Kaspersky Security for Mobile

Manuel d'administrateur

VERSION DE L'APPLICATION : 10.0 SERVICE PACK 1

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 : 26/01/2015

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

CONTENU

PRESENTATION DU MANUEL

Le manuel de l'administrateur de la solution complète Kaspersky Security for Mobile est destiné aux experts assurant l'installation et l'administration de Kaspersky Security for Mobile, ainsi qu'aux experts assurant l'assistance technique auprès des entreprises utilisant Kaspersky Security for Mobile.

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

- préparatifs de l'installation, installation et activation de Kaspersky Security for Mobile ;
- configuration et utilisation de Kaspersky Security for Mobile.

Ce manuel renseigne également les sources d'informations sur l'application 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 11)

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

Kaspersky Security for Mobile (cf. page 13)

Cette section reprend les informations sur le rôle, les fonctionnalités et la structure de la solution complète Kaspersky Security for Mobile.

Architecture de l'application (cf. page 19)

Cette section décrit les modules de Kaspersky Endpoint Security et leur interaction.

Schémas types de déploiement de la solution complète (cf. page 22)

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

Préparation du déploiement de la solution complète (cf. page 30)

Cette section décrit les préparatifs à réaliser avant de déployer les applications mobiles Kaspersky Endpoint Security 10 sur les appareils des utilisateurs.

Mise à jour d'une version antérieure de Kaspersky Security for Mobile (cf. page 40)

Cette section reprend les informations sur la mise à jour de la version précédente de Kaspersky Security for Mobile.

Kaspersky Lab ZAO (cf. page 138)

Cette section contient des informations sur Kaspersky Lab ZAO.

Informations sur le code tiers (cf. page 139)

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

Avertissements relatifs aux marques (cf. page 140)

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

Index

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 jaune sous le titre "Exemple".

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
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.
➧ *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 UNE RECHERCHE AUTONOME

Vous pouvez utiliser les sources suivantes pour rechercher de manière autonome des informations sur Kaspersky Endpoint Security :

- page de Kaspersky Endpoint Security sur le site Internet de Kaspersky Lab ;
- page de Kaspersky Endpoint Security sur le site Internet du 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.

Une connexion Internet est requise pour consulter les sources d'informations sur les sites Internet.

Page de Kaspersky Endpoint Security sur le site Internet de Kaspersky Lab

La page de Kaspersky Endpoint Security (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 de Kaspersky Endpoint Security 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 de Kaspersky Endpoint Security dans la Base de connaissances

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

La page de Kaspersky Endpoint Security 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 qui portent non seulement sur Kaspersky Endpoint Security, mais également sur 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 permet d'obtenir des informations sur les fenêtres de Kaspersky Endpoint Security, la description des paramètres de l'application et contient des liens vers des descriptions des tâches dans lesquelles ces paramètres sont utilisés.

L'aide complète contient les informations relatives à la configuration et à l'utilisation de Kaspersky Endpoint Security.

Documentation

La documentation de l'application reprend également les manuels.

Le manuel de l'administrateur fournit des informations sur l'exécution des tâches suivantes :

- préparatifs de l'installation, installation et activation de Kaspersky Endpoint Security ;
- configuration et utilisation de Kaspersky Endpoint Security.

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

Cette section décrit les fonctions, les modules et la distribution de la solution complète Kaspersky Security for Mobile. Elle présente également les configurations matérielle et logicielle requises pour Kaspersky Security for Mobile.

DANS CETTE SECTION

PRESENTATION DE KASPERSKY SECURITY FOR MOBILE

Kaspersky Security for Mobile est une solution complète dédiée à la protection et à l'administration des appareils mobiles d'entreprise, ainsi que des appareils personnels des employés utilisés dans un but professionnel. La distribution de Kaspersky Security for Mobile contient le plug-in d'administration de Kaspersky Endpoint Security 10 Service Pack 1 for Mobile (cf. page 19), le plug-in d'administration de Kaspersky Mobile Device Management 10 Service Pack 1 (cf. page. 19) et le paquet d'applications mobiles Kaspersky Endpoint Security pour différents systèmes d'exploitation (cf. page 20).

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 appareils mobiles de l'entreprise, des ordinateurs clients et des systèmes virtuels. Le plug-in d'administration de Kaspersky Endpoint Security 10 Service Pack 1 for Mobile (ci-après, le plug-in d'administration de Kaspersky Endpoint Security) permet de connecter les appareils mobiles au Serveur d'administration de l'entreprise et de configurer des stratégies assurant leur sécurité. Les appareils mobiles peuvent être administrés dès qu'ils ont été connectés au Serveur d'administration. L'administrateur peut commander à distance les appareils administrés. Le plug-in d'administration de Kaspersky Mobile Device Management 10 Service Pack 1 (ci-après, le plug-in d'administration de Kaspersky Mobile Device Management) permet de configurer les paramètres de configuration des appareils iOS et des appareils connectés au serveur de l'entreprise selon le protocole Exchange ActiveSync® sans passer par iPhone Configuration Utility ou par le profil d'administration Exchange ActiveSync.

Les applications mobiles Kaspersky Endpoint Security prennent en charge les systèmes d'exploitation pour appareils mobiles iOS, Android™ et Windows Phone®. Les applications mobiles Kaspersky Endpoint Security permettent de maintenir à jour la sécurité des appareils mobiles professionnels et des données qu'ils contiennent.

Les modules de la solution Kaspersky Security for Mobile offrent les possibilités suivantes à l'administrateur :

- connexion à distance des appareils mobiles des utilisateurs au serveur de l'entreprise ;
- configuration à distance de la protection antivirus des appareils mobiles ;
- configuration à distance des appareils mobiles conformément aux exigences de l'entreprise en matière de sécurité ;
- protection des données stockées sur les appareils mobiles contre les fuites d'informations en cas de perte ou de vol ;
- contrôle de la conformité aux exigences en matière de sécurité de l'entreprise ;
- contrôle de l'utilisation d'Internet sur les appareils mobiles ;
- installation à distance d'applications mobiles tierces sur les appareils des utilisateurs avec possibilité d'utiliser un mécanisme spécial de protection des données (les conteneurs) ;
- configuration de la messagerie d'entreprise sur les appareils mobiles du réseau, y compris si le serveur de messagerie Microsoft® Exchange est déployé au sein de l'entreprise ;
- configuration des paramètres pour une utilisation du réseau de l'entreprise sur les appareils mobiles ;
- configuration de l'utilisation des calendriers de l'entreprise sur les appareils mobiles ;
- configuration de la synchronisation des contacts de l'entreprise ;
- configuration des restrictions matérielles et opérationnelles des appareils mobiles, des restrictions portant sur l'utilisation des applications mobiles et du contenu multimédia ;
- configuration des notifications à l'administrateur relatives aux événements survenant sur les appareils des utilisateurs, via la messagerie électronique ou les SMS.

NOUVEAUTES

Kaspersky Security for Mobile présente les nouvelles fonctionnalités suivantes :

- Prise en charge de certificats communs sur les appareils mobiles pour l'identification des utilisateurs dans Kaspersky Security Center et pour assurer des échanges de données sécurisés avec le Serveur d'administration.
- Prise en charge de l'envoi de commandes depuis Kaspersky Security Center pour protéger les informations contre tout accès non autorisé en cas de perte ou de vol de l'appareil.
- Prise en charge du portail d'entreprise Self Service Portal grâce auquel l'utilisateur peut :
  - télécharger le programme d'installation de l'application mobile Kaspersky Endpoint Security for Android ;
  - télécharger le profil provisioning pour appareil iOS ;
  - administrer les appareils à l'aide de commandes spéciales.
- Prise en charge d'un nouveau système de privilèges d'accès aux fonctions Kaspersky Security for Mobile dans la Console d'administration de Kaspersky Security Center.
- Administration des appareils mobiles sous protocole Exchange ActiveSync (ci-après, les appareils EAS). Les propriétés de la stratégie permettent à l'administrateur de configurer les paramètres suivants pour les appareils EAS :
  - les exigences en matière de mot de passe système ;
  - les paramètres de synchronisation de l'appareil avec le serveur Microsoft Exchange ;
  - les restrictions des fonctions de l'appareil EAS ;
  - les restrictions relatives au fonctionnement des applications sur l'appareil EAS.
- Pour les appareils tournant sous Android (ci-après, les appareils Android) :
  - Restriction du fonctionnement des applications systèmes.
  - Restriction d'accès à tous les sites Internet, à l'exception de ceux indiqués dans la stratégie.
  - Prise en charge du système d'exploitation Android version 5.0.
  - Prise en charge du service Google Cloud Messaging.
  - Administration des appareils Samsung prenant en charge KNOX 1 et KNOX 2. Les propriétés de la stratégie permettent à l'administrateur de configurer les paramètres suivants pour les appareils Samsung :
    - paramètres du Pare-feu ;
    - paramètres du réseau VPN (uniquement pour KNOX 1) ;
    - paramètres du point d'accès APN ;
    - paramètres du serveur de messagerie Microsoft Exchange.
- Pour les appareils fonctionnant avec iOS (ci-après, les appareils iOS) :
  - Basculement entre les modes de fonctionnement professionnel et personnalisé de Kaspersky Safe Browser.
  - Prise en charge du système d'exploitation iOS versions 7.0, 7.1, 8.0.

- Configuration des paramètres de configuration les appareils iOS.
- Administration des appareils mobiles sous protocole iOS MDM (ci-après, les appareils iOS MDM).

- Pour les appareils tournant sous Windows Phone (ci-après, les appareils Windows Phone) :
  - Basculement entre les modes de fonctionnement professionnel et personnalisé de Kaspersky Safe Browser.
  - Prise en charge de l'envoi de la commande de géolocalisation de l'appareil depuis Kaspersky Security Center.

PAQUET DE DISTRIBUTION

Le paquet de distribution de la solution complète Kaspersky Security for Mobile contient les composants suivants :

- l'archive auto-extractible sc_package_fr contenant les fichiers d'installation des applications mobiles pour les principaux systèmes pris en charge :
  - adb.exe, AdbWinApi.dll, AdbWinUsbApi.dll : ensemble des fichiers nécessaires à l'installation de l'application mobile Kaspersky Endpoint Security 10 for Android ;
  - installer.ini – fichier de configuration contenant les paramètres de connexion au Serveur d'administration;
  - KSM_10_5_11_xxx.apk : fichier d'installation de l'application mobile Kaspersky Endpoint Security 10 for Android ;
  - kmlisten.exe : utilitaire de distribution du paquet d'installation sur un appareil 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.
- klcfginst_fr.exe — fichier d'installation du plug-in d'administration de Kaspersky Endpoint Security 10 for Mobile à l'aide du système d'administration à distance Kaspersky Security Center.
- klmdminst.exe — fichier d'installation du plug-in d'administration de Kaspersky Mobile Device Management for Mobile à l'aide du système d'administration à distance Kaspersky Security Center.
- KSM_10_5_11_xxx.apk : fichier d'installation de l'application mobile Kaspersky Endpoint Security 10 for Android.
- KSM_10_3_xx_fr.zip : fichier d'installation de l'application mobile Kaspersky Endpoint Security 10 for iOS.
- sms_utility_10.1.25fr.apk : utilitaire Kaspersky SMS Broadcasting.
- SigningUtility.zip : archive contenant l'utilitaire de signature de la distribution de l'application mobile et des conteneurs pour les appareils iOS.
- paquet de documentation:
  - Manuel de l'administrateur de la solution complète Kaspersky Security for Mobile ;
  - aide contextuelle du plug-in d'administration de Kaspersky Endpoint Security 10 for Mobile;
  - aide contextuelle du plug-in d'administration de Kaspersky Mobile Device Management ;
  - aide contextuelle de l'application mobile Kaspersky Endpoint Security 10 for Android.

CONFIGURATIONS LOGICIELLES ET MATERIELLES

Kaspersky Endpoint Security requiert les configurations matérielle et logicielle suivantes :

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, reportez-vous au *Manuel de l'administrateur du Kaspersky Security Center*.

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

- Kaspersky Security Center 10 Service Pack 1;
- Serveur de gestion des appareils mobiles Exchange ActiveSync ;
- Serveur de gestion des appareils mobiles iOS MDM.

Pour le déploiement du plug-in d'administration de Kaspersky Endpoint Security, l'ordinateur de l'administrateur doit satisfaire aux exigences logicielles suivantes : Kaspersky Security Center 10.0.

Pour le déploiement des applications mobiles de Kaspersky Endpoint Security, l'ordinateur de l'administrateur doit satisfaire les prérequis logiciels suivants :

- Pour le déploiement sur les appareils Android :
  - Kaspersky Security Center 10.0 ;
  - utilitaire Kaspersky SMS Broadcasting.
- Pour le déploiement sur les appareils iOS :
  - Kaspersky Security Center 10.0 ;
  - Serveur de gestion des appareils mobiles iOS MDM ;
  - utilitaire Kaspersky SMS Broadcasting ;
  - utilitaire Key Chain Access.

Pour déployer l'application mobile Kaspersky Safe Browser for iOS via le Serveur des appareils mobiles iOS MDM, vous devrez créer un identifiant Apple séparé sur le site d'Apple https://appleid.apple.com et participer au programme Apple Developer Program ou Apple Developer Enterprise Program. La participation à Apple Developer Program permet d'installer Kaspersky Safe Browser for Mobile sur un maximum de 100 appareils par an. La participation à Apple Developer Entreprise Program permet chaque année d'installer Kaspersky Safe Browser sur un nombre illimité d'appareils de votre entreprise.

La signature de la distribution de l'application Kaspersky Safe Browser for iOS et des applications mobiles tierces du conteneur implique que l'administrateur possède un ordinateur répondant à la configuration logicielle suivante :

- Mac OS X 10.6.6 ou supérieur, Mac OS X 10.7, OS X 10.8 ;
- iPhone Configuration Utility 3.5 ou supérieur pour Mac ou iPhone Configuration Utility 3.6.2 ou supérieur pour Windows.

Pour le déploiement des applications mobiles de Kaspersky Endpoint Security sur les appareils administrés par le protocole Exchange ActiveSync, l'ordinateur de l'administrateur doit répondre à la configuration logicielle suivante :

- Kaspersky Security Center 10.0 ;
- Serveur de gestion des appareils mobiles Exchange ActiveSync.

L'installation des applications mobiles de Kaspersky Endpoint Security s'exécute sur les appareils mobiles des utilisateurs administrés par les systèmes d'exploitation suivants :

- Android 2.3, 3.0, 3.1, 3.2, 4.0, 4.1, 4.2, 4.3, 4.4, 5.0.
- Apple iOS 7.0, 7.1, 8.
- Windows Phone 8.1.

ARCHITECTURE DE L'APPLICATION

Cette section décrit les modules de Kaspersky Endpoint Security et leur interaction.

DANS CETTE SECTION

PRESENTATION DU PLUG-IN D'ADMINISTRATION DE KASPERSKY ENDPOINT SECURITY

Le plug-in d'administration de Kaspersky Endpoint Security assure l'administration par interface des appareils 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 appareils mobiles ;
- configurer à distance les applications de Kaspersky Endpoint Security sur les appareils 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 des utilisateurs.

Pour en savoir plus sur l'utilisation des plug-ins d'administration dans le Kaspersky Security Center, reportez-vous au *Manuel de l'administrateur du Kaspersky Security Center*.

PRESENTATION DU PLUG-IN D'ADMINISTRATION DE KASPERSKY MOBILE DEVICE MANAGEMENT

Le plug-in d'administration de Kaspersky Mobile Device Management fournit une interface d'administration des appareils mobiles via la Console d'administration du Kaspersky Security Center. Le plug-in d'administration de Kaspersky Mobile Device Management vous permet d'exécuter les actions suivantes :

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

Pour en savoir plus sur l'utilisation des plug-ins d'administration dans le Kaspersky Security Center, reportez-vous au *Manuel de l'administrateur du Kaspersky Security Center*.

PRESENTATION DES APPLICATIONS MOBILES DE KASPERSKY ENDPOINT SECURITY

Les applications mobiles de Kaspersky Endpoint Security peuvent être installées sur les appareils mobiles Android, iOS, Windows Phone. Les applications mobiles de Kaspersky Endpoint Security assurent la protection des appareils mobiles contre les virus ou autres programmes présentant un menace, les appels et SMS indésirables, et les menaces Internet. Les applications mobiles de Kaspersky Endpoint Security permettent également de contrôler l'activité réseau de l'utilisateur et de protéger les données confidentielles contre tout accès non autorisé. Plusieurs modules d'applications sont conçus pour assurer la protection contre les différentes menaces. Cela permet de configurer de manière flexible les paramètres des applications mobiles en fonction des besoins d'un utilisateur particulier.

La section ci-dessous décrit les modules de chaque application mobile entrant de le paquet d'applications mobiles Kaspersky Endpoint Security.

Application mobile Kaspersky Endpoint Security for Android

Application dédiée à la protection des appareils Android. L'application comprend les modules suivants :

- **Anti-Virus**. Ce composant permet de détecter et de neutraliser les menaces sur l'appareil mobile à l'aide des bases antivirus de l'application et du service en nuage de Kaspersky Security Network. L'Anti-Virus présente les composants suivants :
  - La **protection** permet de découvrir les menaces dans les fichiers ouverts, d'analyser les nouvelles applications et de prévenir l'infection de l'appareil en temps réel.
  - 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 de l'appareil tandis que l'analyse d'un dossier porte sur un dossier en particulier. L'analyse complète et l'analyse d'un dossier détectent les menaces dans les fichiers installés 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.
  - La **mise à jour** permet de télécharger les nouvelles bases antivirus de l'application.
- **Antivol**. Ce composant protège les informations de l'appareil contre tout accès non autorisé en cas de perte ou de vol de l'appareil. Le module permet de verrouiller et de localiser l'appareil, ou de supprimer à distance les données de celui-ci à l'aide d'un SMS ou du Kaspersky Security Center.
- **Filtre des appels et SMS**. Module qui permet de bloquer les SMS et les appels entrants indésirables en fonction du mode sélectionné. Le filtrage des SMS et des appels entrants s'effectue à l'aide des listes de contacts autorisés et interdits. Le module permet de bloquer ou de transmettre les SMS et les appels entrants provenant des contacts interdits ou autorisés. Selon le mode sélectionné, le module permet également de transmettre les appels et SMS entrants provenant de tous les numéros du répertoire de l'appareil (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 module 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) pour obtenir un accès à leurs comptes bancaires. Le composant analyse les sites Internet avant leur ouverture à l'aide du service en nuage de Kaspersky Security Network. A l'issue de l'analyse, la Protection Internet ouvre le site considéré comme inoffensif et bloque le site considéré comme malveillant. Ce module prend également en charge le filtrage des sites Internet en fonction des catégories définies dans Kaspersky Security Network, ce qui permet par exemple à l'administrateur de limiter l'accès aux pages Internet reprises dans la catégorie « Jeux de hasard » ou « Réseaux sociaux ».
- **Conteneurs**. Contrôle l'activité des applications lancées sur l'appareil mobile de l'utilisateur. Ce module permet de placer une application tierce dans une enveloppe spéciale. Cette enveloppe permet de contrôler les actions des applications qu'elle comporte tout en protégeant les données personnelles et professionnelles figurant dans l'appareil de l'utilisateur. Le module permet de configurer les paramètres de chiffrement des données de l'application dans le conteneur et l'autorisation de l'utilisateur lors du lancement d'une application. Il contrôle également la transmission de données à d'autres applications et restreint l'accès des applications à Internet.

Vous pouvez indiquer si les applications des conteneurs sont recommandées ou requises sur les appareils des utilisateurs.

