation sur l'appareil. La préparation de l'application comprend les étapes suivantes :

1. L'administrateur envoie à l'utilisateur les paramètres de synchronisation de l'appareil mobile avec le Serveur d'administration (adresse du serveur et port) en utilisant l'une des méthodes disponibles (par exemple par message électronique).
2. L'utilisateur configure les paramètres de synchronisation de l'appareil mobile avec le Serveur d'administration dans l'Assistant de configuration initiale ou dans les paramètres de Kaspersky Safe Browser.

   Pour en savoir plus sur la configuration des paramètres de synchronisation de l'appareil mobile avec le Serveur d'administration et sur l'obtention d'un certificat commun, consultez le *Manuel de l'utilisateur de Kaspersky Safe Browser*.
3. L'administrateur crée un certificat commun pour l'utilisateur de l'appareil mobile (cf. page 33).
4. L'utilisateur reçoit une notification lui proposant d'installer le certificat commun. Lorsque l'utilisateur confirme, le certificat commun est installé sur l'appareil mobile.

Pour la synchronisation avec le Serveur d'administration, l'accès Internet doit être activé sur l'appareil mobile.

Au terme de la synchronisation suivante de l'appareil mobile avec le Serveur d'administration, l'appareil mobile sur lequel Kaspersky Safe Browser est installé est placé dans le dossier **Périphériques non définis** dans le groupe d'administration indiqué lors de l'installation de l'application (par défaut, il s'agit du groupe **KSM 10**). Vous pouvez déplacer le périphérique mobile dans le dossier **Ordinateurs administrés** du groupe que vous avez créé manuellement ou à l'aide de règles de déplacement automatique (cf. section "Création de règles du transfert automatique des périphériques dans le groupe d'administration" à la page 31).

Activation de l'application

Pour que la solution complète Kaspersky Security for Mobile fonctionne parfaitement, la licence acquise par l'organisation sur le Kaspersky Security Center doit s'étendre à la fonctionnalité **Gestion des appareils mobiles**. Pour en savoir plus sur la licence du Kaspersky Security Center et les options de licence, consultez le *Manuel de l'administrateur du Kaspersky Security Center*.

Pour activer l'application mobile, il faut créer une stratégie pour le groupe d'administration dans lequel se trouve l'appareil, et indiquer une clé du stockage de Kaspersky Security Center pour cette stratégie. L'activation de l'application mobile s'effectue après l'application de la stratégie de groupe lors de la synchronisation des appareils mobiles avec le Serveur d'administration. Suite à l'installation de l'application, le périphérique mobile tente de se synchroniser au Serveur d'administration toutes les trois heures. Après l'application d'une stratégie, la fréquence de synchronisation du périphérique avec le Serveur d'administration sera celle que vous aurez spécifiée lors de la création de cette stratégie. Par défaut, la synchronisation s'exécute toutes les six heures. Pour en savoir plus sur la création d'une stratégie de groupe, consultez le*Manuel de l'administrateur de Kaspersky Security for Mobile*.

Vous pouvez ajouter une clé au stockage de Kaspersky Security Center à l'aide d'un code d'activation ou d'un fichier clé. Pour en savoir plus sur l'ajout d'une clé au stockage de Kaspersky Security Center, consultez le *Manuel de l'administrateur du Kaspersky Security Center*. Lors de la connexion suivante du périphérique mobile au Serveur d'administration, les informations sur la licence seront téléchargées sur le périphérique avec la stratégie. L'application mobile installée sur l'appareil sera activée.

Si l'application n'est pas activée dans les trois jours qui suivent l'installation sur l'appareil mobile, ses fonctionnalités seront automatiquement restreintes. Lorsqu'elle fonctionne en mode restreint, l'application continue à effectuer la synchronisation avec le Serveur d'administration.

En mode restreint, les fonctions de configuration à distance de la Protection Internet et d'envoi de commandes de l'Antivol à l'appareil en cas de vol ou de perte ne sont pas disponibles.

Suppression de l'application

La suppression de l'application mobile Kaspersky Safe Browser est exécutée par l'utilisateur sur son appareil mobile selon la méthode traditionnelle pour la plate-forme iOS.

Pour en savoir plus sur la suppression de l'application, consultez le *Manuel de l'utilisateur de Kaspersky Safe Browser*.