- **Gestion de l'appareil**. Permet de configurer l'utilisation obligatoire du mot de passe pour déverrouiller l'appareil mobile et la longueur minimale de ce mot de passe. Le module permet d'interdire l'utilisation des réseaux Wi-Fi, de l'appareil photo ou du module Bluetooth sur l'appareil et de configurer le profil TouchDown. Il permet également de configurer les paramètres de connexion de l'appareil mobile au réseau sans fil via Kaspersky Security Center.

- **Contrôle des applications**. Le composant permet de configurer à l'aide de Kaspersky Security Center les paramètres de lancement des applications sur l'appareil mobile de l'utilisateur. Vous pouvez indiquer des applications dont l'installation est requise ou recommandée sur l'appareil de l'utilisateur, et créer des listes d'applications dont le lancement est autorisé ou interdit. Ce module bloque toute tentative de lancement d'applications interdites et consigne les informations sur les tentatives d'accès dans les rapports du Kaspersky Security Center. Il prend également en charge l'utilisation de conteneurs (enveloppes spéciales pour les applications mobiles permettant de contrôler les activités des applications qu'elles incluent). Vous pouvez indiquer si les applications des conteneurs sont recommandées ou requises sur les appareils des utilisateurs.

- **Contrôle de la conformité à la stratégie de sécurité corporative**. Permet de détecter les infractions aux exigences à la sécurité corporative sur les appareils mobiles des utilisateurs et d'imposer des restrictions sur les appareils en cas de non conformité aux paramètres définis.

- **Quarantaine**. Place dans un stockage spécial et isolé les fichiers qui ont été détectés lors de l'analyse de l'appareil ou au cours du fonctionnement normal de la protection. La quarantaine compacte les fichiers avant leur isolement afin de protéger votre appareil. Ce module 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 l'appareil mobile de l'utilisateur. Ce module regroupe les rapports dès leur création. Les rapports peuvent conserver un maximum de 200 entrées. Lorsque le nombre d'entrées dépasse 200, le module remplace les entrées les plus anciennes par les entrées les plus récentes.

- **Avancé**. Permet de configurer les paramètres avancés de Kaspersky Endpoint Security : notifications contextuelles sur l'application, notifications sonores sur les événements, widget sur l'écran principal de l'appareil. Ce module permet de déchiffrer les données qui sont restées chiffrées après la désactivation du chiffrement dans les conteneurs, de recevoir des certificats d'accès aux ressources du réseau de l'entreprise et de supprimer Kaspersky Endpoint Security de l'appareil mobile. Il permet également de recevoir des informations sur la licence et des informations d'ordre général sur Kaspersky Endpoint Security.

- **Administration des appareils Samsung**. Permet de configurer via Kaspersky Security Center les paramètres du point d'accès (APN) et du Pare-feu, ainsi que les paramètres de connexion de l'appareil mobile à un réseau privé virtuel (VPN) et au serveur de messagerie Exchange. La configuration des paramètres est disponible pour les appareils Android Samsung prenant en charge l'utilisation de Samsung KNOX.

Application mobile de Kaspersky Safe Browser for iOS

L'application est protégée par le navigateur Internet pour les appareils iOS. Cette application assure un accès sécurisé à Internet à partir des appareils iOS connectés au réseau de l'entreprise. L'application comporte les modules suivants :

- **Protection Internet**. Permet de bloquer les sites Internet malveillants dont le but est de diffuser un code nuisible. Ce module 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) pour obtenir un accès à leurs comptes bancaires. Le composant analyse les sites Internet avant leur ouverture à l'aide du service en nuage de Kaspersky Security Network. A l'issue de l'analyse, la Protection Internet ouvre le site considéré comme inoffensif et bloque le site considéré comme malveillant. Ce module prend également en charge le filtrage des sites Internet en fonction des catégories définies dans Kaspersky Security Network, ce qui permet par exemple à l'administrateur de limiter l'accès aux pages Internet reprises dans la catégorie « Jeux de hasard » ou « Réseaux sociaux ».

- **Conteneurs**. Contrôle l'activité des applications lancées sur l'appareil mobile de l'utilisateur. Ce module place l'application tierce dans une enveloppe spéciale qui permet de contrôler les actions des applications qu'elle comporte tout en protégeant les données personnelles et professionnelles figurant dans l'appareil de l'utilisateur. Le module permet de configurer les paramètres de chiffrement des données de l'application dans le conteneur et l'autorisation de l'utilisateur lors du lancement d'une application. Il contrôle également la transmission de données à d'autres applications et restreint l'accès des applications à Internet.

Application mobile de Kaspersky Safe Browser for Windows Phone

L'application est protégée par le navigateur Internet pour les appareils Windows Phone. Cette application assure un accès sécurisé à Internet à partir des appareils Windows Phone connectés au réseau de l'entreprise. L'application comporte les modules suivants :

- **Protection Internet**. Permet de bloquer les sites Internet malveillants dont le but est de diffuser un code nuisible. Ce module 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) pour obtenir un accès à leurs comptes bancaires. Le composant analyse les sites Internet avant leur ouverture à l'aide du service en nuage de Kaspersky Security Network. A l'issue de l'analyse, la Protection Internet ouvre le site considéré comme inoffensif et bloque le site considéré comme malveillant. Ce module prend également en charge le filtrage des sites Internet en fonction des catégories définies dans Kaspersky Security Network, ce qui permet par exemple à l'administrateur de limiter l'accès aux pages Internet reprises dans la catégorie « Jeux de hasard » ou « Réseaux sociaux ».

- **Antivol**. Ce composant protège les informations de l'appareil contre tout accès non autorisé en cas de perte ou de vol de l'appareil. Le composant permet de localiser l'appareil mobile à l'aide d'un SMS ou à l'aide de Kaspersky Security Center.

Pour en savoir plus sur l'utilisation des applications mobiles de Kaspersky Endpoint Security dans le Kaspersky Security Center, reportez-vous au *Manuel de l'administrateur du Kaspersky Security Center*.

SCHEMAS TYPES DE DEPLOIEMENT DE LA SOLUTION COMPLETE

Cette section décrit les schémas typiques de déploiement de la solution complète Kaspersky Security for Mobile :

- schéma de déploiement du plug-in d'administration de Kaspersky Endpoint Security (cf. page 22) ;
- schéma de déploiement du plug-in d'administration de Kaspersky Mobile Device Management (cf. page 19) ;
- schéma de déploiement de l'application mobile Kaspersky Endpoint Security for Android (cf. page 23) ;
- schéma de déploiement de l'application mobile Kaspersky Safe Browser for iOS (cf. page 27) ;
- schéma de déploiement de l'application mobile Kaspersky Safe Browser for Windows Phone (cf. page 29).

SCHEMA DE DEPLOIEMENT DU PLUG-IN D'ADMINISTRATION DE KASPERSKY ENDPOINT SECURITY

Le schéma de déploiement du plug-in d'administration comprend les étapes suivantes :

1. Préparation de l'installation du plug-in de Kaspersky Endpoint Security for Mobile.

   a. Mise à jour de la version du composant Serveur d'Administration (cf. section "Mise à jour de la version du composant Serveur d'Administration" à la page 31).

   b. Configuration de l'interface de la Console d'administration de Kaspersky Security Center.

   c. Création des groupes d'administration pour les appareils mobiles faisant partie des ordinateurs gérés dans le système Kaspersky Security Center. Les appareils équipés de l'application Kaspersky Endpoint Security seront placés dans ces groupes manuellement ou selon des règles de transfert automatique.

2. Installation du plug-in de Kaspersky Endpoint Security for Mobile (cf. section "Installation du plug-in de Kaspersky Endpoint Security for Mobile" à la page 41).

SCHEMA DE DEPLOIEMENT DU PLUG-IN D'ADMINISTRATION DE KASPERSKY MOBILE DEVICE MANAGEMENT

Le schéma de déploiement comprend les étapes suivantes :

1. Préparation de l'installation du plug-in de Kaspersky Mobile Device Management.

   a. Mise à jour de la version du composant Serveur d'Administration (cf. section "Mise à jour de la version du composant Serveur d'Administration" à la page 31).

   b. Configuration de l'interface de la Console d'administration de Kaspersky Security Center.

   c. Création des groupes d'administration pour les appareils mobiles faisant partie des ordinateurs gérés dans le système Kaspersky Security Center. Les appareils équipés de l'application Kaspersky Endpoint Security seront placés dans ces groupes manuellement ou selon des règles de transfert automatique.

2. Installation du plug-in de Kaspersky Mobile Device Management (cf. section "Installation du plug-in d'administration des appareils EAS et iOS MDM" à la page 41).

SCHEMAS DE DEPLOIEMENT DE L'APPLICATION MOBILE KASPERSKY ENDPOINT SECURITY FOR ANDROID

L'installation de l'application mobile Kaspersky Endpoint Security sur les appareils Android peut s'effectuer de l'une des manières suivantes :

- via l'envoi aux utilisateurs de messages de courrier électronique comportant un lien vers le programme d'installation de l'application mobile ;
- via l'envoi aux utilisateurs de SMS comportant un lien vers la distribution de l'application mobile ;
- via les stations de travail auxquelles les utilisateurs connectent leurs appareils mobiles ;
- via Google Play, où l'utilisateur télécharge lui-même le programme d'installation de la même façon qu'une application Android standard.

DANS CETTE SECTION

SCHEMA DE DEPLOIEMENT VIA L'ENVOI DE SMS

Le schéma de déploiement de l'application mobile Kaspersky Endpoint Security for Android via l'envoi de SMS permet d'envoyer aux utilisateurs une distribution contenant les paramètres de connexion de l'appareil au Serveur d'administration. Lors de l'application mobile, les utilisateurs n'ont pas besoin d'indiquer manuellement les paramètres de la connexion.

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

Le schéma de déploiement comprend les étapes suivantes :

1. Préparation de l'installation de l'application mobile :

   a. Installation dans Kaspersky Security Center du composant Prise en charge des appareils mobiles. Cette étape correspond à la création du certificat du Serveur d'administration des appareils mobiles.

   b. Mise à jour de la version du composant Serveur d'administration.

   c. Configuration de l'interface de la Console d'administration de Kaspersky Security Center.

   d. Configuration des paramètres de connexion des appareils mobiles. Cette étape correspond à la configuration des paramètres de connexion des appareils mobiles dans les propriétés du Serveur d'administration pour garantir la synchronisation des appareils mobiles avec le Serveur d'administration.

   e. Création des groupes d'administration pour les appareils mobiles faisant partie des ordinateurs gérés dans le système Kaspersky Security Center. Les appareils équipés de l'application Kaspersky Endpoint Security seront placés dans ces groupes manuellement ou selon des règles de transfert automatique.

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

   g. Installation du plug-in d'administration de Kaspersky Endpoint Security sur le poste de travail de l'administrateur.

   h. Configuration du mode d'envoi de SMS aux utilisateurs.

   i. Création du paquet d'installation pour l'installation à distance de Kaspersky Endpoint Security 10 for Mobile.

   j. Configuration des paramètres du paquet d'installation pour l'installation à distance de Kaspersky Endpoint Security 10 for Mobile.

   k. Création du paquet autonome d'installation pour Kaspersky Endpoint Security 10 for Mobile. Le paquet autonome inclut les paramètres de connexion au Serveur d'administration. Le paquet autonome est disponible dans le dossier partagé et sur le serveur Internet du Kaspersky Security Center. Lors de la création de l'envoi SMS, vous devez sélectionner le chemin d'accès au serveur Internet du Kaspersky Security Center.

   l. Création d'un certificat commun pour le compte de l'utilisateur (cf. page 39). Cette étape permet d'éditer un certificat rattaché au compte d'un utilisateur d'appareils mobiles en vue de son identification.

2. Installation de l'application mobile sur les appareils.

    a. Composition et envoi aux utilisateurs d'appareils mobiles d'un SMS avec un lien vers le paquet autonome d'installation.

    b. Téléchargement du paquet autonome d'installation sur l'appareil mobile. Cette étape permet à l'utilisateur de télécharger sur l'appareil la distribution préparée de l'application mobile sur le serveur Internet de Kaspersky Security Center.

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

    d. Téléchargement du certificat commun sur l'appareil mobile de l'utilisateur. Cette étape permet à l'utilisateur de télécharger sur son appareil le certificat qui lui a été créé.

3. Préparation de l'application mobile au fonctionnement sur l'appareil :

    a. Création d'une stratégie de groupe pour l'administration des paramètres de Kaspersky Endpoint Security.

    b. Activation de l'application sur les appareils mobiles des utilisateurs.

SCHEMA DE DEPLOIEMENT VIA LE POSTE DE TRAVAIL

Le déploiement de l'application mobile Kaspersky Endpoint Security for Android via le poste de travail s'utilise lorsque les utilisateurs connectent les appareils mobiles aux ordinateurs de bureau.

Le schéma de déploiement comprend les étapes suivantes :

1. Préparation de l'installation de l'application mobile :

    a. Installation dans Kaspersky Security Center du composant Prise en charge des appareils mobiles. Cette étape correspond à la création du certificat du Serveur d'administration des appareils mobiles.

    b. Mise à jour de la version du composant Serveur d'administration.

    c. Configuration de l'interface de la Console d'administration de Kaspersky Security Center.

    d. Configuration des paramètres de connexion des appareils mobiles. Cette étape correspond à la configuration des paramètres de connexion des appareils mobiles dans les propriétés du Serveur d'administration pour garantir la synchronisation des appareils mobiles avec le Serveur d'administration.

    e. Création des groupes d'administration pour les appareils mobiles faisant partie des ordinateurs gérés dans le système Kaspersky Security Center. Les appareils équipés de l'application Kaspersky Endpoint Security seront placés dans ces groupes manuellement ou selon des règles de transfert automatique.

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

    g. Installation du plug-in d'administration de Kaspersky Endpoint Security sur le poste de travail de l'administrateur.

    h. Création du paquet d'installation pour l'installation à distance de Kaspersky Endpoint Security 10 for Mobile.

    i. Configuration des paramètres du paquet d'installation pour l'installation à distance de Kaspersky Endpoint Security 10 for Mobile.

2. Installation de l'application mobile sur les appareils.

    a. La création de la tâche d'installation à distance permet de transmettre la distribution de l'application Kaspersky Endpoint Security for Android aux postes de travail des utilisateurs et d'installer l'utilitaire d'envoi de la distribution sur les appareils mobiles.

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

c. Installation de l'application sur l'appareil mobile. Cette étape permet à l'utilisateur d'installer l'application sur l'appareil mobile.

3. Préparation de l'application mobile au fonctionnement sur l'appareil :

   a. Création d'une stratégie de groupe pour l'administration des paramètres de Kaspersky Endpoint Security.

   b. Activation de l'application sur les appareils mobiles des utilisateurs.

SCHEMA DE DEPLOIEMENT VIA GOOGLE PLAY

Le déploiement via Google Play est possible au cas où il serait plus pratique pour l'utilisateur de télécharger et d'installer lui-même la distribution de l'application mobile à partir de Google Play.

Le déploiement de l'application via Google Play ne demande pas de création de la distribution avec les paramètres de connexion au serveur d'administration. L'utilisateur indique lui-même les paramètres de connexion au Serveur d'administration dès le premier lancement de l'application mobile sur l'appareil.

Le schéma de déploiement comprend les étapes suivantes :

1. Préparation de l'installation de l'application mobile :

   a. Installation dans Kaspersky Security Center du composant Prise en charge des appareils mobiles. Cette étape correspond à la création du certificat du Serveur d'administration des appareils mobiles.

   b. Mise à jour de la version du composant Serveur d'administration.

   c. Configuration de l'interface de la Console d'administration de Kaspersky Security Center.

   d. Configuration des paramètres de connexion des appareils mobiles. Cette étape correspond à la configuration des paramètres de connexion des appareils mobiles dans les propriétés du Serveur d'administration pour garantir la synchronisation des appareils mobiles avec le Serveur d'administration.

   e. Création des groupes d'administration pour les appareils mobiles faisant partie des ordinateurs gérés dans le système Kaspersky Security Center. Les appareils équipés de l'application Kaspersky Endpoint Security seront placés dans ces groupes manuellement ou selon des règles de transfert automatique.

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

   g. Installation du plug-in d'administration de Kaspersky Endpoint Security sur le poste de travail de l'administrateur.

   h. Création d'un certificat commun pour le compte de l'utilisateur (cf. page 39). Cette étape permet d'éditer un certificat rattaché au compte d'un utilisateur d'appareils mobiles en vue de son identification.

2. Installation de l'application mobile sur les appareils. Cette étape permet à l'utilisateur d'installer l'application et de télécharger le certificat sur son appareil mobile.

3. Préparation de l'application mobile au fonctionnement sur l'appareil :

   a. Création d'une stratégie de groupe pour l'administration des paramètres de Kaspersky Endpoint Security.

   b. Activation de l'application sur les appareils mobiles des utilisateurs.

   c. Configuration initiale de l'application. Dans le cadre de cette étape, l'utilisateur définit les paramètres de connexion de l'appareil mobile au Serveur d'administration.

SCHEMAS DE DEPLOIEMENT DE L'APPLICATION MOBILE KASPERSKY SAFE BROWSER FOR IOS

L'installation de l'application mobile Kaspersky Safe Browser for iOS sur les appareils peut être effectuée aussi bien par l'administrateur lors de la connexion des appareils iOS au Serveur des appareils mobiles iOS MDM, que par l'utilisateur lui-même en téléchargeant l'application mobile depuis l'Apple Store.

DANS CETTE SECTION

SCHEMA DE DEPLOIEMENT VIA LE SERVEUR DE GESTION DES APPAREILS MOBILES IOS MDM

Pour l'installation de l'application mobile Kaspersky Endpoint Security for iOS sur les appareils mobiles des utilisateurs, il est nécessaire que le Serveur de gestion des appareils mobiles iOS MDM soit déployé dans le Kaspersky Security Center. Le serveur de gestion des appareils mobiles iOS MDM fait partie des paquets d'installation du Serveur d'administration du Kaspersky Security Center, si la licence acquise couvre la fonctionnalité Administration des appareils mobiles. Le Serveur d'administration gère les appareils mobiles iOS à l'aide du Serveur des appareils mobiles iOS MDM. L'administration centralisée des paramètres de l'application mobile est effectuée à l'aide des stratégies appliquées aux groupes des appareils gérés.

Pour en savoir plus sur l'installation du serveur de gestion des appareils mobiles iOS MDM, consultez le *Manuel d'implantation du Kaspersky Security Center*.

Le schéma de déploiement comprend les étapes suivantes :

1. Préparation de l'installation de l'application mobile :
   a. Installation dans Kaspersky Security Center du composant Prise en charge des appareils mobiles. Cette étape correspond à la création du certificat du Serveur d'administration des appareils mobiles.
   b. Mise à jour de la version du composant Serveur d'administration.
   c. Configuration de l'interface de la Console d'administration de Kaspersky Security Center.
   d. Configuration des paramètres de connexion des appareils mobiles. Cette étape correspond à la configuration des paramètres de connexion des appareils mobiles dans les propriétés du Serveur d'administration pour garantir la synchronisation des appareils mobiles avec le Serveur d'administration.
   e. Création des groupes d'administration pour les appareils mobiles faisant partie des ordinateurs gérés dans le système Kaspersky Security Center. Les appareils équipés de l'application Kaspersky Endpoint Security seront placés dans ces groupes manuellement ou selon des règles de transfert automatique.
   f. Création des règles de déplacement automatique des appareils mobiles dans le groupe.
   g. Installation du plug-in d'administration de Kaspersky Endpoint Security sur le poste de travail de l'administrateur.
   h. Création d'un certificat commun pour le compte de l'utilisateur (cf. page 39). Cette étape permet d'éditer un certificat rattaché au compte d'un utilisateur d'appareils mobiles en vue de son identification.

2. Installation de l'application mobile sur les appareils.

    a. Réception du Apple Push Notification Certificate (ci-après, le certificat APN).

    b. Installation du certificat APN sur le Serveur de gestion des appareils mobiles iOS MDM.

    c. Création du profil iOS MDM et distribution de celui-ci sur les appareils des utilisateurs.

    d. Réception du certificat Developer Certificate.

    e. Création du profil d'approvisionnement qui autorise l'installation d'applications mobiles tierces sur les appareils des utilisateurs.

    f. Signature de la distribution de l'application.

    g. Installation de l'application mobile sur les appareils. Cette étape permet à l'utilisateur d'installer l'application sur son appareil mobile et de télécharger le certificat qui lui a été établi. (cf. section "Installation de l'application mobile sur l'appareil" à la page 51)

3. Préparation de l'application mobile au fonctionnement sur l'appareil :

    a. Création d'une stratégie de groupe pour l'administration des paramètres de Kaspersky Endpoint Security.

    b. Activation de l'application sur les appareils mobiles des utilisateurs.

    c. Configuration initiale de l'application mobile sur les appareils des utilisateurs. À cette étape, l'utilisateur indique les paramètres de connexion au Serveur d'administration.

SCHEMA DE DEPLOIEMENT VIA L'APPLE STORE

Le déploiement via l'Apple Store est possible au cas où il serait plus pratique pour l'utilisateur de télécharger et d'installer lui-même la distribution de l'application mobile à partir de l'Apple Store.

Le déploiement de l'application via l'Apple Store n'implique pas la création de la distribution avec les paramètres de connexion au serveur d'administration. L'utilisateur indique lui-même les paramètres de connexion au Serveur d'administration dès le premier lancement de l'application mobile sur l'appareil.

Le schéma de déploiement comprend les étapes suivantes :

1. Préparation de l'installation de l'application mobile :

    a. Installation dans Kaspersky Security Center du composant Prise en charge des appareils mobiles. Cette étape correspond à la création du certificat du Serveur d'administration des appareils mobiles.

    b. Mise à jour de la version du composant Serveur d'administration.

    c. Configuration de l'interface de la Console d'administration de Kaspersky Security Center.

    d. Configuration des paramètres de connexion des appareils mobiles. Cette étape correspond à la configuration des paramètres de connexion des appareils mobiles dans les propriétés du Serveur d'administration pour garantir la synchronisation des appareils mobiles avec le Serveur d'administration.

    e. Création des groupes d'administration pour les appareils mobiles faisant partie des ordinateurs gérés dans le système Kaspersky Security Center. Les appareils équipés de l'application Kaspersky Endpoint Security seront placés dans ces groupes manuellement ou selon des règles de transfert automatique.

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

    g. Installation du plug-in d'administration de Kaspersky Endpoint Security sur le poste de travail de l'administrateur.

    h. Création d'un certificat commun pour le compte de l'utilisateur (cf. page 39). Cette étape permet d'éditer un certificat rattaché au compte d'un utilisateur d'appareils mobiles en vue de son identification.

2. Installation de l'application mobile sur les appareils. Cette étape permet à l'utilisateur d'installer l'application sur son appareil mobile et de télécharger le certificat qui lui a été établi.

3. Préparation de l'application mobile au fonctionnement sur l'appareil :

   a. Création d'une stratégie de groupe pour l'administration des paramètres de Kaspersky Endpoint Security.

   b. Activation de l'application sur les appareils mobiles des utilisateurs.

   c. Configuration initiale de l'application. Dans le cadre de cette étape, l'utilisateur définit les paramètres de connexion de l'appareil mobile au Serveur d'administration.

SCHEMA DE DEPLOIEMENT DE L'APPLICATION MOBILE KASPERSKY SAFE BROWSER FOR WINDOWS PHONE

L'installation de l'application mobile Kaspersky Safe Browser for Windows Phone implique que l'utilisateur télécharge lui-même la distribution de l'application mobile à partir du site Internet de la boutique Windows Phone et qu'il l'installe sur l'appareil. Il n'est pas nécessaire de créer la distribution de l'application avec les paramètres de connexion de l'appareil au Serveur d'administration.

Le schéma de déploiement comprend les étapes suivantes :

1. Préparation de l'installation de l'application mobile :

   a. Installation dans Kaspersky Security Center du composant Prise en charge des appareils mobiles. Cette étape correspond à la création du certificat du Serveur d'administration des appareils mobiles.

   b. Mise à jour de la version du composant Serveur d'administration.

   c. Configuration de l'interface de la Console d'administration de Kaspersky Security Center.

   d. Configuration des paramètres de connexion des appareils mobiles. Cette étape correspond à la configuration des paramètres de connexion des appareils mobiles dans les propriétés du Serveur d'administration pour garantir la synchronisation des appareils mobiles avec le Serveur d'administration.

   e. Création des groupes d'administration pour les appareils mobiles faisant partie des ordinateurs gérés dans le système Kaspersky Security Center. Les appareils équipés de l'application Kaspersky Endpoint Security seront placés dans ces groupes manuellement ou selon des règles de transfert automatique.

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

   g. Installation du plug-in d'administration de Kaspersky Endpoint Security sur le poste de travail de l'administrateur.

2. Installation de l'application mobile sur les appareils. Cette étape permet à l'utilisateur d'installer l'application sur son appareil mobile.

3. Préparation de l'application mobile au fonctionnement sur l'appareil :

   a. Création d'une stratégie de groupe pour l'administration des paramètres de Kaspersky Endpoint Security.

   b. Activation de l'application sur les appareils mobiles des utilisateurs.

   c. Configuration initiale de l'application. Dans le cadre de cette étape, l'utilisateur définit les paramètres de connexion de l'appareil mobile au Serveur d'administration.

PREPARATIFS DU DEPLOIEMENT DE LA SOLUTION COMPLETE

Avant de déployer la solution complète Kaspersky Security for Mobile, il est nécessaire de s'assurer que les conditions suivantes sont remplies :

1. Les modules de Kaspersky Security Center sont installés sur le réseau de l'entreprise : le Serveur d'administration et la Console d'administration. Afin d'administrer les appareils iOS MDM et les appareils EAS, le Serveur des appareils mobiles iOS MDM et le Serveur des appareils mobiles Exchange ActiveSync doivent être installés (cf. *Manuel de déploiement de Kaspersky Security Center*).

2. Les modules de Kaspersky Security Center installés sont conformes à la configuration système requise pour le déploiement de la solution complète Kaspersky Security for Mobile. Si la version du Serveur d'administration n'est pas conforme aux pré-requis, vous devrez supprimer l'ancienne version du module et installer la version spécifiée dans les pré-requis système après avoir effectué une copie de sauvegarde des données du Serveur d'administration.

3. Le module Prise en charge des appareils mobiles est installé. Ce module assure l'administration des appareils mobiles via le Kaspersky Security Center. Le module Prise en charge des appareils mobiles est installé en même temps que le Serveur d'administration.

   Si le module Prise en charge des appareils mobiles n'a pas été installé ou si la version du Serveur d'administration n'est pas conforme à la configuration système requise pour le déploiement de la solution complète Kaspersky Security for Mobile, l'administrateur doit supprimer l'ancienne version du Serveur d'administration et installer la version spécifiée dans les pré-requis système après avoir effectué une copie de sauvegarde des données du Serveur d'administration.

4. Les appareils EAS sont connectés au Serveur des appareils mobiles Exchange ActiveSync et les appareils iOS MDM sont connectés au Serveur iOS MDM *(cf. Manuel de l'administrateur de Kaspersky Security Center)*.

DANS CETTE SECTION

INSTALLATION DU MODULE PRISE EN CHARGE DES APPAREILS MOBILES

L'administration des appareils mobiles via le Kaspersky Security Center s'appuie sur le module Prise en charge des appareils mobiles. Le module Prise en charge des appareils mobiles s'installe lors de l'installation du Serveur d'administration (à l'étape **Sélection des modules**, il faut impérativement cocher la case **Prise en charge des appareils mobiles**).

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

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

MISE A JOUR DE LA VERSION DU COMPOSANT SERVEUR D'ADMINISTRATION

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

Pour mettre à jour le Serveur d'administration, procédez comme suit :

1. Faites une copie de sauvegarde des données du Serveur d'administration (cf. *Manuel de l'administrateur du Kaspersky Security Center*).
2. Lancez l'assistant d'installation de la version du Serveur d'Administration conforme aux exigences logicielles de Kaspersky Endpoint Security 10 for Mobile.
3. A l'étape **Sélection des modules**, cochez la case **Prise en charge des appareils mobiles**.

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

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

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

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

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

1. Sélectionnez dans l'arborescence de la console le Serveur d'administration auquel seront connectés les appareils mobiles.
2. Dans le menu contextuel Serveur d'administration, choisissez l'option **Propriétés**.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.
3. Ouvrez la section **Paramètres**.
4. Dans le groupe **Paramètres de connexion au Serveur d'administration**, cochez la case **Ouvrir le port pour les appareils mobiles**.
5. Dans le champ **Port pour les appareils mobiles**, spécifiez le port que les appareils 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 appareils mobiles** est décochée ou qu'un port invalide a été indiqué pour la connexion, les appareils mobiles ne pourront pas se connecter au Serveur d'administration.

Affichage du dossier Appareils mobiles dans la Console d'administration

L'affichage du dossier **Appareils mobiles** dans la Console d'administration permet de consulter la liste des appareils mobiles gérés par le Serveur d'administration et de définir leurs paramètres d'administration.

*Pour activer l'affichage du dossier **Appareils mobiles** dans la Console d'administration, procédez comme suit :*

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

CONFIGURATION DE L'ENVOI DES SMS

Le déploiement des applications mobiles Kaspersky Endpoint Security sur les appareils des utilisateurs via un SMS nécessite de sélectionner la méthode d'envoi des SMS.

Il existe deux options d'envoi de masse des SMS aux utilisateurs via le Kaspersky Security Center :

- Via la passerelle de messagerie. Pour envoyer des SMS via la passerelle de messagerie, il est nécessaire de spécifier le serveur SMTP et le port dans les paramètres du Kaspersky Security Center.

  Pour en savoir plus sur l'envoi de SMS aux utilisateurs à l'aide du Kaspersky Security Center, reportez-vous au *Manuel de l'administrateur du Kaspersky Security Center*.

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

  Pour pouvoir utiliser l'appareil mobile comme expéditeur de tous les SMS en provenance du Kaspersky Security Center, vous devez installer l'utilitaire spécial Kaspersky SMS Broadcasting sur l'appareil. L'utilitaire Kaspersky SMS Broadcasting est installé sur l'appareil mobile en tant qu'application standard Android. Suite à son installation sur l'appareil, l'utilitaire Kaspersky SMS Broadcasting demande l'adresse et le port du Serveur d'administration du Kaspersky Security Center et se synchronise au Serveur d'administration. A l'issue de cette synchronisation, l'appareil s'affiche dans la Console d'administration, dans la section **Expéditeurs des SMS** de la fenêtre des propriétés du dossier **Rapports et notifications** figurant dans la liste des appareils susceptibles d'envoyer des SMS. Il est conseillé d'utiliser l'appareil mobile avec l'utilitaire Kaspersky SMS Broadcasting en tant qu'expéditeur des SMS, notamment si vous souhaitez recevoir des rapports sur la transmission de ces SMS.

  Pour en savoir plus sur l'obtention de l'utilitaire Kaspersky SMS Broadcasting et sur son installation sur l'appareil mobile, consultez la section relative à la configuration de l'envoi de SMS dans le *Manuel de déploiement du Kaspersky Security Center*.

Pour configurer l'envoi de SMS, procédez comme suit :

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

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

3. Dans la section **Notification** de la liste déroulante, sélectionnez le type de notification **SMS**.

4. Spécifiez l'option d'envoi des messages textes préférée:

   - Si vous souhaitez 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 SMPT.

   - Si vous souhaitez envoyer les SMS à partir de l'appareil mobile où est installé l'utilitaire Kaspersky SMS Broadcasting, sélectionnez l'option **Envoyer les SMS à l'aide de l'utilitaire Kaspersky SMS Broadcasting** et indiquez les paramètres d'envoi : numéros de téléphone des utilisateurs, texte de la notification.

Pour plus d'informations sur l'utilisation du Kaspersky Security Center pour l'envoi de SMS aux utilisateurs, reportez-vous au *Manuel d'administrateur du Kaspersky Security Center*.

CONFIGURATION DE L'ENVOI DES MESSAGES ELECTRONIQUES

Il est nécessaire de configurer les envois du Serveur d'administration pour le déploiement des applications mobiles Kaspersky Endpoint Security sur les appareils des utilisateurs via un message électronique.

Pour configurer l'envoi des notifications par e-mail, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration auquel vous souhaitez connecter les appareils mobiles.
2. Dans l'arborescence de la console, sélectionnez le dossier **Rapports et notifications**. Sélectionnez **Propriétés** dans le menu contextuel du dossier.
3. Dans la section **Notifications** de la liste déroulante, sélectionnez comme type de notification **E-mail**.
4. Dans le champ **Serveur SMTP**, spécifiez l'adresse du serveur de messagerie.

   Vous pouvez utiliser comme adresse l'adresse IP ou le nom de l'ordinateur dans le réseau Windows (nom NetBIOS).
5. Dans le champ **Port du serveur SMTP**, spécifiez le numéro du port de communication du serveur SMTP.

   Le port 25 est le port choisi par défaut.
6. Cliquez sur **Appliquer** pour que les modifications soient appliquées.

CREATION D'UN GROUPE D'ADMINISTRATION

La configuration centralisée des paramètres de l'application Kaspersky Endpoint Security installés sur les appareils 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 Kaspersky Endpoint Security sur les appareils des utilisateurs. Si vous installez les applications mobiles Kaspersky Endpoint Security via les postes de travail des utilisateurs, il vous est conseillé de créer des groupes d'administration dédiés pour les postes de travail.

Vous devez ensuite configurer le placement automatique dans ce groupe des appareils sur lesquels vous souhaitez installer Kaspersky Endpoint Security. Il faut ensuite définir les paramètres communs à l'ensemble des appareils à l'aide d'une stratégie de groupe.

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

1. Sélectionnez dans l'arborescence de la console le Serveur d'administration auquel les appareils mobiles sont connectés.
2. Dans l'arborescence de la console, sélectionnez le dossier **Ordinateurs administrés**.
3. Si vous souhaitez créer un sous-groupe pour un groupe d'administration existant, sélectionnez dans le dossier **Ordinateurs administrés** le sous-dossier dans lequel vous souhaitez créer un sous-groupe.
4. Lancez la procédure de création du groupe à l'aide de l'une des méthodes suivantes:

   - dans le menu contextuel du dossier **Ordinateurs administrés** ou dans le menu contextuel du sous-dossier, choisissez l'option **Créer → Groupe** ;
   - dans la zone de travail du dossier **Ordinateurs administrés** ou dans le sous-dossier, sélectionnez l'onglet **Groupes** et cliquez sur le lien **Créer un sous-groupe** pour ouvrir une fenêtre.
5. 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.

Si vous utilisez plusieurs postes de travail pour installer Kaspersky Endpoint Security sur des appareils mobiles, il vous est conseillé de créer un groupe pour postes de travail sur le Serveur d'administration et d'y placer ces postes de travail. Ensuite, vous pouvez créer pour ce groupe une tâche de groupe pour installer l'application Kaspersky Endpoint Security à distance. Cette opération vous permettra d'installer l'application simultanément via toutes les stations de travail faisant partie du groupe.

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

CREATION DES REGLES DU TRANSFERT AUTOMATIQUE DES APPAREILS DANS LE GROUPE D'ADMINISTRATION

L'administration centralisée des paramètres des applications Kaspersky Endpoint Security installées sur des appareils mobiles n'est possible que si ces appareils se trouvent dans un **groupe d'administration créé au préalable** du nœud Ordinateurs administrés pour lequel une stratégie de groupe a été définie.

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

L'administrateur peut créer une règle de transfert automatique des appareils mobiles depuis le dossier **Périphériques non définis** vers le groupe d'administration sélectionné du dossier **Ordinateurs administrés**.

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

1. Sélectionnez dans l'arborescence de la console le Serveur d'administration auquel les appareils mobiles sont connectés.

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

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

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

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

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

5. Dans la section **Général**, effectuez les actions suivantes:

   - Spécifiez le nom de la règle.

   - Indiquez le groupe d'administration vers lequel seront déplacés les appareils mobiles une fois que l'application mobile Kaspersky Endpoint Security 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.

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

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

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

- Dans la section **Programmes**, 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 appareils 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 appareils conformes aux critères définis depuis le dossier **Périphériques non définis** vers le groupe d'administration que vous avez indiqué. Les appareils 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 appareils non repartis, cf. *Manuel d'administrateur de Kaspersky Security Center*.

CREATION DU PAQUET D'INSTALLATION

Le paquet d'installation Kaspersky Endpoint Security 10 for Mobile est une archive auto-extractible sc_package.exe qui contient les fichiers pour l'installation des applications mobiles sur l'appareil :

- adb.exe, AdbWinApi.dll, AdbWinUsbApi.dll : ensemble des fichiers nécessaires à l'installation de l'application mobile Kaspersky Endpoint Security 10 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 10 for Android ;

- kmlisten.exe : utilitaire de distribution du paquet d'installation sur un appareil 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 10 for Mobile, procédez comme suit :

1. Sélectionnez dans l'arborescence de la console le Serveur d'administration auquel les appareils mobiles sont connectés.

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

3. 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.

4. 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**.

5. Dans la fenêtre de l'assistant **Sélection de la distribution de l'application à installer**, à l'aide du bouton **Sélectionner**, ouvrez le dossier où vous avez placé la distribution de l'application et sélectionnez l'archive auto-extractible sc_package.exe.

   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.

Avant d'utiliser le paquet d'installation ainsi créé pour l'application mobile Kaspersky Endpoint Security for Android, il est nécessaire de configurer les paramètres du paquet d'installation.

CONFIGURATION DU PAQUET D'INSTALLATION

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

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

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

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

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

4. Sous l'onglet **Paramètres**, indiquez les paramètres de connexion des appareils mobiles au Serveur d'administration et le nom du groupe d'administration où les appareils 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 appareils mobiles dans le format qui a été spécifié lors de l'installation du composant **Prise en charge des appareils mobiles** pendant le déploiement du Serveur d'administration.

     Selon le format du nom du Serveur d'administration pour le module **Prise en charge des appareils 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 crée 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 appareils mobiles lorsqu'ils sont ajoutés à un groupe d'administration. Le nom de l'appareil mobile sous Android est formé selon la règle <adresse e-mail de l'utilisateur (modèle de l'appareil mobile – device ID)>.

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

CREATION D'UN PAQUET AUTONOME D'INSTALLATION POUR KASPERSKY ENDPOINT SECURITY FOR ANDROID

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

1. Sélectionnez dans l'arborescence de la console le Serveur d'administration auquel les appareils mobiles sont connectés.

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

3. Spécifiez le paquet d'installation pour l'application Kaspersky Endpoint Security 10 for Mobile.

4. 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.

5. 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.

6. Si vous souhaitez ouvrir le dossier partagé : dans le groupe **Actions suivantes**, cliquez sur le lien **Ouvrir le dossier**.

7. Si vous souhaitez diffuser le chemin vers le paquet autonome d'installation aux utilisateurs par le biais d'un message électronique : 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.