Kaspersky Safe Browser for Windows Phone

Cette section contient des informations concernant l'utilisation de Kaspersky Safe Browser sur le système d'exploitation Windows Phone : instructions d'installation, préparation de l'application, activation et suppression de l'application.

Dans cette section

Mise à jour d'une version précédente de l'application

Il est possible de mettre à jour une version précédente de l'application via la boutique Windows Phone. C'est l'utilisateur de l'appareil mobile qui met à jour Kaspersky Safe Browser à l'aide de la boutique Windows Phone. La mise à jour s'effectue selon la méthode classique pour la plateforme Windows Phone. L'utilisateur utilise son propre compte Microsoft pour la mise à jour de l'application.

Installation à partir de la boutique Windows Phone

C'est l'utilisateur de l'appareil mobile qui installe Kaspersky Safe Browser manuellement à partir de la boutique Windows Phone. L'installation s'effectue selon la méthode classique pour la plate-forme Windows Phone. L'utilisateur utilise son propre compte Microsoft pour installer l'application.

Pour en savoir plus sur la procédure d'installation de Kaspersky Safe Browser à partir de la boutique Windows Phone, consultez le *Manuel de l'utilisateur de Kaspersky Safe Browser*.

Préparation de l'application

La préparation de l'application s'effectue après son installation sur l'appareil. La préparation de l'application comprend les étapes suivantes :

1. L'administrateur envoie à l'utilisateur les paramètres de synchronisation de l'appareil mobile avec le Serveur d'administration (adresse du serveur et port) en utilisant l'une des méthodes disponibles (par exemple par message électronique).

2. L'utilisateur configure les paramètres de synchronisation de l'appareil mobile avec le Serveur d'administration dans l'Assistant de configuration initiale ou dans les paramètres de Kaspersky Safe Browser.

   Pour en savoir plus sur la configuration des paramètres de synchronisation de l'appareil mobile avec le Serveur d'administration et sur l'obtention d'un certificat commun, consultez le *Manuel de l'utilisateur de Kaspersky Safe Browser*.

3. L'administrateur crée un certificat commun pour l'utilisateur de l'appareil mobile (cf. page 33).

4. L'utilisateur reçoit une notification lui proposant d'installer le certificat commun. Lorsque l'utilisateur confirme, le certificat commun est installé sur l'appareil mobile.

Pour la synchronisation avec le Serveur d'administration, l'accès Internet doit être activé sur l'appareil mobile.

Au terme de la synchronisation suivante de l'appareil mobile avec le Serveur d'administration, l'appareil mobile sur lequel Kaspersky Safe Browser est installé est placé dans le dossier **Périphériques non définis** dans le groupe d'administration indiqué lors de l'installation de l'application (par défaut, il s'agit du groupe **KSM 10**). Vous pouvez déplacer le périphérique mobile dans le dossier **Ordinateurs administrés** du groupe que vous avez créé manuellement ou à l'aide de règles de déplacement automatique (cf. section "Création de règles du transfert automatique des périphériques dans le groupe d'administration" à la page 31).

Activation de l'application

Pour que la solution complète Kaspersky Security for Mobile fonctionne parfaitement, la licence acquise par l'organisation sur le Kaspersky Security Center doit s'étendre à la fonctionnalité **Gestion des appareils mobiles**. Pour en savoir plus sur la licence du Kaspersky Security Center et les options de licence, consultez le *Manuel de l'administrateur du Kaspersky Security Center*.

Pour activer l'application mobile, il faut créer une stratégie pour le groupe d'administration dans lequel se trouve l'appareil, et indiquer une clé du stockage de Kaspersky Security Center pour cette stratégie. L'activation de l'application mobile s'effectue après l'application de la stratégie de groupe lors de la synchronisation des appareils mobiles avec le Serveur d'administration. Suite à l'installation de l'application, le périphérique mobile tente de se synchroniser au Serveur d'administration toutes les trois heures. Après l'application d'une stratégie, la fréquence de synchronisation du périphérique avec le Serveur d'administration sera celle que vous aurez spécifiée lors de la création de cette stratégie. Par défaut, la synchronisation s'exécute toutes les six heures. Pour en savoir plus sur la création d'une stratégie de groupe, consultez le*Manuel de l'administrateur de Kaspersky Security for Mobile*.