8. Si vous souhaitez 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.

9. Si vous souhaitez 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. Elle comporte les informations suivantes :

   - liste des paquets autonomes d'installation ;
   - chemin réseau vers le dossier partagé dans le champ **Chemin** ;
   - 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.

CREATION D'UN CERTIFICAT COMMUN

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

Sous Android, il n'est possible de créer un certificat public qu'avec les appareils équipés d'une version Android 4.0 ou une version supérieure.

Pour créer un certificat commun, procédez comme suit :

1. Dans l'arborescence de la console du Kaspersky Security Center, sélectionnez l'entrée **Administration des appareils mobiles**.
2. A l'entrée **Administration des appareils mobiles**, sélectionnez le dossier **Certificats**.
3. Dans la zone de travail du dossier **Certificats**, cliquez sur le lien **Ajouter un certificat** pour lancer l'assistant d'installation de certificats.
4. Dans la fenêtre **Sélection de l'utilisateur** de l'assistant, indiquez les utilisateurs pour lesquels vous souhaitez créer un certificat commun.
5. Dans la fenêtre **Type de certificat** de l'assistant, sélectionnez l'option **Certificat commun**.
6. Dans la fenêtre **Source du certificat** de l'assistant, indiquez le mode de création du certificat commun.
   - Si vous souhaitez que le certificat commun soit créé à l'aide des outils du Serveur d'administration de manière automatique, sélectionnez l'option **Créer le certificat à l'aide des outils du Serveur d'administration**.
   - Si vous souhaitez attribuer à un utilisateur un certificat préalablement créé, 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.

     Si vous ne souhaitez pas indiquer le type d'appareil mobile et le mode de notification de l'utilisateur à propos de la création du certificat, décochez la case **Publier le certificat**.
7. 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.
8. Dans la fenêtre de l'assistant **Paquets d'installation**, sélectionnez le paquet autonome pour l'installation de Kaspersky Endpoint Security pour Android.
9. 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 appareil mobile à propos de la création du certificat.
10. 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 appareil mobile. Afin d'obtenir un certificat, il est nécessaire de lancer la synchronisation de l'appareil mobile avec le Serveur d'administration.

MISE A JOUR D'UNE VERSION ANTERIEURE DE KASPERSKY SECURITY FOR MOBILE

Si une version antérieure de la solution globale Kaspersky Security for Mobile est déjà déployée dans votre entreprise, vous pouvez mettre à niveau chacun des modules de la solution.

Mise à jour des plug-ins d'administration

Afin de mettre à jour les plug-ins d'administration de Kaspersky Endpoint Security et de Kaspersky Mobile Device Management, il est nécessaire de supprimer la version précédente du plug-in dans Kaspersky Security Center. Ce faisant, les groupes d'administration existants dans le dossier **Ordinateurs administrés** et les règles de déplacement automatique des appareils 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 une nouvelle fonctionnalité de la solution complète Kaspersky Security for Mobile apparaîtront dans les stratégies déjà existantes et présenteront des valeurs par défaut.

Mise à jour de l'application mobile

Vous pouvez mettre à jour l'application mobile Kaspersky Endpoint Security en installant la dernière version de l'application (par exemple, mettre à niveau Kaspersky Endpoint Security 8 for Smartphone vers Kaspersky Endpoint Security 10). L'utilisateur sera invité à supprimer la version précédente lors du premier lancement de l'application mobile Kaspersky Endpoint Security 10. Il est recommandé de supprimer la version précédente de l'application.

INSTALLATION DE LA SOLUTION COMPLETE

Cette section décrit l'installation des modules de la solution complète Kaspersky Security for Mobile.

DANS CETTE SECTION

INSTALLATION DU PLUG-IN D'ADMINISTRATION DE KASPERSKY ENDPOINT SECURITY FOR MOBILE

- *Afin d'installer le plug-in d'administration de Kaspersky Endpoint Security,*

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

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

Vous pouvez vérifier l'installation du plug-in pour l'application Kaspersky Endpoint Security 10 for Mobile en consultant la liste des plug-ins d'administration des applications qui est affichée dans la section **Avancé** de la fenêtre des propriétés du Serveur d'administration.

INSTALLATION DU PLUG-IN D'ADMINISTRATION DES APPAREILS EAS ET IOS MDM

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

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

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

Vous pouvez vérifier l'installation du plug-in pour l'application Kaspersky Mobile Device Management en consultant la liste des plug-ins d'administration des applications qui est affichée dans la section **Avancé** de la fenêtre des propriétés du Serveur d'administration.

INSTALLATION DE L'APPLICATION MOBILE KASPERSKY ENDPOINT SECURITY FOR ANDROID

Cette section décrit les options d'installation de l'application mobile Kaspersky Endpoint Security 10 for Android sur les appareils Android.

DANS CETTE SECTION

INSTALLATION VIA L'ENVOI DE MESSAGES ELECTRONIQUES

Pour installer l'application mobile Kaspersky Endpoint Security for Android sur les appareils des utilisateurs via l'envoi de messages électroniques, il est nécessaire de créer un paquet d'installation et d'en définir les paramètres. Ensuite, vous devez composer un paquet autonome d'installation sur la base de ce paquet d'installation. Ce paquet doit être distribué parmi les utilisateurs des appareils mobiles à l'aide de l'envoi de messages électroniques contenant le paquet, un lien vers le serveur Internet du Kaspersky Security Center, un dossier administrateur partagé ou une autre ressource où se trouve le paquet autonome d'installation.

L'utilisateur télécharge lui-même la distribution de l'application mobile sur l'appareil. Une fois le téléchargement sur l'appareil terminé, l'Assistant d'installation de l'application se lance. L'utilisateur effectue l'installation de Kaspersky Endpoint Security 10 for Android sur son appareil en suivant les indications de l'Assistant.

DANS CETTE SECTION

ENVOI DE MESSAGES ELECTRONIQUES AUX UTILISATEURS

Avant d'envoyer les messages électroniques aux utilisateurs, assurez-vous que l'envoi de notifications par message électronique est configuré dans la Console d'administration du Kaspersky Security Center.

Pour envoyer aux utilisateurs un courrier électronique contenant le lien vers le paquet autonome d'installation de l'application Kaspersky Endpoint Security for Android, procédez comme suit :

1. Sélectionnez dans l'arborescence de la console le Serveur d'administration auquel les appareils mobiles sont connectés.
2. Dans l'arborescence de la console, sélectionnez le dossier **Comptes utilisateurs**.
3. Sélectionnez un ou plusieurs utilisateurs.

Il est conseillé d'analyser les comptes des utilisateurs quant à l'existence d'une adresse e-mail.

4. Dans le menu contextuel du compte utilisateur, sélectionnez l'option **Envoyer par message électronique**.

   La fenêtre de création d'un message électronique s'ouvre.

5. Créez un message comportant un lien vers le paquet autonome d'installation de Kaspersky Endpoint Security for Android :

   - Saisissez le sujet du message.
   - Saisissez le texte du message en indiquant le lien vers le paquet autonome d'installation du serveur Internet du Kaspersky Security Center ou le chemin pour y parvenir dans votre dossier partagé.
   - Cochez les cases **Envoyer à l'adresse électronique principale** et **Envoyer à l'adresse électronique complémentaire** si vous voulez utiliser une adresse de messagerie principale et une adresse de messagerie complémentaire.
   - S'il faut créer des codes QR pour les liens, cochez la case **Créer les codes QR graphiques pour les adresses Internet et les envoyer dans un message**.

6. Appuyez sur **OK** pour commencer l'envoi.

INSTALLATION DE L'APPLICATION MOBILE SUR L'APPAREIL APRES LA RECEPTION DU MESSAGE ELECTRONIQUE

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

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

Si tous les paramètres de connexion de l'appareil au Serveur d'administration ont été indiqués lors de la création du paquet d'installation, la configuration initiale de l'application mobile n'est pas nécessaire. L'utilisateur doit seulement installer le certificat commun sur l'appareil mobile (cf. section "Installation d'un certificat commun" à la page 54) afin d'identifier l'appareil dans la Console d'administration de Kaspersky Security Center.

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

L'application Kaspersky Endpoint Security for Android sera ainsi installée sur l'appareil mobile de l'utilisateur. Une fois que l'appareil mobile équipé de Kaspersky Endpoint Security (ci-après, l'appareil KES) aura été connecté au Serveur d'administration, il deviendra administré et pourra être contrôlé à distance par l'administrateur.

INSTALLATION VIA L'ENVOI DE SMS

Pour installer l'application mobile Kaspersky Endpoint Security for Android via l'envoi de SMS, il est nécessaire de créer un paquet d'installation et d'en définir les paramètres. Ensuite, vous devez composer un paquet autonome d'installation sur la base de ce paquet d'installation. Ce paquet doit être distribué parmi les utilisateurs des appareils mobiles à l'aide de l'envoi de SMS contenant un lien vers le serveur Internet du Kaspersky Security Center ou une autre ressource comportant le paquet autonome d'installation de l'application.

L'utilisateur télécharge lui-même la distribution de l'application mobile sur l'appareil à partir de la ressource réseau spécifiée dans l'envoi. Une fois le téléchargement sur l'appareil terminé, l'Assistant d'installation de l'application se lance. L'utilisateur effectue l'installation de Kaspersky Endpoint Security for Android sur son appareil en suivant les indications de l'Assistant.

DANS CETTE SECTION

ENVOI DE SMS AUX UTILISATEURS

Avant d'envoyer des SMS aux utilisateurs, assurez-vous que l'envoi de SMS est configuré dans la Console d'administration du Kaspersky Security Center.

Pour envoyer un SMS aux utilisateurs avec le lien vers le paquet autonome d'installation de Kaspersky Endpoint Security for Android, procédez comme suit :

1. Sélectionnez dans l'arborescence de la console le Serveur d'administration auquel les appareils mobiles sont connectés.
2. Dans l'arborescence de la console, sélectionnez le dossier **Comptes utilisateurs**.
3. Sélectionnez un ou plusieurs utilisateurs.

   Il est conseillé d'analyser les comptes des utilisateurs quant à la présence de numéros de téléphone.
4. Dans le menu contextuel du compte utilisateur, sélectionnez l'option **Envoyer un SMS**.

   La fenêtre de création d'un SMS s'ouvre.
5. Sélectionnez le type du numéro de téléphone de l'utilisateur vers lequel vous souhaitez envoyer le message en cochant une ou plusieurs cases à côté de **Utiliser le numéro de mobile**, **Utiliser le numéro de téléphone complémentaire** ou **Utiliser le numéro de téléphone principal**.
6. Saisissez le texte du message en insérant le lien vers le paquet autonome d'installation stocké sur le serveur Internet.
7. Cliquez sur le bouton **OK** pour l'envoi.

INSTALLATION DE L'APPLICATION MOBILE SUR L'APPAREIL APRES LA RECEPTION DU SMS

Après avoir reçu un SMS de l'administrateur contenant le lien vers le paquet autonome, l'utilisateur peut télécharger le fichier de distribution de l'application sur son appareil par les moyens à sa disposition.

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

Si tous les paramètres de connexion de l'appareil au Serveur d'administration ont été indiqués lors de la création du paquet d'installation, la configuration initiale de l'application mobile n'est pas nécessaire. L'utilisateur doit seulement installer le certificat commun sur l'appareil mobile (cf. section "Installation d'un certificat commun" à la page 54) afin d'identifier l'appareil dans la Console d'administration de Kaspersky Security Center.

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

L'application Kaspersky Endpoint Security for Android sera ainsi installée sur l'appareil mobile de l'utilisateur. Une fois que l'appareil KES a été connecté au Serveur d'administration, il peut être administré. L'administrateur peut commander à distance l'appareil administré.

INSTALLATION VIA LE POSTE DE TRAVAIL

Pour installer l'application mobile Kaspersky Endpoint Security for Android via le poste de travail, il est nécessaire de créer un paquet d'installation et d'en définir les paramètres. Ensuite, vous devez créer et lancer la tâche d'installation à distance pour les postes de travail auxquels les appareils mobiles des utilisateurs sont connectés. Pour créer cette tâche, l'administrateur peut utiliser l'Assistant d'installation à distance de la Console d'administration du Kaspersky Security Center.

DANS CETTE SECTION

CREATION DE LA TACHE D'INSTALLATION A 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 10 for Mobile.

3. Si les postes de travail auxquels se connectent les appareils mobiles des utilisateurs se trouvent dans le groupe **Ordinateurs non définis** de la fenêtre **Sélection des ordinateurs pour l'installation**, cliquez sur le bouton **Sélectionner les ordinateurs pour l'installation**.

4. Si vous avez créé un groupe d'administration dédié aux postes de travail et que vous souhaitez définir une tâche d'installation à distance simultanée pour tous les postes de travail : dans la fenêtre **Sélection des ordinateurs pour l'installation**, cliquez sur le bouton **Installation sur le groupe des ordinateurs administrés**.

5. Si vous souhaitez créer une tâche d'installation à distance uniquement pour une partie des postes de travail du groupe d'administration, dans la fenêtre **Sélection des ordinateurs pour l'installation**, cliquez sur le bouton **Sélectionner les ordinateurs pour l'installation**.

6. Si vous souhaitez créer une tâche d'installation à distance pour des postes de travail de différents groupes d'administration, dans la fenêtre **Sélection des ordinateurs pour l'installation**, cliquez sur le bouton **Sélectionner les ordinateurs pour l'installation**.

7. 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 appareils est installé et lancé automatiquement. Cet utilitaire contrôle la connexion des appareils mobiles à l'ordinateur. Dès que l'utilisateur connecte au poste de travail un appareil dont la configuration système permet d'installer les applications de Kaspersky Endpoint Security, l'utilitaire affiche un message qui propose d'installer l'application sur l'appareil mobile connecté. Si l'utilisateur autorise l'installation, l'utilitaire télécharge la distribution de l'application sur l'appareil. Une fois le téléchargement sur l'appareil terminé, l'Assistant d'installation de l'application se lance. L'utilisateur effectue lui-même l'installation de Kaspersky Endpoint Security for Android sur son appareil en suivant les indications de l'Assistant.

TELECHARGEMENT DE LA DISTRIBUTION DE L'APPLICATION SUR L'APPAREIL VIA LE POSTE DE TRAVAIL

Le téléchargement de la distribution de l'application Kaspersky Endpoint Security for Android sur l'appareil 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 répondant aux pré-requis matériels et logiciels, l'utilitaire propose à l'utilisateur d'y installer Kaspersky Endpoint Security 10 for Android.

Pour copier le fichier de distribution de l'application Kaspersky Endpoint Security 10 for Android à partir du poste de travail sur l'appareil mobile, l'utilisateur doit procéder comme suit :

1. Connecter l'appareil 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 appareils détectés, choisir l'appareil 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 appareils choisis et va afficher les résultats du fonctionnement. L'installation de Kaspersky Endpoint Security for Android commence automatiquement sur l'appareil dès la fin du téléchargement de la distribution.

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, l'utilisateur doit cocher la case **Interrompre l'exécution automatique de l'application d'installation de Kaspersky Endpoint Security 10 for Mobile** de la fenêtre **KSM10** à chaque connexion de l'appareil mobile à l'ordinateur.

INSTALLATION DE L'APPLICATION MOBILE SUR L'APPAREIL

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

Si tous les paramètres de connexion de l'appareil au Serveur d'administration ont été indiqués lors de la création du paquet d'installation, la configuration initiale de l'application mobile n'est pas nécessaire. L'utilisateur doit seulement installer le certificat commun sur l'appareil mobile (cf. section "Installation d'un certificat commun" à la page 54) afin d'identifier l'appareil dans la Console d'administration de Kaspersky Security Center.

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

INSTALLATION DE L'APPLICATION DEPUIS GOOGLE PLAY

L'installation de l'application depuis Google Play s'applique lorsque les utilisateurs préfèrent télécharger eux-mêmes l'application depuis Google Play et l'installer.

Pour installer l'application mobile Kaspersky Endpoint Security for Android, l'utilisateur doit accéder à Google Play depuis son appareil, choisir l'application **Kaspersky Endpoint Security** et appuyer sur le bouton **Installer**. L'utilisateur utilise son propre compte Google pour installer l'application. Une fois que l'application aura été installée sur l'appareil mobile, l'utilisateur devra définir lors de la première exécution les paramètres de connexion au Serveur d'administration et installer le certificat commun (cf. section "Installation d'un certificat commun" à la page 54).

L'application Kaspersky Endpoint Security for Android sera ainsi installée sur l'appareil mobile de l'utilisateur. Au terme de la synchronisation de l'appareil mobile avec le Serveur d'administration, l'appareil mobile de l'utilisateur sur lequel Kaspersky Endpoint Security for Android est installé (appareil KES) est placé dans le dossier **Périphériques non définis**, dans le groupe défini 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 que vous avez créé manuellement ou à l'aide de règles de déplacement automatique.

INSTALLATION DE L'APPLICATION MOBILE KASPERSKY SAFE BROWSER FOR IOS

Cette section décrit les options d'installation de l'application mobile Kaspersky Safe Browser sur les appareils iOS.

DANS CETTE SECTION

INSTALLATION VIA LE SERVEUR DES APPAREILS MOBILES IOS MDM

Pour installer l'application mobile Kaspersky Safe Browser for iOS sur le poste de travail de l'administrateur, il est nécessaire que le Serveur des appareils mobiles iOS MDM soit installé.

L'installation de l'application mobile Kaspersky Safe Browser for iOS via le Serveur de gestion des appareils mobiles iOS MDM comprend les étapes suivantes :

1. Réception du certificat Apple Push Notification (certificat APN).

   Le certificat APN est émis par le service de notifications push de la société Apple. Le certificat APN permet au Serveur d'administration de se connecter au service des APN http://developer.apple.com/library/ios/documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/Chapters/ApplePushService.html pour l'envoi de notifications push sur les appareils mobiles iOS MDM.

2. Création du profil iOS MDM.

   Le profil iOS MDM comporte un ensemble de paramètres dédiés à la connexion des appareils mobiles iOS MDM au Serveur d'administration.

3. Réception du certificat de développeur iOS Developer Certificate.

   Le certificat de développeur est émis par le service du centre de développement iOS de la société Apple. Le certificat de développeur permet de signer l'application Kaspersky Safe Browser for iOS pour l'installation de l'application sur les appareils mobiles des utilisateurs.

4. Création 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.

5. Signature de la distribution Kaspersky Safe Browser for iOS.

6. Installation de Kaspersky Safe Browser for iOS et téléchargement du certificat commun sur les appareils mobiles des utilisateurs.

DANS CETTE SECTION

OBTENTION DU CERTIFICAT DE DEVELOPPEUR

Pour obtenir l'iOS Developer Certificate (ci-après le certificat de développeur) sur le site Internet Apple Developer Portal, vous devez obligatoirement être inscrit au programme Apple Developer Program et posséder un identifiant Apple https://developer.apple.com/.

Pour obtenir le certificat de développeur, procédez comme suit :

1. Accédez au site Apple Developer Portal https://developer.apple.com/ et consultez la rubrique **iOS Dev Center**.
2. Choisissez l'option **Member Center**.
3. Choisissez l'option **Certificates, Identifiers&Profiles**.
4. Créez un certificat de développeur de style iOS App Development en suivant les instructions.
5. Enregistrez le certificat de développeur reçu dans le dossier contenant la distribution de l'application mobile Kaspersky Endpoint Security ou importez-le dans Key Chain Access si vous avez l'intention d'utiliser le cache du certificat.

Pour en savoir plus sur l'obtention du certificat de développeur, consultez le site Apple Developer Portal https://developer.apple.com/.

CREATION DU PROFIL D'APPROVISIONNEMENT

Pour créer un profil provisioning sur le site Apple Developer Portal https://developer.apple.com/, vous devez être inscrit au programme Apple Developer Program et posséder un identifiant Apple.

Pour créer un profil provisioning, procédez comme suit :

1. Accédez au site Apple Developer Portal https://developer.apple.com/ et consultez la rubrique **iOS Dev Center**.
2. Choisissez l'option **Member Center**.
3. Choisissez l'option **Certificates, Identifiers&Profiles**.
4. En fonction du type du compte avec lequel vous êtes inscrit sur le Apple Developer Portal https://developer.apple.com/, réalisez une des opérations suivantes :
   - Si votre compte est de type **Developer**, ajoutez l'appareil mobile pour lequel il faut créer le profil d'approvisionnement. Vous pouvez ajouter un profil provisioning sur un maximum de 100 appareils mobiles.
   - Si votre compte est de type **Developer Enterprise**, choisissez la section **Distribution Profiles**. Vous pourrez y créer des profils d'approvisionnement sur n'importe quel nombre d'appareils.

5. Créez le profil d'approvisionnement en suivant les instructions.

6. Enregistrez le profil provisioning obtenu dans le dossier avec la distribution de l'application mobile Kaspersky Endpoint Security for iOS.

Pour en savoir plus sur la création d'un profil provisioning, consultez le site Apple Developer Portal https://developer.apple.com/.

SIGNATURE DE LA DISTRIBUTION DE L'APPLICATION

La signature de la distribution de l'application mobile Kaspersky Safe Browser for iOS s'opère à l'aide de l'utilitaire make_container. Cet utilitaire se trouve dans l'archive SigningUtility.zip qui figure dans la distribution de la solution complète Kaspersky Security for Mobile.

Pour lancer l'utilitaire make_container, l'ordinateur doit tourner sous Mac OS. L'utilitaire make_container est une application de console. Pour le lancer, utilisez le terminal via **Applications** → **Utilitaires** → **Terminal**.

Pour signer la distribution de Kaspersky Safe Browser for iOS, procédez comme suit :

1. Ouvrez le dossier contenant la distribution de l'application.

2. Sur l'ordinateur sous Mac OS, lancez le terminal via **Applications** → **Utilitaires** → **Terminal**.

3. Sur la ligne de commande du terminal, saisissez cd afin d'ouvrir le dossier contenant l'utilitaire make_container.

4. Dans la ligne de commande du terminal, saisissez la commande qui lance l'utilitaire make_container avec les arguments obligatoires suivants :

   -m – argument pour la création d'un fichier manifest. Les paramètres suivants sont définis pour cette clé :

   - nom bref de l'application pour l'entrée dans le fichier manifest;
   - nom complet de l'application pour l'entrée dans le fichier manifest ;
   - chemin d'accès complet au serveur externe qui hébergera la distribution signée de l'application pour l'entrée dans le fichier manifest;
   - lien vers le fichier de la petite icône de l'application (paramètre facultatif) ;
   - lien vers le fichier de la grande icône de l'application (paramètre facultatif) ;

   -s --sign – arguments pour la signature de la distribution de l'application. Les paramètres suivants sont définis pour cette clé :

   - cache de votre certificat de développeur;
   - identifiant de l'application ;
   - chemin d'accès au profil d'approvisionnement.

   -o – désigne le chemin d'accès au fichier qui sera créé et signé. Les paramètres suivants sont définis pour cette clé :

   - chemin d'accès à la distribution signée de l'application portant l'extension ipa;
   - chemin d'accès à la distribution non signée de l'application avec l'extension app.

   Après l'exécution de la commande saisie, la distribution signée de l'application avec l'extension ipa est créée, ainsi que le fichier manifest avec l'extension plist qui reprend le lien vers la distribution de l'application pour l'installation sur les appareils mobiles.

5. Enregistrez la distribution de l'application obtenue et le fichier manifest sur un serveur externe, en cliquant sur le lien indiqué dans les paramètres de la commande de lancement de l'utilitaire make-container. Par exemple, http://example.com/kes.ipa.

Exemple :

./make_container -m 'KES' 'Kaspersky Endpoint Security' 'http://example.com/kes.ipa' 'http://example.com/large_icon.png' 'http://example.com/small_icon.jpg' -s --sign 6ACE20618C570E56BB5F507327039811FF9ECEF3 com.kaspersky.kes-example ./example.mobileprovision -o ./kes-example.ipa ./KES.app

où figurent les paramètres suivants :

./make_container – lancement de l'utilitaire make_container.

'KES' : abréviation du nom de l'application.

'Kaspersky Endpoint Security' – nom long de l'application.

'http://example.com/kes.ipa' – lien vers le serveur externe qui hébergera la distribution signée de l'application.

'http://example.com/large_icon.png' – lien vers le fichier de la grande icône de l'application. Cette icône apparaîtra pendant le chargement de l'application sur l'appareil mobile de l'utilisateur.

'http://example.com/small_icon.jpg' – lien vers le fichier de la petite icône de l'application. Cette icône apparaîtra pendant le chargement de l'application sur l'appareil mobile de l'utilisateur.

6ACE20618C570E56BB5F507327039811FF9ECEF3 – cache du certificat de développeur que vous utilisez. Le cache apparaît dans les propriétés du certificat du développeur importé dans Key Chain Access.

com.kaspersky.kes-example: ID de l'application.

./example.mobileprovision – chemin d'accès au dossier contenant le profil d'approvisionnement.

./kes-example.ipa – chemin d'accès au dossier qui contiendra la distribution signée de l'application.

./KES.app – chemin d'accès au dossier qui contiendra la distribution non signée de l'application.

INSTALLATION DE L'APPLICATION MOBILE SUR L'APPAREIL

Pour installer Kaspersky Safe Browser for iOS sur un appareil mobile, procédez comme suit :

1. Dans l'arborescence de la console du Serveur d'administration, choisissez le dossier **Appareils mobiles**.
2. Choisissez le sous-dossier **Serveur des appareils mobiles** dans le dossier **Appareils mobiles**.
3. Dans la zone de travail du dossier, sélectionnez le Serveur iOS MDM.
4. Sélectionnez l'option **Propriétés** dans le menu contextuel du Serveur iOS MDM.

   La fenêtre **<Serveur iOS MDM>** s'ouvre.
5. Dans la fenêtre **<Serveur des appareils mobiles iOS MDM>**, sélectionnez la section **Applications administrées**.
6. Cliquez sur le bouton **Ajouter**.
7. Dans le champ **Nom de l'application** de la fenêtre **Ajout d'une application** qui s'ouvre, saisissez le nom de l'application administrée.

8. Saisissez le lien vers le serveur externe qui héberge le fichier manifest **Apple ID ou lien vers l'application**.

9. Si vous souhaitez que Kaspersky Safe Browser soit supprimé après la suppression du profil MDM de l'appareil mobile, cochez la case **Supprimer l'application après la suppression du profil**.

10. Sélectionnez le sous-dossier **Appareils mobiles iOS MDM** dans le dossier **Appareils mobiles**.

11. Sélectionnez un ou plusieurs appareils de la liste.

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

    - Choisissez l'option **Installer l'application sur l'appareil** dans le menu contextuel. Dans la fenêtre **Sélection de l'application à installer** qui s'ouvre, sélectionnez Kaspersky Safe Browser dans la liste des applications administrées.

    - Suivez le lien **Installer l'application sur l'appareil** dans le bloc des appareils sélectionnés. Dans la fenêtre **Sélection de l'application à installer** qui s'ouvre, sélectionnez Kaspersky Safe Browser dans la liste des applications administrées.

    L'application mobile se télécharge automatiquement sur l'appareil de l'utilisateur. L'application demande à l'utilisateur s'il accepte l'installation. Si l'utilisateur accepte l'installation, l'application mobile s'installe sur l'appareil. L'icône de l'application Browser apparaît sur l'appareil. Elle indique la progression de son téléchargement.

Une fois Kaspersky Safe Browser for iOS installée, l'utilisateur doit effectuer la configuration initiale de l'application sur l'appareil. L'utilisateur indique les paramètres de connexion au Serveur d'administration reçus de l'administrateur par e-mail, ainsi que son adresse e-mail. L'utilisateur doit également installer le certificat commun (cf. section "Installation d'un certificat commun" à la page 54) pour identifier l'appareil mobile dans la Console d'administration du Kaspersky Security Center.

Lors de la synchronisation suivante de l'appareil mobile avec le Serveur d'administration, l'appareil mobile de l'utilisateur sur lequel Kaspersky Safe Browser for iOS est installé (ci-après, l'appareil KES) est placé dans le dossier **Périphériques non définis** dans le groupe défini 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 que vous avez créé manuellement ou à l'aide de règles de déplacement automatique.

INSTALLATION DE L'APPLICATION VIA L'APPLE STORE

L'installation de l'application peut s'effectuer via l'Apple Store si les utilisateurs préfèrent télécharger et installer eux-mêmes l'application via l'Apple Store.

Pour installer l'application mobile Kaspersky Safe Browser for iOS, l'utilisateur doit se rendre lui-même, depuis son appareil, sur l'Apple Store, puis sélectionner l'application **Kaspersky Safe Browser** et cliquer sur **Installer**. L'utilisateur installe l'application en utilisant son propre identifiant Apple. Une fois que l'application aura été installée sur l'appareil mobile, l'utilisateur devra définir lors de la première exécution les paramètres de connexion au Serveur d'administration et installer le certificat commun (cf. section "Installation d'un certificat commun" à la page 54).

L'application Kaspersky Safe Browser for iOS sera ainsi installée sur l'appareil mobile de l'utilisateur. Au terme de la synchronisation de l'appareil mobile avec le Serveur d'administration, l'appareil mobile de l'utilisateur sur lequel Kaspersky Safe Browser for iOS est installé (l'appareil KES) est placé dans le dossier **Périphériques non définis** dans le groupe défini 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 que vous avez créé manuellement ou à l'aide de règles de déplacement automatique.

INSTALLATION DE L'APPLICATION MOBILE KASPERSKY SAFE BROWSER FOR WINDOWS PHONE

Pour installer l'application mobile Kaspersky Safe Browser for Windows Phone, l'utilisateur doit se rendre lui-même, depuis son appareil, sur la boutique en ligne Windows Phone, puis sélectionner l'application **Kaspersky Safe Browser** et l'installer. Après l'installation de l'application sur l'appareil mobile, l'utilisateur devra lors de la première exécution configurer les paramètres de connexion au Serveur d'administration et installer un certificat commun (cf. section "Installation d'un certificat commun" à la page 54).

L'application Kaspersky Safe Browser for Windows Phone sera ainsi installée sur l'appareil mobile de l'utilisateur. Une fois que l'appareil mobile équipé de Kaspersky Safe Browser (ci-après, l'appareil KES) aura été connecté au Serveur d'administration, il deviendra administré et pourra être contrôlé à distance par l'administrateur.

PREPARATION DES APPLICATIONS MOBILES KASPERSKY ENDPOINT SECURITY AU FONCTIONNEMENT SUR LES APPAREILS

Cette section fournit des informations sur la configuration des applications mobiles de Kaspersky Endpoint Security sur les appareils des utilisateurs, ainsi que sur la répartition des appareils dans les groupes d'administration.

DANS CETTE SECTION

INSTALLATION D'UN CERTIFICAT COMMUN

Afin d'identifier l'utilisateur et d'assurer la sécurité de l'échange de données avec le Serveur d'administration, l'utilisateur doit créer un certificat commun. Pour installer un certificat, l'utilisateur doit cliquer sur le bouton **Obtenir un certificat** dans les paramètres de l'application, puis saisir ses données de domaine. Si l'utilisateur n'a pas installé de certificat commun, la synchronisation avec le Serveur d'administration sera impossible.

Au terme de la synchronisation de l'appareil mobile avec le Serveur d'administration, l'appareil mobile de l'utilisateur sur lequel Kaspersky Endpoint Security est installé est placé dans le dossier **Périphériques non définis** dans le groupe défini 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 que vous avez créé manuellement ou à l'aide de règles de déplacement automatique.

DEFINITION DES PARAMETRES DE CONNEXION DES APPAREILS MOBILES AU SERVEUR D'ADMINISTRATION

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

- un paquet autonome ou un fichier d'installation préconfiguré est installé sur l'appareil mobile Android (par exemple, lors du déploiement à l'aide de l'envoi de messages électroniques ou de SMS) ;
- l'application est installée sur un appareil mobile après la connexion au poste de travail.

Dans les autres cas, lors du premier lancement sur l'appareil, l'utilisateur doit définir les paramètres de connexion au Serveur d'administration reçus de l'administrateur :

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

- **Numéro du port SSL**. L'utilisateur doit saisir le numéro du port de Serveur d'administration destiné à la connexion des appareils mobiles. Le numéro de port par défaut est 13292. Le numéro du port est indiqué dans les propriétés du Serveur d'administration, section Paramètres**.**

- **Groupe**. L'utilisateur doit indiquer le nom du groupe d'administration auquel appartient son appareil.

- **Adresse de courrier électronique**. L'utilisateur doit indiquer son adresse électronique professionnelle.

ACTIVATION DES APPLICATIONS MOBILES

Dans Kaspersky Security Center, la licence peut couvrir différents groupes fonctionnels. Pour pouvoir utiliser toutes les fonctionnalités des plug-ins d'administration de Kaspersky Endpoint Security 10, de Kaspersky Mobile Device Management 10 et des applications Kaspersky Endpoint Security sur les appareils mobiles, la licence pour le Kaspersky Security Center acquise par l'entreprise doit couvrir la fonctionnalité Administration des appareils mobiles. La fonctionnalité Administration des appareils mobiles sert à connecter des appareils mobiles au Serveur d'administration et à les gérer via Exchange ActiveSync et iOS MDM, ainsi qu'à administrer ceux équipés de l'application Kaspersky Endpoint Security 10.

Pour plus d'informations sur la licence pour le Kaspersky Security Center et les options de la licence, consultez le *Manuel d'administrateur du Kaspersky Security Center*.

L'activation des applications Kaspersky Endpoint Security 10 est une procédure particulière, car les informations sur la licence sont transmises sur l'appareil en même temps que la stratégie lors de la synchronisation de l'appareil avec le Serveur d'administration. Suite à l'installation de l'application, l'appareil mobile tente de se synchroniser au Serveur d'administration toutes les trois heures. Après l'application d'une stratégie, la fréquence de synchronisation de l'appareil 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 activer l'application sur l'appareil mobile, vous devez créer une stratégie pour le groupe dont l'appareil fait partie et spécifiez pour cette stratégie une clé qui se trouve dans le stockage du Serveur d'administration et qui a été ajoutée à l'aide d'un code d'activation ou d'un fichier de licence. Lors de la connexion suivante de l'appareil mobile au Serveur d'administration, les informations sur la licence seront téléchargées sur l'appareil avec la stratégie. L'application Kaspersky Endpoint Security 10 installée sur l'appareil sera activée.

Si l'application n'est pas activée dans les trois jours qui suivent l'installation de Kaspersky Endpoint Security 10 sur l'appareil mobile, ses fonctionnalités seront automatiquement restreintes. La plupart de ses modules seront désactivés. Lorsqu'elle passe en mode de fonctionnement avec fonctionnalités restreintes, l'application cesse d'effectuer une synchronisation automatique avec le Serveur d'administration. Aussi, si pour de quelconques raisons l'application n'a pas été activée dans les trois jours qui suivent son installation, l'utilisateur doit effectuer la synchronisation avec le Serveur d'administration manuellement.

CREATION D'UN CERTIFICAT DE MESSAGERIE

Afin de connecter le client de messagerie au serveur et de télécharger les messages sur l'appareil mobile de l'utilisateur, il est nécessaire de créer un certificat de messagerie.

Pour créer un certificat de messagerie, procédez comme suit :

1. Dans l'arborescence de la console du Kaspersky Security Center, sélectionnez l'entrée **Administration des appareils mobiles**.

2. A l'entrée **Administration des appareils mobiles**, sélectionnez le dossier **Certificats**.

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

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

5. Dans la fenêtre **Type de certificat** de l'assistant, sélectionnez l'option **Certificat de messagerie**.

6. Dans la fenêtre **Source du certificat** de l'assistant, indiquez le mode de création du certificat de messagerie :

   - Si vous souhaitez que le certificat de messagerie soit créé à l'aide des outils du Serveur d'administration de manière automatique, sélectionnez l'option **Créer le certificat à l'aide des outils du Serveur d'administration**.

   - Si vous souhaitez attribuer à un utilisateur un certificat préalablement créé, 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.

     Si vous ne souhaitez pas indiquer le type d'appareil mobile et le mode de notification de l'utilisateur à propos de la création du certificat, décochez la case **Publier le certificat**.

7. 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 de messagerie.

8. Si vous avez sélectionné un type d'appareil administré selon le protocole iOS MDM dans la fenêtre **Type d'appareil**, indiquez le tag pour le certificat à créer dans la liste déroulante de la fenêtre **Tag du certificat**.

9. Si vous avez sélectionné un appareil Android administré par Kaspersky Security for Mobile dans la fenêtre **Type d'appareil**, configurez les paramètres de notification, par SMS ou courrier électronique, de l'utilisateur de l'appareil mobile à propos de la création d'un certificat, dans la fenêtre **Mode de notification des utilisateurs**.

10. Dans la fenêtre **Informations sur le certificat**, 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 de messagerie sera créé et pourra être installé par un utilisateur sur un appareil mobile. Afin d'obtenir un certificat, il est nécessaire de lancer la synchronisation de l'appareil mobile avec le Serveur d'administration.

CREATION D'UN CERTIFICAT POUR VPN

Afin de connecter l'appareil mobile de l'utilisateur à un réseau privé virtuel, il est nécessaire de créer un certificat pour VPN.

Pour créer un certificat pour VPN, procédez comme suit :

1. Dans l'arborescence de la console du Kaspersky Security Center, sélectionnez l'entrée **Administration des appareils mobiles**.

2. A l'entrée **Administration des appareils mobiles**, sélectionnez le dossier **Certificats**.

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

   L'assistant d'installation de certificats s'ouvre.

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

5. Dans la fenêtre **Type de certificat** de l'assistant, sélectionnez l'option **Certificat pour VPN**.

6. Dans la fenêtre **Source du certificat** de l'assistant, indiquez le mode de création du certificat pour VPN :

- Si vous souhaitez que le certificat pour VPN soit créé à l'aide des outils du Serveur d'administration de manière automatique, sélectionnez l'option **Créer le certificat à l'aide des outils du Serveur d'administration**.

- Si vous souhaitez attribuer à un utilisateur un certificat préalablement créé, 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.

  Si vous ne souhaitez pas indiquer le type d'appareil mobile et le mode de notification de l'utilisateur à propos de la création du certificat, décochez la case **Publier le certificat**.

7. 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 pour VPN.

8. Si vous avez sélectionné un type d'appareil administré selon le protocole iOS MDM dans la fenêtre **Type d'appareil**, indiquez le tag pour le certificat à créer dans la liste déroulante de la fenêtre **Tag du certificat**.

9. Si vous avez sélectionné un appareil Android administré par Kaspersky Security for Mobile dans la fenêtre **Type d'appareil**, configurez les paramètres de notification, par SMS ou courrier électronique, de l'utilisateur de l'appareil mobile à propos de la création d'un certificat, dans la fenêtre **Mode de notification des utilisateurs**.

10. 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 pour VPN sera créé et pourra être installé par un utilisateur sur un appareil mobile. Afin d'obtenir un certificat, il est nécessaire de lancer la synchronisation de l'appareil mobile avec le Serveur d'administration.