Vous pouvez ajouter une clé au stockage de Kaspersky Security Center à l'aide d'un code d'activation ou d'un fichier clé. Pour en savoir plus sur l'ajout d'une clé au stockage de Kaspersky

Security Center, consultez le *Manuel de l'administrateur du Kaspersky Security Center*. Lors de la connexion suivante du périphérique mobile au Serveur d'administration, les informations sur la licence seront téléchargées sur le périphérique avec la stratégie. L'application mobile installée sur l'appareil sera activée.

Si l'application n'est pas activée dans les trois jours qui suivent l'installation sur l'appareil mobile, ses fonctionnalités seront automatiquement restreintes. Lorsqu'elle fonctionne en mode restreint, l'application continue à effectuer la synchronisation avec le Serveur d'administration.

En mode restreint, les fonctions de configuration à distance de la Protection Internet et d'envoi de commandes de l'Antivol à l'appareil en cas de vol ou de perte ne sont pas disponibles.

Suppression de l'application

La suppression de l'application mobile Kaspersky Safe Browser est exécutée par l'utilisateur sur son appareil mobile selon la méthode traditionnelle pour la plate-forme Windows Phone.

Pour en savoir plus sur la suppression de l'application, consultez le *Manuel de l'utilisateur de Kaspersky Safe Browser*.

Installation des plug-ins d'administration

Cette section décrit l'installation du plug-in d'administration de la solution complète Kaspersky Security for Mobile sur le poste de travail de l'administrateur.

Dans cette section

Installation du plug-in d'administration de Kaspersky Endpoint Security

► *Afin d'installer le plug-in d'administration des périphériques KES de Kaspersky Endpoint Security,*

copiez le fichier du plug-in klcfinst.exe à partir du fichier de distribution de la solution complète, et lancez-le sur le poste de travail de l'administrateur.

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

Vous pouvez vérifier que le plug-in d'administration de Kaspersky Endpoint Security est installé en consultant la liste des plug-ins d'administration d'applications installés dans la fenêtre des propriétés du Serveur d'administration, accessible dans la section **Avancé** → **Informations concernant les plug-ins d'administration d'applications installés**.

Installation du plug-in d'administration de Kaspersky Mobile Device Management

► *Afin d'installer le plug-in d'administration des périphériques EAS et iOS MDM de Kaspersky Mobile Device Management,*

copiez le fichier du plug-in klmdminst.exe à partir du fichier de distribution de la solution complète, et lancez-le sur le poste de travail de l'administrateur.

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

Vous pouvez vérifier que le plug-in de Kaspersky Mobile Device Management est installé en consultant la liste des plug-ins d'administration d'applications installés dans la fenêtre des propriétés du Serveur d'administration, accessible dans la section **Avancé** → **Informations concernant les plug-ins d'administration d'applications installés**.

Mise à jour des plug-ins d'administration

Pour mettre à jour les plug-ins d'administration de Kaspersky Endpoint Security et de Kaspersky Mobile Device Management, il est nécessaire de télécharger la dernière version de l'application sur la page Kaspersky Security for Mobile (http://www.kaspersky.ru/business-security/mobile#tab=frame-1) et de lancer l'Assistant d'installation de chaque plug-in. Les versions précédentes des plug-ins seront automatiquement supprimées lors de l'exécution de l'Assistant d'installation.

Lors de la mise à jour des plug-ins d'administration, les groupes d'administration existants dans le dossier **Ordinateurs administrés** et les règles de déplacement automatique des périphériques depuis le dossier **Périphériques non définis** vers ces groupes, sont sauvegardés. Les stratégies de groupe pour appareils mobiles existantes sont également sauvegardées. Les nouveaux paramètres des stratégies réalisant de nouvelles fonctionnalités de la solution complète Kaspersky Security for Mobile apparaîtront dans les stratégies déjà existantes et présenteront des valeurs par défaut.

Glossaire

A

Administrateur d'appareil

Ensemble de privilèges d'application sur un périphérique Android qui permet à l'application d'utiliser la stratégie d'administration du périphérique. Ceci est indispensable pour exploiter toutes les fonctions de Kaspersky Endpoint Security sur un périphérique Android.

Appareil EAS

Appareil mobile qui se connecte au serveur d'administration selon le protocole Exchange ActiveSync.

Appareil iOS MDM

un périphérique mobile fonctionnant avec iOS et administré par le Serveur des périphériques mobiles iOS MDM.