STRATEGIES DE GROUPE POUR L'ADMINISTRATION DES APPAREILS MOBILES

Cette section contient des informations sur les stratégies de groupe à l'aide desquelles l'administrateur peut gérer de façon centralisée les appareils mobiles et les applications mobiles qui y sont installées. Cette section décrit également l'algorithme de création de stratégies de groupe pour l'administration des appareils mobiles. Vous pouvez créer une stratégie de groupe pour les programmes suivants :

- Kaspersky Endpoint Security ;
- Kaspersky Mobile Device Management.

DANS CETTE SECTION

A PROPOS DE LA STRATEGIE DE GROUPE

Une *stratégie de groupe* est un ensemble unique de paramètres pour l'administration des appareils mobiles appartenant à un groupe d'administration, et des applications mobiles qui y sont installées. Vous pouvez créer une stratégie de groupe à l'aide de l'assistant de création d'une stratégie pour les applications Kaspersky Endpoint Security et Kaspersky Mobile Device Management. Une stratégie de groupe créée pour l'application Kaspersky Endpoint Security sera nommée s*tratégie d'administration des appareils KE*S (cf. page 59). Une stratégie de groupe créée pour l'application Kaspersky Mobile Device Management sera nommée *stratégie d'administration des appareils EAS et iOS MDM* (cf. page 60).

Grâce à cette stratégie, vous pouvez configurer les paramètres d'administration pour un groupe d'appareils ou pour chaque appareil séparément. Il est possible de définir les paramètres d'administration pour les groupes d'appareils dans la fenêtre des propriétés de la stratégie de groupe. Lorsqu'il s'agit d'un appareil en particulier, cette configuration s'effectue dans la fenêtre des paramètres locaux de l'application. Les paramètres d'administration définis spécifiquement pour un appareil peuvent différer de ceux indiqués dans la stratégie du groupe auquel cet appareil appartient.

Chaque paramètre de la stratégie est verrouillé par un cadenas qui indique que la modification du paramètre est interdite dans les stratégies des niveaux inférieurs (pour les groupes et Serveurs d'administration secondaires) et dans les paramètres locaux de l'application.

Les valeurs de paramètres définies dans la stratégie et dans les paramètres locaux de l'application sont enregistrées sur le Serveur d'administration. Elles sont diffusées sur les appareils mobiles lors de la synchronisation et sont considérées comme des paramètres actifs des applications Kaspersky Endpoint Security. Si l'utilisateur installe d'autres valeurs de paramètres non verrouillées, elles seront transmises au Serveur d'administration dès la synchronisation suivante. De même, elles seront enregistrées dans les paramètres locaux à la place des valeurs que l'administrateur avait définies auparavant.

Afin de maintenir l'actualité de la sécurité de l'entreprise sur les appareils KES des utilisateurs, vous pouvez contrôler leur conformité à la stratégie de groupe pour l'administration des appareils KES.

Pour en savoir plus sur l'utilisation des stratégies et des groupes d'administration dans la Console d'administration du Kaspersky Security Center, reportez-vous au *Manuel de l'administrateur du Kaspersky Security Center*.

DANS CETTE SECTION

A PROPOS DE LA STRATEGIE DE GROUPE POUR L'ADMINISTRATION DES APPAREILS KES

Le plug-in d'administration de Kaspersky Endpoint Security permet de créer des stratégies de groupe pour l'administration des appareils KES. Une stratégie de groupe pour l'administration des appareils KES offre à l'administrateur les possibilités suivantes :

- définir les paramètres de la protection antivirus sur les appareils mobiles : paramètres d'analyse des appareils, paramètres de protection des appareils via les technologies cloud, paramètres de mise à jour des bases antivirus (uniquement pour les appareils Android) (cf. page 65) ;
- définir les paramètres du module Antivol (uniquement pour les appareils Android) (cf. page 68) :
  - géolocalisation à distance des appareils perdus ou volés ;
  - verrouillage à distance de l'appareil mobile de l'utilisateur en cas de perte ou de vol ;
  - suppression à distance des données de l'entreprise sur l'appareil mobile ;
  - verrouillage à distance des conteneurs ;
  - suppression à distance de toutes les données de l'appareil et réinitialisation complète.
- définir à distance la synchronisation automatique des appareils avec le Serveur d'administration (cf. page 64) ;
- contrôler la fréquentation des sites Internet sur les appareils mobiles (uniquement pour les appareils Android) (cf. page 70) ;
- administrer le mot de passe pour le déverrouillage de l'appareil (uniquement pour les appareils Android et iOS) (cf. page 70) ;
- configurer l'utilisation des conteneurs : autorisation et chiffrement des données des conteneurs (uniquement pour les appareils Android et iOS) (cf. page 78) ;
- configurer les fonctions matérielles des appareils mobiles : utilisation de l'appareil photo, du Bluetooth ou du Wi-Fi (uniquement pour les appareils Android) (cf. page 71) ;
- administrer le mot de passe système de l'appareil (uniquement pour les appareils Android) (cf. page 71) ;
- configurer les paramètres de la messagerie d'entreprise pour son utilisation via le client de messagerie TouchDown (uniquement pour les appareils Android) (cf. page 71) ;
- supprimer à distance l'application mobile Kaspersky Endpoint Security for Android des appareils (cf. page 74) ;
- configurer les paramètres des réseaux sans fil pour leur utilisation sur les appareils mobiles (uniquement pour les appareils Android) (cf. page 75) ;
- contrôler le lancement des applications mobiles sur les appareils en fonction de leur catégorie (uniquement pour les appareils Android) (cf. page 75) ;

- contrôler l'installation d'applications mobiles tierces sur les appareils (uniquement pour les appareils Android) (cf. page 75) ;
- contrôler la conformité des appareils à la stratégie (uniquement pour les appareils Android) (cf. page 81) ;
- administrer les appareils Android Samsung prenant en charge KNOX (cf. page 85) :
  - configurer les points d'accès (APN) (pour KNOX toutes versions confondues) ;
  - contrôler l'activité réseau des appareils (pour KNOX 1 et 2) ;
  - configurer un réseau privé virtuel (VPN) (pour KNOX 1) ;
  - configurer la synchronisation avec le serveur Microsoft Exchange (pour KNOX 1 et 2).
- activer à distance les applications mobiles Kaspersky Endpoint Security sur les appareils (cf. page 85).

A PROPOS DE LA STRATEGIE DE GROUPE POUR L'ADMINISTRATION DES APPAREILS EAS ET IOS MDM

Le plug-in d'administration de Kaspersky Mobile Device Management permet de créer des stratégies de groupe afin de définir les paramètres de configuration des appareils EAS et iOS MDM sans avoir à utiliser iPhone Configuration Utility ou le profil d'administration de Exchange ActiveSync.

Une stratégie de groupe pour l'administration des appareils EAS et iOS MDM offre à l'administrateur les possibilités suivantes :

- pour l'administration des appareils EAS :
  - configurer les paramètres du mot de passe pour le déverrouillage de l'appareil (cf. page 91) ;
  - configurer la conservation de données sur l'appareil sous forme chiffrée (cf. page 91) ;
  - configurer les paramètres de synchronisation de la messagerie professionnelle (cf. page 92) ;
  - configurer les fonctions matérielles des appareils mobiles, telles que l'utilisation de supports amovibles, de l'appareil photo ou du Bluetooth (cf. page 93) ;
  - configurer des restrictions relatives à l'utilisation des applications mobiles sur l'appareil (cf. page 94).
- pour l'administration des appareils iOS MDM :
  - configurer l'utilisation du mot de passe sur l'appareil (cf. page 96) ;
  - configurer des restrictions relatives à l'utilisation des fonctions matérielles de l'appareil ou à l'installation et à la suppression des applications mobiles (cf. page 97) ;
  - configurer des restrictions relatives à l'utilisation des applications mobiles préinstallées telles que YouTube™, iTunes Store ou Safari (cf. page 97) ;
  - configurer des restrictions relatives au visionnage du contenu multimédia (comme des films ou des émissions) selon la région de l'appareil mobile (cf. page 97) ;
  - configurer les paramètres de connexion de l'appareil à Internet via un serveur proxy (proxy HTTP global) (cf. page 98) ;
  - configurer les paramètres du compte utilisateur unique à l'aide duquel l'utilisateur peut accéder aux applications et services de l'entreprise (technologie d'authentification unique) (cf.page 99) ;

- contrôler l'utilisation d'Internet (sites Internet consultés) sur les appareils mobiles (cf. page 100) ;
- configurer les paramètres des réseaux sans fil (Wi-Fi), des points d'accès (APN) et des réseaux privés virtuels (VPN) à l'aide de plusieurs mécanismes d'authentification et protocoles réseaux (cf. pages 101, 124 et 104) ;
- configurer les paramètres de connexion aux appareils AirPlay pour la diffusion sans fil de photos, musiques et vidéos (cf. page 111) ;
- configurer les paramètres de connexion aux imprimantes AirPrint pour l'impression sans fil de documents (cf. page 112) ;
- configurer les paramètres de synchronisation avec le serveur Microsoft Exchange et les comptes utilisateur pour l'utilisation de la messagerie professionnelle sur les appareils (cf. pages 113 et 115) ;
- configurer les données de compte de l'utilisateur pour la synchronisation avec le service des répertoires LDAP (cf. page 116) ;
- configurer les données de compte de l'utilisateur pour la connexion aux services CalDAV et CardDAV qui permettent d'accéder aux calendriers et aux listes de contacts de l'entreprise (cf. page 117, cf. page 118) ;
- configurer les paramètres de l'interface iOS sur l'appareil de l'utilisateur tels que les polices et les icônes des sites Internet favoris (cf. pages 121 et 119) ;
- ajouter de nouveaux certificats de sécurité sur l'appareil (cf. page 121) ;
- configurer les paramètres du serveur SCEP pour que l'appareil obtienne automatiquement les certificats depuis le Centre de certification (cf. page 122) ;
- ajouter des paramètres personnalisés pour le fonctionnement des applications mobiles.

La stratégie d'administration des appareils EAS et iOS MDM se distingue par le fait qu'elle s'applique au groupe d'administration auquel appartiennent le Serveur des appareils mobiles iOS MDM et le Serveur des appareils mobiles Exchange ActiveSync (ci-après, les serveurs des appareils mobiles). Tous les paramètres définis dans cette stratégie sont d'abord appliqués aux serveurs d'appareils mobiles, puis aux appareils mobiles qu'ils gèrent. En cas d'utilisation d'une structure hiérarchique de groupes d'administration, les serveurs d'appareils mobiles secondaires obtiennent les paramètres de stratégie des serveurs d'appareils mobiles principaux et les diffusent sur les appareils mobiles.

CREATION D'UNE STRATEGIE DE GROUPE

Cette section décrit la création de stratégies de groupe pour les appareils utilisant les applications mobiles Kaspersky Endpoint Security et de stratégies pour les appareils EAS et iOS MDM.

Les stratégies créées pour le groupe d'administration sont affichées dans l'espace de travail du groupe sous l'onglet **Stratégies**. A côté du nom de chacune des stratégies est affichée l'icône qui indique son statut (active/inactive). Plusieurs stratégies pour différentes applications peuvent être créées dans un même groupe. Seule une stratégie peut être active pour une même application. Si vous créez une nouvelle stratégie active, la stratégie active précédente devient inactive.

Vous pouvez modifier la stratégie après sa création.

Pour créer une stratégie pour les applications Kaspersky Endpoint Security 10 Service Pack 1 for Mobile et Kaspersky Mobile Device Management 10 Service Pack 1, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez le groupe d'administration pour lequel vous souhaitez créer une stratégie.
2. Dans la zone de travail du groupe, choisissez l'onglet **Stratégies**.
3. Cliquez sur le lien **Créer une stratégie** pour lancer l'Assistant de création d'une stratégie.

L'Assistant de création de stratégies s'ouvre. Il faut suivre ses indications.

Utilisez le bouton **Suivant** pour naviguer entre les fenêtres de l'Assistant. Pour interrompre l'Assistant, cliquez sur le bouton **Annuler** dans la fenêtre de l'Assistant. Dans ce cas, aucune stratégie ne sera créée.

ETAPE 1. DEFINITION DU NOM DE LA STRATEGIE DE GROUPE

Saisissez à cette étape le nom de la nouvelle stratégie dans le champ **Nom**. Si vous saisissez un nom qui existe déjà, (1) est ajouté automatiquement au nom saisi.

Passez à l'étape suivante de l'Assistant de création de stratégie.

ETAPE 2. SELECTION DE L'APPLICATION POUR LA CREATION DE LA STRATEGIE DE GROUPE

Sélectionnez l'application pour la création de la stratégie de groupe dans la liste des applications présentées à cette étape :

- **Kaspersky Endpoint Security 10 Service Pack 1 for Mobile**, pour les appareils utilisant l'application mobile Kaspersky Endpoint Security.
- **Kaspersky Mobile Device Management 10 Service Pack 1**, pour les appareils EAS et iOS MDM.

La création d'une stratégie pour les appareils mobiles n'est possible que si le plug-in d'administration de Kaspersky Endpoint Security 10 for Mobile et le plug-in d'administration de Kaspersky Mobile Device Management 10 Service Pack 1 sont installés sur le poste de travail de l'administrateur (cf. section "Installation du plug-in d'administration des appareils EAS et iOS MDM" à la page 41). Si les plug-ins ne sont pas installés, le nom de l'application correspondante ne figure pas dans la liste des applications.

Passez à l'étape suivante de l'Assistant de création de stratégie.

ETAPE 3. SELECTION DE L'ETAT DE LA STRATEGIE

Cette étape de l'Assistant permet de sélectionner l'état de la stratégie :

- **Stratégie active**. L'Assistant enregistre la stratégie créée sur le serveur d'administration. La stratégie sera utilisée en tant que stratégie active sur l'appareil dès la synchronisation suivante de l'appareil mobile avec le Serveur d'administration.
- **Stratégie inactive**. L'Assistant enregistre la stratégie créée sur le serveur d'administration en guise de stratégie de réserve. La stratégie pourra être activée ultérieurement en fonction des événements. Si nécessaire, la stratégie inactive peut être transformée en stratégie active.

Il est possible de créer plusieurs stratégies pour une seule application dans le groupe, mais seule l'une d'entre elles peut être active. Quand vous créez une stratégie active, la stratégie active précédente devient automatiquement inactive.

Quittez l'Assistant.

CONFIGURATION DE LA STRATEGIE DE GROUPE POUR L'ADMINISTRATION DES APPAREILS KES

Une stratégie pour l'application Kaspersky Endpoint Security vous aide à configurer les paramètres d'administration des appareils KES et des applications mobiles Kaspersky Endpoint Security installées sur les appareils mobiles.

Pour configurer la stratégie de groupe pour l'administration des appareils KES, procédez comme suit :

1. Dans l'arborescence de la Console d'administration du Kaspersky Security Center, sélectionnez le groupe d'administration auquel appartiennent les appareils KES et dont vous souhaitez configurer les paramètres.

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 Service Pack 1 10 for Mobile.

   Si nécessaire, vous pouvez créer une nouvelle stratégie de groupe à l'aide de l'assistant de création d'une stratégie.

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

La fenêtre **Propriétés : <nom de la stratégie>** s'ouvre. Cette fenêtre permet de configurer les paramètres de la stratégie de groupe.

RESTRICTION DES PRIVILEGES D'INSTALLATION

Les administrateurs du Kaspersky Security Center peuvent définir des privilèges d'accès des utilisateurs de la Console d'administration aux différentes fonctions de l'application selon leurs attributs dans l'entreprise.

Dans l'interface de la Console d'administration, la configuration des privilèges d'accès s'effectue dans la fenêtre des propriétés du Serveur d'administration, dans les sections **Sécurité** et **Rôles des utilisateurs**. La section **Rôles des utilisateurs** permet d'ajouter des rôles d'utilisateur types accompagnés d'un ensemble de privilèges définis. La section **Sécurité** permet de définir des privilèges pour un utilisateur ou pour un groupe d'utilisateurs et d'attribuer des rôles à un utilisateur ou à un groupe d'utilisateurs. Les privilèges des utilisateurs pour chaque application sont définis par *zone opérationnelle*.

Vous pouvez également définir les privilèges des utilisateurs par zone opérationnelle pour l'application Kaspersky Endpoint Security. Le tableau ci-dessous reprend les zones opérationnelles de Kaspersky Endpoint Security et les onglets de stratégie qui figurent dans ces zones opérationnelles.

Tableau 2. Zones opérationnelles de l'application

ZONE OPERATIONNELLE	ONGLET DE LA STRATEGIE
Protection	Protection, Analyse, Mise à jour
Contrôle des applications	Contrôle des applications, Applications tierces
Contrôle de la conformité	Contrôle de la conformité
Conteneurs	Conteneurs
Paramètres de l'appareil	Administration de l'appareil, Synchronisation
Administration des appareils Samsung	Paramètres généraux, Paramètres de KNOX 1, Paramètres de KNOX 2
Administration du système	Paramètres avancés, Paramètres de l'appareil
Protection Internet	Protection Internet

L'administrateur peut attribuer les privilèges d'accès suivants pour chaque zone opérationnelle :

- **Autorisation de la modification**. L'utilisateur de la Console d'administration peut modifier les paramètres de la stratégie dans la fenêtre des propriétés.
- **Interdiction de la modification**. L'utilisateur de la Console d'administration ne peut pas modifier les paramètres de la stratégie dans la fenêtre des propriétés. Les onglets de la stratégie qui figurent dans la zone opérationnelle pour laquelle ce privilège a été défini n'apparaissent pas dans l'interface.

Pour en savoir plus sur l'utilisation des privilèges et des rôles des utilisateurs dans la Console d'administration du Kaspersky Security Center, reportez-vous au *Manuel de l'administrateur du Kaspersky Security Center.*

CONFIGURATION DES PARAMETRES DE LA SYNCHRONISATION

Afin d'appliquer une stratégie de groupe aux appareils mobiles des utilisateurs, il convient de configurer les paramètres de connexion au Serveur d'Administration.

La configuration des paramètres de connexion au serveur d'administration est possible pour les appareils sous Android, Windows Phone et iOS.

Par défaut, les appareils mobiles se synchronisent automatiquement avec le Serveur d'administration toutes les six heures. La synchronisation automatique en itinérance est désactivée.

Pour configurer les paramètres de synchronisation des appareils mobiles avec le Serveur d'administration, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Synchronisation**.
3. Dans le groupe **Connexion au Serveur d'administration**, configurez les paramètres de synchronisation de l'appareil avec le Serveur d'administration :
   a. Sélectionnez la fréquence de lancement de la synchronisation dans la liste déroulante **Lancer la synchronisation**.
   b. Si vous souhaitez interdire la synchronisation automatique avec le Serveur d'administration quand l'appareil est en itinérance, cochez la case **Désactiver la synchronisation en itinérance**.

L'interdiction de la synchronisation en itinérance n'est pas disponible sous Android.

4. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Les paramètres de synchronisation avec le Serveur d'Administration seront ainsi configurés sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DES MODULES DE PROTECTION ANTIVIRUS

Les paramètres des modules de protection ne peuvent être modifiés que pour les appareils Android.

Cette section contient les informations sur la configuration des paramètres des modules de protection antivirus.

DANS CETTE SECTION

CONFIGURATION DE L'ANALYSE DE L'APPAREIL

Afin de rechercher les virus et autres programmes malveillants, il convient de configurer les paramètres de l'analyse de l'appareil mobile de l'utilisateur.

La configuration des paramètres d'analyse de l'appareil est disponible uniquement pour les appareils Android.

Par défaut, l'application Kaspersky Endpoint Security analyse uniquement les fichiers exécutables enregistrés sur l'appareil et sur la carte mémoire, ainsi que le contenu des archives. Quand l'application détecte un objet infecté, elle tente de le réparer. Si la réparation de l'objet est impossible, celui-ci est placé en quarantaine. L'analyse complète programmée n'est pas exécutée.

Pour configurer les paramètres d'analyse de l'appareil mobile de l'utilisateur, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Analyse**.

3. Configurez les paramètres d'analyse dans le groupe de paramètres **Paramètres d'analyse de l'appareil** :

   - Si vous souhaitez que l'application analyse tous les fichiers enregistrés sur l'appareil et sur la carte mémoire, décochez la case **Analyser uniquement les fichiers exécutables**.

   - Si vous souhaitez que l'application ignore le contenu des archives, décochez la case **Analyser les archives en les décompressant**.

   - Si vous souhaitez que l'application tente de réparer les objets malveillants, cochez la case **Réparer les fichiers si possible**.

Si la réparation est impossible, l'application exécute l'action sélectionnée dans la liste **Action si la réparation est impossible** pour les objets n'ayant pas été réparés. Si la case est décochée, Kaspersky Endpoint Security exécute, en cas de détection d'une menace, l'action sélectionnée dans la liste **Action en cas de détection d'une menace**.

4. Dans le groupe **Analyse programmée**, configurez le lancement automatique de l'analyse complète du système de fichiers de l'appareil. Pour ce faire, appuyez sur **Planification** et dans la fenêtre **Planification** qui s'ouvre, définissez la fréquence d'exécution de l'analyse complète.

5. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Les paramètres d'analyse de l'appareil seront ainsi configurés sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DE LA PROTECTION DU SYSTEME DE FICHIERS

Afin de protéger en temps réel le système de fichiers de l'appareil mobile contre les infections, il convient de configurer les paramètres de la protection de l'appareil mobile de l'utilisateur.

La configuration des paramètres de protection de l'appareil est disponible uniquement pour les appareils Android.

La protection est activée par défaut. Les appareils Android bénéficient également de l'analyse complémentaire des nouvelles applications à l'aide du service cloud de Kaspersky Security Network et de la détection des logiciels publicitaires et des programmes licites qui pourraient être exploités par des individus malintentionnés pour nuire à l'appareil et aux données de l'utilisateur. Quand Kaspersky Endpoint Security détecte un objet infecté, il tente de le réparer. Si la réparation de l'objet est impossible, celui-ci est placé en quarantaine.

➧ *Pour définir les paramètres de protection du système de fichiers de l'appareil mobile, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Protection**.

3. Dans le groupe **Protection**, définissez les paramètres de protection du système de fichiers de l'appareil mobile :

   - Si vous souhaitez activer la protection en temps réel contre les menaces sur l'appareil de l'utilisateur, cochez la case **Activer la protection.**

   - Si vous souhaitez activer le mode de protection élargie de l'appareil mobile de l'utilisateur contre les menaces, cochez la case **Mode de protection élargie**.

   - Si vous souhaitez activer l'analyse complémentaire des nouvelles applications avant leur premier lancement sur l'appareil de l'utilisateur à l'aide du service cloud Kaspersky Security Network, cochez la case **Utiliser Kaspersky Security Network pour l'analyse**.

   - Si vous souhaitez bloquer les logiciels publicitaires et les programmes pouvant être exploités par des individus malintentionnés pour nuire à l'appareil ou aux données de l'utilisateur, cochez la case **Publicité, numéroteurs et autres**.

4. Si vous souhaitez activer la protection des fichiers exécutables, cochez la case **Analyser seulement les fichiers exécutables** dans le groupe **Paramètres de protection**. Si la case n'est pas cochée, Kaspersky Endpoint Security analyse les fichiers de tout type.

5. Sélectionnez une des options suivantes dans la liste **Action si la réparation est impossible**:

   - **Supprimer**;
   - **Ignorer**;
   - **Quarantaine**.

6. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Les paramètres de protection du système de fichiers de l'appareil seront ainsi configurés sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DE LA MISE A JOUR

Afin de maintenir l'actualité de l'application mobile Kaspersky Endpoint Security, il convient de configurer les paramètres de la mise à jour des bases et de la version de l'application.

La configuration des paramètres de mise à jour de l'application est disponible uniquement pour les appareils Android.

La mise à jour des bases de l'application est désactivée par défaut lorsque l'appareil est en itinérance. La mise à jour programmée des bases de l'application n'est pas exécutée.

Pour définir les paramètres de mise à jour des bases antivirus de l'application sur l'appareil mobile, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Mise à jour**.

3. Si vous souhaitez que Kaspersky Endpoint Security télécharge les mises à jour selon une programmation quand l'appareil est en itinérance cochez la case **Autoriser la mise à jour en itinérance** dans le groupe **Autoriser la mise à jour en itinérance**.

   Même si la case est décochée, l'utilisateur peut lancer manuellement la mise à jour des bases antivirus en itinérance. La mise à jour des bases antivirus sur les appareils Android en itinérance n'est pas disponible.

4. Indiquez dans le groupe **Source des mises à jour** la source des mises à jour à partir de laquelle Kaspersky Endpoint Security copiera et installera les mises à jour des bases antivirus de l'application :

   - **Serveurs de Kaspersky Lab** ;
   - **Serveur d'administration** ;
   - **Autre source**.

5. Dans le groupe de paramètres **Mise à jour programmée**, configurez le lancement de la mise à jour des bases antivirus sur l'appareil de l'utilisateur :

   a. Cliquez sur le bouton **Planification**.

   b. Dans la fenêtre **Planification** qui s'ouvre, définissez la fréquence et l'heure d'exécution de la mise à jour.

6. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Les paramètres de mise à jour des bases antivirus et de la version de l'application seront ainsi configurés sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DE LA PROTECTION CONTRE L'ACCES NON AUTORISE

Les paramètres de la protection contre l'accès non autorisé ne peuvent être modifiés que pour les appareils Android.

Cette section contient des informations sur la configuration des paramètres de la protection de l'appareil mobile contre l'accès non autorisé.

DANS CETTE SECTION

CONFIGURATION DE L'ANTIVOL

Afin de protéger les données sur l'appareil mobile de l'utilisateur contre tout accès non autorisé en cas de perte ou de vol de l'appareil, il convient de configurer les paramètres de l'Antivol.

La configuration des paramètres de l'Antivol est disponible uniquement pour les appareils Android.

Toutes les fonctions de l'Anti-Vol sont activées par défaut.

Pour configurer les paramètres de l'Antivol, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Antivol**.
3. Si vous souhaitez qu'en cas de perte ou de vol de l'appareil mobile, l'application envoie, sur exécution d'une commande de votre part, les coordonnées de la position de l'appareil à l'adresse électronique indiquée :
   a. Cochez la case **Activer la Géolocalisation**.
   b. Indiquez dans le champ ci-dessous l'adresse électronique à laquelle seront envoyés les messages contenant les données de géolocalisation de l'appareil.
4. Si vous souhaitez que l'application envoie, en cas de remplacement de la carte SIM, le nouveau numéro de téléphone de l'appareil à l'adresse électronique ou au numéro de téléphone indiqué :
   a. Cochez la case **Activer la Surveillance SIM**.
   b. Dans le champ **Envoyer le message par email**, indiquez l'adresse électronique du destinataire du message.
   c. Dans le champ **Envoyer le SMS vers un numéro de téléphone**, indiquez le numéro de téléphone du destinataire du message.

5. Si vous souhaitez qu'en cas de perte ou de vol de l'appareil mobile, l'application bloque celui-ci sur exécution d'une commande de votre part :

   a. Cochez la case **Activer le Verrouillage**.

   b. Si vous souhaitez verrouiller l'appareil mobile en cas de remplacement de la carte SIM, cochez la case **Verrouiller en cas de remplacement de la carte SIM**.

   c. Dans le champ **Texte en cas de verrouillage**, indiquez le texte du message qui sera affiché sur l'écran de l'appareil mobile verrouillé.

6. Si vous souhaitez qu'en cas de perte ou de vol de l'appareil mobile, l'application supprime les données de celui-ci sur exécution d'une commande de votre part :

   a. Cochez la case **Activer la Suppression**.

   b. Si vous souhaitez avoir la possibilité de supprimer à distance les données personnelles et professionnelles de l'appareil mobile de l'utilisateur, cochez la case **Supprimer les données d'entreprise**.

   c. Si vous souhaitez avoir la possibilité de supprimer à distance toutes les données de l'appareil mobile de l'utilisateur, cochez la case **Supprimer toutes les données**.

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

Les paramètres de protection des données contre l'accès non autorisé seront ainsi configurés sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DE L'ENVOI DE COMMANDES A L'APPAREIL MOBILE

Afin de protéger les données sur l'appareil mobile de l'utilisateur contre tout accès non autorisé en cas de perte ou de vol de l'appareil, il convient de configurer les paramètres d'envoi de commandes à l'appareil mobile.

Par défaut, l'envoi de commandes à l'appareil mobile est désactivé.

Pour configurer les paramètres d'envoi de commandes à l'appareil mobile, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Antivol**.

3. Dans le groupe de paramètres **Envoi de commandes** , procédez comme suit :

   a. Si vous souhaitez qu'en cas de perte ou de vol de l'appareil mobile, l'application détermine les coordonnées de la position de celui-ci sur exécution d'une commande de votre part, cochez la case **Géolocalisation**. La détermination des coordonnées géographiques est disponible uniquement pour les appareils Android et Windows Phone.

   b. Si vous souhaitez que l'application bloque l'appareil sur exécution d'une commande de votre part, cochez la case **Verrouillage**. Le verrouillage est disponible uniquement pour les appareils Android.

      Pour déverrouiller l'appareil mobile, l'utilisateur devra saisir le code à usage unique prévu à cet effet.

   c. Si vous souhaitez que l'application supprime les données de l'appareil sur exécution d'une commande de votre part, cochez la case **Suppression des données** et sélectionnez le type de données :

      - Si vous souhaitez que l'application supprime les données personnelles et professionnelles de l'appareil, sélectionnez **Données d'entreprise**.

- Si vous souhaitez que l'application supprime toutes les données de l'appareil, sélectionnez **Toutes les données**.

La suppression est disponible uniquement pour les appareils Android.

4. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Les paramètres d'envoi de commandes en cas de perte ou de vol de l'appareil seront ainsi configurés sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DE L'UTILISATION D'UN MOT DE PASSE A USAGE UNIQUE POUR LE DEVERROUILLAGE DE L'APPAREIL

Afin de déverrouiller l'appareil mobile de l'utilisateur lorsque celui-ci a été verrouillé par l'application en cas de perte ou de vol, un code à usage unique doit être saisi. Ce code à usage unique est généré par l'application et est unique pour chaque appareil mobile.

Pour configurer l'utilisation d'un mot de passe à usage unique pour le déverrouillage de l'appareil mobile, procédez comme suit :

1. Dans l'arborescence de la console du Kaspersky Security Center, sélectionnez l'entrée **Administration des appareils mobiles**.
2. A l'entrée **Administration des appareils mobiles**, sélectionnez le dossier **Appareils mobiles**.
3. Sélectionnez l'appareil mobile pour lequel vous souhaitez recevoir un code de déverrouillage à usage unique.
4. Cliquez-droit pour ouvrir le menu contextuel, puis sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés : <nom de l'appareil>** s'ouvre.
5. Dans la fenêtre **Propriétés**, choisissez la section **Applications**.
6. Sélectionnez l'application Kaspersky Endpoint Security puis cliquez sur le bouton **Propriétés**.

   La fenêtre **Paramètres de l'application Kaspersky Endpoint Security 10 Service Pack 1 for Mobile** s'ouvre.
7. Dans la fenêtre **Paramètres de l'application Kaspersky Endpoint Security 10 Service Pack 1 for Mobile**, sélectionnez **AntiVol**.
8. Dans le groupe **Envoi des instructions**, le champ **Code à usage unique** indiquera le code spécifique à l'appareil sélectionné que l'utilisateur doit saisir afin de déverrouiller son appareil mobile.
9. Cliquez sur le bouton **OK** pour enregistrer les modifications apportées.

CONFIGURATION DES PARAMETRES DE LA PROTECTION INTERNET

Afin de protéger les données personnelles de l'utilisateur de l'appareil mobile lors de la navigation sur Internet, il convient de configurer les paramètres d'accès aux sites sur la base de listes prédéfinies de sites Internet autorisés ou interdits.

La configuration des paramètres de la Protection Internet est disponible uniquement pour les appareils Android, Windows Phone et iOS.

La Protection Internet est activée par défaut : l'accès aux sites Internet des catégories **Phishing** et **Programme malveillant** est limité.

Pour configurer l'accès de l'utilisateur aux sites Internet, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Protection Internet**.

3. Dans le groupe de paramètres **Mode de fonctionnement** sélectionnez le mode de fonctionnement de la Protection Internet souhaité :

   - Si vous souhaitez que l'application limite l'accès de l'utilisateur aux sites Internet en fonction de leur contenu :

     a. sélectionnez l'élément **Interdire les sites Internet des catégories sélectionnées** dans le groupe de paramètres **Mode de fonctionnement**.

     b. Composez la liste des catégories interdites en cochant les cases des catégories de sites Internet pour lesquels l'application doit interdire l'accès à l'utilisateur. Vous pouvez indiquer l'adresse Internet complète du site (par exemple, pictures.example.com) ou utiliser des expressions régulières (par exemple, *.example.com).

   - Si vous souhaitez que l'application n'autorise l'accès qu'aux sites indiqués par l'administrateur :

     a. sélectionnez l'élément **Autoriser uniquement les sites Internet indiqués** dans le groupe de paramètres **Mode de fonctionnement**.

     b. Composez la liste des sites Internet en ajoutant les adresses des sites auxquels l'application ne bloquera pas l'accès.

   - Si vous souhaitez que l'application interdise l'accès à n'importe quel site Internet, sélectionnez l'élément **Interdire tous les sites Internet** dans le groupe de paramètres **Mode de fonctionnement**.

4. Si vous souhaitez lever les restrictions sur l'accès de l'utilisateur à certains sites en fonction du contenu, décochez la case **Activer la Protection Internet**.

5. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Les paramètres d'accès de l'utilisateur aux sites Internet seront ainsi configurés sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DE L'ADMINISTRATION DE L'APPAREIL

Les paramètres d'administration ne peuvent être modifiés que pour les appareils Android.

Cette section contient les informations sur la configuration des paramètres d'administration de l'appareil mobile.

DANS CETTE SECTION

CONFIGURATION DU MOT DE PASSE SYSTEME

Afin d'assurer la sécurité d'un appareil Android, il est indispensable de configurer le mot de passe système qui sera demandé au moment du démarrage de l'appareil.

Par défaut, Kaspersky Endpoint Security ne demande pas de saisir ou de définir un mot de passe système lors du démarrage de l'appareil mobile. Ce mot de passe doit compter quatre caractères minimum.

Pour configurer l'utilisation du mot de passe système, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Administration de l'appareil**.
3. Si vous souhaitez que l'application recherche l'existence d'un mot de passe système au démarrage de l'appareil, cochez la case **Imposer la définition d'un mot de passe pour déverrouiller l'appareil** dans le groupe **Sécurité**.

   Si l'application détecte qu'aucun mot de passe n'a été défini sur l'appareil, l'utilisateur devra en choisir un. Le mot de passe est affiché selon paramètres définis par l'administrateur.
4. Indiquez le nombre minimum de caractères dans le mot de passe.
5. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Les paramètres d'utilisation du mot de passe système seront ainsi configurés sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DE L'UTILISATION DU WI-FI, DE L'APPAREIL PHOTO ET DU BLUETOOTH

Afin d'assurer la sécurité de l'appareil Android, il est indispensable de configurer les paramètres d'utilisation du Wi-Fi, de l'appareil photo et du Bluetooth.

Par défaut, l'utilisateur peut utiliser le Wi-Fi, l'appareil photo et le Bluetooth sur l'appareil mobile sans aucune restriction.

Pour configurer l'utilisation du Wi-Fi, de l'appareil photo et du Bluetooth sur l'appareil mobile, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Administration de l'appareil**.
3. Dans le groupe **Restrictions**, configurez l'utilisation du module Wi-Fi, de l'appareil photo et du Bluetooth :
   - Si vous souhaitez désactiver le module Wi-Fi sur l'appareil mobile de l'utilisateur, cochez la case **Désactiver le Wi-Fi**.
   - Si vous souhaitez désactiver l'appareil photo sur l'appareil mobile de l'utilisateur, cochez la case **Désactiver la caméra**.

     L'appareil photo peut être désactivé sur les appareils Android dont la version est ultérieure à 4.0.
   - Si vous souhaitez désactiver la connectivité Bluetooth sur l'appareil mobile de l'utilisateur, cochez la case **Désactiver le Bluetooth**.
4. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Les restrictions relatives à l'utilisation du Wi-Fi, de l'appareil photo et du Bluetooth seront ainsi configurées sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DE TOUCHDOWN

Afin d'assurer une utilisation sécurisée de la messagerie professionnelle sur l'appareil mobile de l'utilisateur, il convient de configurer les paramètres du client de messagerie TouchDown.

Par défaut, les paramètres du client de messagerie TouchDown ne sont pas définis.

Pour configurer les paramètres client de messagerie TouchDown, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Administration de l'appareil**.
3. Dans le groupe **Profil TouchDown**, définissez les paramètres du client de messagerie TouchDown :
   - Indiquez l'adresse IP ou le nom DNS du serveur sur lequel se trouve le serveur de messagerie dans le champ **Adresse du serveur**.
   - Indiquez le nom du domaine Active Directory® dans lequel le compte utilisateur est enregistré dans le champ **Domaine**.
4. Si vous souhaitez établir un certificat dans le client de messagerie TouchDown, cochez la case **Ne pas vérifier le certificat du serveur**.

   Il faut au préalable ajouter ce certificat à l'appareil de l'utilisateur dans la Console d'administration Kaspersky Security Center à l'entrée **Comptes utilisateur**.
5. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Les paramètres du client de messagerie TouchDown seront ainsi configurés sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DES PARAMETRES AVANCES

Les paramètres avancés de la stratégie de groupe ne peuvent être modifiés que pour les appareils Android.

Cette section contient les informations sur la configuration complémentaires de Kaspersky Endpoint Security.

DANS CETTE SECTION

CONFIGURATION DU FILTRAGE DES APPELS ET DES SMS

Afin de bloquer les appels et SMS indésirables entrants sur l'appareil mobile de l'utilisateur, il convient de configurer les paramètres du Filtre des appels et des SMS.

Pour configurer les paramètres du Filtre des appels et des SMS, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Paramètres avancés**.

3. Cochez la case **Autoriser l'utilisation du Filtre des appels et des SMS**.

4. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Le filtrage des appels et SMS indésirables entrants sera ainsi autorisé sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée. L'utilisateur peut modifier les paramètres du Filtre des appels et des SMS via l'interface de l'application sur son appareil et consulter le journal des événements survenus pendant le fonctionnement du composant.

CONFIGURATION DES PARAMETRES DE SUPPRESSION DE KASPERSKY ENDPOINT SECURITY

Afin de supprimer Kaspersky Endpoint Security de l'appareil mobile de l'utilisateur, il convient de configurer les paramètres de suppression de l'application.

Pour configurer les paramètres de suppression de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Paramètres avancés**.

3. Dans le groupe **Administration de l'application**, configurez les paramètres de suppression à partir de l'appareil Android :

   - Si vous souhaitez que l'utilisateur puisse supprimer lui-même l'application de l'appareil mobile, cochez la case **Autoriser la suppression de Kaspersky Endpoint Security for Android**.