C

Certificat Apple Push Notification service (APNs)

Certificat signé par la société Apple. Il permet d'exécuter les fonctions du service Apple Push Notification. Grâce au service Apple Push Notification, le Serveur de gestion des périphériques mobiles iOS MDM peut administrer les périphériques iOS.

Conteneur

Enveloppe spéciale pour les applications mobiles qui permet de contrôler les activités des applications qu'elle contient. Le conteneur protège les données personnelles et professionnelles figurant sur l'appareil mobile. Le conteneur utilisé sur les appareils iOS est signé par le même certificat que Kaspersky Safe Browser for iOS.

F

Fichier manifest

Fichier au format PLIST contenant un lien vers le fichier de l'application (fichier ipa) situé sur un serveur Internet. Ce fichier est utilisé par les périphériques iOS pour chercher, télécharger et installer des applications depuis un serveur Internet.

G

Groupe d'administration

Ensemble d'appareils administrés, notamment des périphériques mobiles, réunis suivant leurs fonctionnalités et les applications dont ils sont équipés. Les périphériques administrés sont regroupés pour assurer une gestion unifiée. Par exemple, le groupe d'administration peut regrouper les périphériques mobiles équipés du même système d'exploitation. Un groupe peut comprendre d'autres groupes d'administration. Vous pouvez créer des stratégies de groupe et des tâches de groupe pour les périphériques qui font partie d'un groupe.

K

Kaspersky Security Network (KSN)

Infrastructure des services en ligne offrant l'accès à la base opérationnelle de connaissances de Kaspersky Lab sur la réputation des fichiers, des ressources Internet et du logiciel. L'utilisation des données de Kaspersky Security Network permet aux applications de Kaspersky Lab de réagir plus rapidement aux menaces, augmente l'efficacité de fonctionnement de certains modules de la protection et réduit la possibilité de faux positifs.

P

Paquet autonome d'installation

Fichier d'installation de l'application Kaspersky Endpoint 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 paquet d'installation pour cette application et représente un cas particulier de paquet d'applications mobiles.

Paquet d'applications mobiles

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

Paquet d'installation

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 paquet d'installation est créé à partir de fichiers spécifiques inclus dans le fichier de distribution de l'application. Le paquet d'installation contient un ensemble de paramètres nécessaires à l'installation de l'application et à son fonctionnement après l'installation. Par défaut, les valeurs de paramètre du paquet d'installation correspondent aux valeurs des paramètres de l'application.

Plug-in 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 son propre plug-in d'administration. Ce plug-in d'administration fait partie de toutes les applications de Kaspersky Lab administrées à l'aide du Kaspersky Security Center.

Poste de travail de l'administrateur

Ordinateur où la Console d'administration du Kaspersky Security Center est déployée. Si le poste de travail de l'administrateur présente un plug-in d'administration de l'application, l'administrateur peut gérer les applications mobiles Kaspersky Endpoint Security déployées sur les périphériques des utilisateurs.

Profil iOS MDM

Profil comportant tout un ensemble de paramètres pour la connexion des périphériques mobiles iOS au Serveur d'administration. Ce profil permet de diffuser les profils de configuration iOS en arrière-plan à l'aide du Serveur de gestion des périphériques mobiles iOS MDM et d'obtenir un

diagnostic étendu sur les périphériques mobiles. Vous devez envoyer le lien vers le profil iOS MDM à l'utilisateur pour permettre au serveur de gestion des périphériques mobiles iOS de détecter et de connecter son appareil mobile fonctionnant avec iOS.

Profil provisioning

Ensemble de paramètres dédiés au fonctionnement de l'application sur les périphériques mobiles iOS. Le profil provisioning comporte des informations sur la licence et est rattaché à une application en particulier.

R

Requête Certificate Signing Request

Fichier contenant les paramètres du serveur d'administration qui, après confirmation de Kaspersky Lab, est envoyé à Apple pour obtenir le certificat APN.

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 de gestion des périphériques mobiles Exchange ActiveSync

Module de Kaspersky Endpoint Security qui permet de connecter les appareils mobiles Exchange ActiveSync au Serveur d'administration. Il est installé sur l'ordinateur client.

Serveur des périphériques mobiles iOS MDM

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

Serveur Internet de Kaspersky Security Center

Le module Kaspersky Security Center qui s'installe avec le Serveur d'administration. Le Serveur Internet est conçu pour transférer via réseau des paquets d'installation autonomes, des profils iOS MDM, ainsi que des fichiers du dossier partagé.

Stratégie

Ensemble de paramètres pour le fonctionnement de l'application et des applications mobiles Kaspersky Endpoint Security sur tous les périphériques du groupe d'administration ou sur des périphériques en particulier. Les stratégies peuvent différer en fonction du groupe d'administration. Chaque stratégie inclut des paramètres pré-définis pour toutes les fonctions des applications mobiles Kaspersky Endpoint Security.

T

Tâche de groupe

Tâche conçue pour le groupe d'administration et exécutable sur tous les périphériques administrés de ce groupe.

U

Utilitaire Kaspersky SMS Broadcasting

Utilitaire pour l'envoi de messages SMS sur les appareils Android des utilisateurs. L'utilitaire est installé sur l'appareil Android de l'administrateur.

Kaspersky Lab AO

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"). En Russie, selon les données d'IDC, Kaspersky Lab est le fournisseur de système de protection informatique favori des particuliers ("IDC Endpoint Tracker 2014").

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, c'est un groupe international qui dispose de 34 succursales dans 31 pays. La société emploie plus de 3000 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 comprend des applications de sécurité informatique pour ordinateurs de bureau et ordinateurs portables ainsi que des applications pour la protection des tablettes, des smartphones et d'autres appareils mobiles.

La société propose des solutions et des technologies de protection et de contrôle des stations de travail et des appareils mobiles, des machines virtuelles, des serveurs de fichiers et des serveurs Web, des passerelles de messagerie et des pare-feu. L'entreprise propose également des produits spécialisés pour la protection contre les attaques DDoS, pour la protection des systèmes d'automatisation industrielle ainsi que pour la prévention des escroqueries financières. Ces solutions, associées à une administration centralisée, permettent de créer et d'exploiter une protection automatisée efficace des entreprises de toutes tailles 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 plate-formes matérielles.

Les experts de la lutte antivirus de Kaspersky Lab travaillent 24h/24. Chaque jour, ils trouvent des centaines de milliers 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.

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, notamment : Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, General Dynamics, Facebook, Juniper Networks, Lenovo, H3C, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. De nombreuses technologies novatrices développées par la société sont brevetées.

REALISATIONS. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a décroché des centaines de récompenses. Ainsi, en 2014, d'après les tests effectués par AV-Comparatives, une société autrichienne renommée dans le domaine de l'évaluation des logiciels antivirus, Kaspersky Lab est l'un des deux meilleurs fournisseurs en termes de nombre de certificats Advanced+ reçus. L'entreprise a donc reçu le certificat Top Rated. 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 400 millions d'utilisateurs. Elle compte également plus de 270 000 entreprises parmi ses clients.

Site de Kaspersky Lab :	http://www.kaspersky.com/fr
Encyclopédie des virus :	http://www.viruslist.com/fr/
Laboratoire d'étude des virus :	http://newvirus.kaspersky.fr/ (pour l'analyse des fichiers et sites Internet suspects)
Forum de Kaspersky Lab :	http://forum.kaspersky.fr

Information sur le code tiers

L'information sur le code tiers se trouve dans le fichier legal_notices.txt, situé dans le dossier d'installation de la solution complète Kaspersky Security for Mobile.

Sur les appareils Android, l'information sur le code tiers est accessible dans les propriétés de l'application Kaspersky Endpoint Security for Android, dans la section **Paramètres avancés**, en appuyant sur le bouton **Infos sur l'application**.

Sur les appareils iOS et Windows Phone, l'information sur le code tiers est accessible dans les propriétés de l'application Kaspersky Safe Browser, dans la section **Infos sur l'application**.

Avis de marques déposées

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

Apple, Keychain, iPhone, iPad, Mac OS, OS X, Safari sont des marques commerciales d'Apple Inc. déposées aux Etats-Unis et dans d'autres pays.

App Store est une marque commerciale d'Apple Inc.

Android, Google et Google Play sont des marques déposées de Google, Inc.

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

ARM est une marque commerciale ou déposée d'ARM Ltd. ou de ses filiales.

Intel, Atom sont des marques commerciales d'Intel Corporation, déposées aux Etats-Unis et dans d'autres pays.

Index

A

C

G

K

P