     Par défaut, l'utilisateur n'a pas la possibilité de supprimer lui-même l'application de l'appareil mobile.

   - Si vous souhaitez supprimer l'application lors de la prochaine synchronisation avec le Serveur d'Administration, cochez la case **Supprimer Kaspersky Endpoint Security for Android de l'appareil**.

4. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Les paramètres de suppression de l'application de l'appareil seront ainsi configurés sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DE LA CONNEXION AUX RESEAUX SANS FIL

Afin de connecter l'appareil mobile de l'utilisateur aux réseaux sans fil, il convient de configurer les paramètres de l'appareil mobile.

Les paramètres de connexion aux réseaux sans fil ne peuvent être modifiés que pour les appareils Android.

Pour modifier les paramètres de connexion aux réseaux sans fil, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Paramètres de l'appareil**.
3. Dans le groupe **Réseaux sans fil**, cliquez sur **Ajouter**.

   La fenêtre **Réseau sans fil** s'ouvre.
4. Dans le fenêtre **Réseau sans fil**, configurez les paramètres de connexion au réseau sans fil :
   a. Dans le champ **Identificateur du réseau SSID**, indiquez le nom du réseau sans fil contenant le point d'accès (SSID).
   b. Dans le groupe **Type de sécurité**, sélectionnez le type de sécurité du réseau sans fil (ouvert ou sécurisé selon les protocoles WEP ou WPA/WPA2 PSK).
   c. Si dans le champ précédent vous avez sélectionné un type de réseau sans fil sécurisé, indiquez le mot de passe pour accéder au réseau dans le champ **Mot de passe**.
   d. Dans le champ **Adresse du serveur proxy et port**, indiquez l'adresse IP ou le nom (adresse Internet) du serveur proxy et le numéro du port.

   Le réseau sans fil ajouté s'affichera dans la liste **Réseaux sans fil** de la section **Paramètres de l'appareil**.

   Vous pouvez modifier ou supprimer les réseaux sans fil mentionnés dans la liste des réseaux sans fil en cliquant sur les boutons **Modifier** et **Supprimer** de la partie supérieure de la liste.
5. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

L'utilisateur pourra ainsi se connecter au réseau sans fil ajouté sans avoir à indiquer les paramètres du réseau une fois la stratégie appliquée sur l'appareil mobile de l'utilisateur.

CONFIGURATION DU CONTROLE DES APPLICATIONS

Cette section contient les informations sur la configuration des paramètres du Contrôle des applications.

La configuration des paramètres du Contrôle des applications est disponible uniquement pour les appareils Android.

DANS CETTE SECTION

CONFIGURATION DES PARAMETRES DE LANCEMENT DES APPLICATIONS

Dans le but d'assurer la sécurité de l'appareil mobile de l'utilisateur, il est indispensable de configurer les paramètres de lancement des applications.

Pour définir les paramètres de lancement des applications sur l'appareil mobile, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Contrôle des applications**.

3. Dans le groupe **Mode de fonctionnement**, sélectionnez le mode de lancement des applications sur l'appareil mobile de l'utilisateur :

   - Si vous souhaitez que l'utilisateur de l'appareil mobile puisse lancer toutes les applications, à l'exception de celles indiquées comme interdites dans la Liste des catégories et des applications, sélectionnez le mode **Applications interdites**.

   - Si vous souhaitez que l'utilisateur de l'appareil mobile puisse lancer uniquement les applications indiquées comme autorisées, recommandées ou obligatoires dans la Liste des catégories et des applications, sélectionnez le mode **Applications autorisées**.

4. Si vous souhaitez que Kaspersky Endpoint Security compose un rapport sur les applications interdites installées sur l'appareil mobile de l'utilisateur, sans pour autant les bloquer, cochez la case **Ne pas bloquer les applications interdites, se limiter au rapport**.

   Lors de la synchronisation suivante de l'appareil mobile de l'utilisateur avec le Serveur d'administration, Kaspersky Endpoint Security génère le rapport **Une application interdite est installée** qui peut être consulté dans la Console d'administration de Kaspersky Endpoint Security ou dans les propriétés locales de l'application.

5. Si vous souhaitez que Kaspersky Endpoint Security bloque l'exécution des applications système sur l'appareil mobile de l'utilisateur en mode **Applications autorisées**, cochez la case **Bloquer les applications système**.

6. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Le mode de lancement des applications sera ainsi configuré sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DE L'INSTALLATION DES APPLICATIONS TIERCES

Conformément aux exigences relatives à la sécurité de l'entreprise, les applications mobiles tierces peuvent être installées sur les appareils des utilisateurs en tant qu'applications autorisées, recommandées ou obligatoires. Vous pouvez télécharger les Paquets d'applications mobiles (cf. section "Paquet d'applications mobiles" à la page **Error! Bookmark not defined.**) créés plus tôt dans le Kaspersky Security Center. En outre, vous pouvez placer une application mobile tierce dans le conteneur (cf. section "Présentation des conteneurs", à la page 78) et la télécharger sur l'appareil mobile de l'utilisateur (cf. section "Création des conteneurs", à la page 79) afin d'assurer la protection des données de l'entreprise.

Pour configurer les paramètres d'installation d'une application mobile tierce sur l'appareil de l'utilisateur, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Contrôle des applications**.

3. Cliquez sur le bouton **Application**.

   La fenêtre **Application mobile** s'ouvre.

4. Indiquez le paquet de l'application mobile de l'une des manières suivantes :

   - Cliquez sur le bouton **Sélectionner** situé à droite du champ **Nom du paquet** et, dans la fenêtre **Paquets d'applications mobiles** qui s'ouvre, sélectionnez le paquet de l'application mobile.

   - Indiquez manuellement le paquet d'applications mobiles :

     a. Sélectionnez le nom système du paquet de l'application mobile dans le champ **Nom du paquet**.

     b. Dans le champ **Nom de l'application**, saisissez le nom du paquet de l'application mobile qui s'affiche sur l'appareil et dans la liste des catégories et des applications.

     c. Dans le champ **Lien vers la distribution**, sélectionnez l'adresse Internet du serveur HTTP où se trouve le paquet de l'application mobile au format http://<server>:<port>. Vous pouvez indiquer l'adresse du serveur Internet Kaspersky Security Center ou celle d'un autre serveur HTTP.

5. Dans la liste **Type d'application**, sélectionnez l'option **Autorisée**, **Interdite**, **Obligatoire** ou **Recommandée**, conformément aux exigences relatives à la sécurité de l'entreprise.

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

   Le paquet de l'application mobile ajouté s'affiche dans la liste des catégories et des applications de la section **Contrôle des applications**.

   > Vous pouvez modifier ou supprimer les paquets d'applications mentionnées dans la liste des catégories et des applications en cliquant sur les boutons **Modifier** et **Supprimer** de la partie supérieure de la liste.

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

Les listes des applications autorisées, interdites, obligatoires et recommandées seront ainsi envoyées à l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

L'utilisateur installe lui-même l'application sur l'appareil mobile en la sélectionnant dans la liste. En cas de tentative d'installation d'une application interdite, Kaspersky Endpoint Security peut bloquer l'application ou générer le rapport **Une application interdite est installée** (cf. section "**Configuration des paramètres de lancement des applications**" à la page 76).

CONFIGURATION DU RAPPORT SUR LES APPLICATIONS INSTALLEES

Vous pouvez consulter les informations relatives aux applications installées sur l'appareil mobile de l'utilisateur à l'aide du rapport sur les applications installées.

Pour configurer la génération du rapport sur les applications installées sur l'appareil mobile de l'utilisateur, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Contrôle des applications**.

3. Dans le groupe **Liste des applications installées** cochez la case **Demander la liste des applications installées**.

   Kaspersky Endpoint Security génère alors le rapport **Liste des applications installées** lors de la synchronisation de l'appareil mobile de l'utilisateur avec le Serveur d'Administration. Un rapport est généré à chaque modification apportée à la liste des applications installées sur l'appareil mobile de l'utilisateur.

4. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

La génération du rapport sur les applications installées sera ainsi activée sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée. Le rapport généré peut être consulté dans la Console d'administration de Kaspersky Endpoint Security à l'entrée **Rapports et notifications** ou dans les propriétés locales de l'application (cf. *Manuel de l'administrateur du Kaspersky Security Center*).

ADMINISTRATION DES APPLICATIONS MOBILES TIERCES

Cette section décrit les différents moyens d'installer des applications mobiles tierces utilisées dans un but professionnel sur les appareils mobiles des utilisateurs.

DANS CETTE SECTION

PRESENTATION DES CONTENEURS

Vous pouvez utiliser des conteneurs afin de contrôler l'activité des applications mobiles lancées sur l'appareil de l'utilisateur. Le *conteneur* est une enveloppe spéciale pour les applications mobiles qui permet de contrôler les activités des applications qu'il contient afin de protéger les données personnelles et d'entreprise stockées dans l'appareil.

Vous pouvez placer seul des applications tierces dans un conteneur. Pour placer l'application dans un conteneur, il faut créer le paquet de l'application mobile dans la Console d'administration (cf. section "Création de conteneurs" à la page 79). La distribution de l'application dans le conteneur est alors placée automatiquement sur le serveur Internet du Kaspersky Security Center.

Les conteneurs peuvent être utilisés uniquement sur des appareils Android et iOS. Pour utiliser l'application du conteneur sur les appareils iOS, le conteneur créé doit être signé. Les conteneurs sont régis par le même certificat que le programme d'installation de Kaspersky Endpoint Security for iOS.

Les paramètres de fonctionnement des conteneurs sur les appareils sont définis par la stratégie appliquée au groupe d'appareils mobiles. Les propriétés de la stratégie permettent de configurer les paramètres suivants pour les conteneurs :

- Possibilité de chiffrer automatiquement les données de l'application dans le conteneur sur l'appareil de l'utilisateur.
- Utilisation de l'autorisation de l'utilisateur lors du lancement de l'application dans le conteneur.

  Pour identifier l'utilisateur, vous pouvez configurer les types d'autorisation suivants :

  - Noms d'utilisateur et mots de passe de domaine. Lors du lancement de l'application dans le conteneur sur l'appareil, l'utilisateur saisit son nom d'utilisateur et son mot de passe Active Directory®.
  - Mot de passe défini par l'utilisateur au premier lancement de l'application dans le conteneur.
- Restriction sur la conservation des données de l'application dans le conteneur sur l'appareil de l'utilisateur.
- Restriction sur l'envoi de données à partir de l'application du conteneur vers d'autres applications mobiles.
- Restriction de l'accès de l'application dans le conteneur à Internet.
- Contrôle de l'envoi de SMS par l'application dans le conteneur sur des appareils Android.
- Contrôle de la réalisation d'appels par l'application dans le conteneur sur des appareils Android.

Vous pouvez utiliser une des méthodes suivantes pour installer l'application dans le conteneur sur l'appareil de l'utilisateur :

- envoyer un message électronique à l'utilisateur contenant un lien vers la distribution de l'application dans le conteneur.
- dans la section **Contrôle des applications** des propriétés de la stratégie, désigner l'application dans le conteneur comme obligatoire ou autorisée pour installation. Suite à la synchronisation de l'appareil mobile avec le Serveur d'administration, la distribution de l'application figurant dans le conteneur est automatiquement copiée sur l'appareil de l'utilisateur.

CREATION DE CONTENEURS

Pour créer un conteneur, 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 la zone de travail du dossier **Paquets d'installation**, cliquez sur le lien **Administrer les paquets d'applications mobiles** pour ouvrir la fenêtre **Administration des paquets d'applications mobiles**.
3. Dans la fenêtre **Administration des paquets d'applications mobiles**, cliquez sur le bouton **Nouveau**.

   L'Assistant de création de paquet d'applications mobiles s'ouvre.
4. Dans le champ **Nom** de la fenêtre **Indiquez le nom du nouveau paquet** de l'Assistant, saisissez le nom du conteneur.

5. Dans le champ **Sélectionnez l'application** de la fenêtre **Paramètres** de l'Assistant, désignez le fichier de l'application mobile que vous souhaitez placer dans le conteneur :

   - Si vous souhaitez créer un conteneur pour appareils Android, choisissez la distribution de l'application mobile avec l'extension apk.

   - Si vous souhaitez créer un conteneur pour appareils iOS, sélectionnez le fichier de l'application portant l'extension ipa ou la distribution de l'application dans l'archive zip (pour Mac OS, extension app).

6. Cochez la case **Créer un conteneur avec l'application sélectionnée**.

   L'application ajoute le conteneur créé à la liste des paquets autonomes dans la fenêtre **Administration des paquets d'applications mobiles**. Le champ **Chemin d'accès** de cette fenêtre reprend le chemin d'accès à l'emplacement où le conteneur est placé automatiquement sur le Serveur d'administration. Le champ **URL** de cette fenêtre reprend le lien vers le serveur Web de Kaspersky Security Center sur lequel le conteneur est automatiquement placé.

   Si vous ne souhaitez pas que le conteneur soit placé sur le serveur Web du Kaspersky Security Center, cliquez sur le bouton **Annuler la publication**.

   Si vous souhaitez envoyer le lien à l'utilisateur directement par courrier électronique pour qu'il télécharge l'application dans le conteneur de son appareil mobile, cliquez sur le bouton **Envoyer par e-mail**.

   Si vous souhaitez enregistrer l'application dans le conteneur localement sur votre poste de travail ou sur le réseau, cliquez sur le bouton **Enregistrer sous**.

Pour pouvoir utiliser le conteneur sur des appareils Android, il n'est pas nécessaire de signer l'application dans le conteneur. Pour utiliser le conteneur sur des appareils iOS, il est nécessaire de signer l'application placée dans le conteneur (cf. section "Signature des applications du conteneur en vue de leur utilisation sur des appareils iOS" à la page 80).

Signature des applications du conteneur en vue de leur utilisation sur des appareils iOS

La signature des applications placées dans le conteneur s'effectue à l'aide de l'utilitaire make_container. Cet utilitaire se trouve dans l'archive SigningUtility.zip qui figure dans la distribution de Kaspersky Endpoint Security.

Pour lancer l'utilitaire make_container, l'ordinateur doit tourner sous Mac OS. L'utilitaire make_container est une application de console. Pour le lancer, utilisez le terminal via **Applications → Utilitaires → Terminal**.

Exemple d'utilisation de la commande pour signer la distribution de Kaspersky Endpoint Security :

Texte de la commande :

./make_container -s --sign 6267202d6d2b595a9e345fe4d8c87777218bede2 ksm.cnt.com.atebits.Tweetie2 ./DevelopProf.mobileprovision -o ./output.ipa ./input.app

où figurent les paramètres suivants :

6267202d6d2b595a9e345fe4d8c87777218bede2 – cache du certificat de développeur que vous utilisez. Le cache apparaît dans les propriétés du certificat du développeur importé dans Key Chain Access.

ksm.cnt.com.atebits.Tweetie2 – ID de l'application.

./DevelopProf.mobileprovision – chemin d'accès au dossier contenant le profil d'approvisionnement.

./output.ipa – chemin d'accès au dossier qui contiendra la distribution signée de l'application.

./input.app – chemin d'accès au dossier qui contiendra la distribution non signée de l'application.

Pour signer l'application dans le conteneur, procédez comme suit :

1. Créez un conteneur dans la Console d'administration (cf. section "Création de conteneurs" à la page 79).
2. Ouvrez le dossier contenant la distribution de l'application que vous souhaitez signer.
3. Sur l'ordinateur sous Mac OS, lancez le terminal via **Applications** → **Utilitaires** → **Terminal**.
4. Sur la ligne de commande du terminal, saisissez cd afin d'ouvrir le dossier contenant l'utilitaire make_container.
5. Sur la ligne de commande du terminal, saisissez la commande qui lance l'utilitaire make_container avec les arguments obligatoires suivants :

   -s --sign – arguments pour la signature de la distribution de l'application. Les paramètres suivants sont définis pour cette clé :

   - cache du certificat du développeur depuis Key Chain Access;
   - ID Apple de l'application de Kaspersky Security Center;

   Il est déconseillé de changer l'identifiant Apple de l'application signée du conteneur. Si vous modifiez l'identifiant Apple, vous ne pourrez pas appliquer la stratégie à l'application sur l'appareil mobile.

   - chemin d'accès au profil d'approvisionnement.

   -o – désigne le chemin d'accès au fichier qui sera créé et signé. Les paramètres suivants sont définis pour cette clé :

   - chemin d'accès à la distribution signée de l'application portant l'extension ipa;
   - chemin d'accès à la distribution non signée de l'application avec l'extension app / app.zip| / ipa/.

   Après l'exécution de la commande saisie, une distribution signée de l'application dans le conteneur est créée.
6. Si vous souhaitez créer un fichier manifest avec le conteneur signé, exécutez la commande décrite ci-dessus avec l'argument -m :

   -m – argument pour la création d'un fichier manifest. Les paramètres suivants sont définis pour cette clé :

   - abréviation du nom de l'application pour l'entrée dans le fichier manifest ;
   - nom complet de l'application pour l'entrée dans le fichier manifest ;
   - chemin d'accès au serveur externe qui hébergera la distribution signée de l'application pour l'entrée dans le fichier manifest ;
   - lien vers le fichier de la petite icône de l'application (paramètre facultatif) ;
   - lien vers le fichier de la grande icône de l'application (paramètre facultatif).

CONFIGURATION DU CONTROLE DE LA CONFORMITE DES APPAREILS MOBILES A LA STRATEGIE DE GROUPE

Cette section décrit l'utilisation du module Contrôle de la conformité de l'application.

Vous pouvez vérifier la conformité des appareils mobiles à la stratégie de groupe à l'aide du module d'application Contrôle de la conformité. Le Contrôle de la conformité s'assure que les appareils mobiles sont conformes à la stratégie et, si nécessaire, modifie le fonctionnement des appareils à l'aide des règles d'analyse. Vous pouvez vérifier régulièrement la conformité des appareils mobiles des utilisateurs vis-à-vis de la stratégie de groupe. Les résultats de la vérification sont consignés dans un rapport.

Vous pouvez vérifier la conformité des appareils Android à la stratégie de groupe.

DANS CETTE SECTION

PRESENTATION DU CONTROLE DE LA CONFORMITE

Le Contrôle de la conformité des appareils KES à la stratégie de groupe est effectué à l'aide des règles de vérification. Les règles de vérification contiennent :

- Les critères de conformité de l'appareil à la stratégie de groupe. Un critère est un paramètre défini de la stratégie de groupe.
- Les actions que l'application exécute sur l'appareil si celui-ci ne répond pas aux critères de conformité à la stratégie de groupe.
- La restriction temporaire correspond à la durée suivant la vérification de l'appareil pendant laquelle l'utilisateur peut corriger lui-même les non conformités à la stratégie de groupe décelées sur l'appareil. Pendant la période de restriction temporaire, l'application n'exécute pas l'action indiquée dans la règle sur l'appareil.

La règle de vérification des appareils mobiles peut être définie dans les propriétés de la stratégie de groupe à l'aide de l'assistant de création des règles de vérification (cf. section "Création d'une stratégie de groupe", à la page 61). Vous pouvez activer ou désactiver la règle de vérification créée dans la section **Contrôle de la conformité**, dans le groupe **Règles de vérification** (cf. section "**Définition des règles de vérification de la conformité**" à la page 84). Vous pouvez activer une ou plusieurs règles de vérification. L'activation de la règle de vérification s'effectue à chaque synchronisation des appareils mobiles avec le Serveur d'administration.

Critères de vérification des appareils

Les critères de vérification font partie des paramètres de la stratégie de groupe. Vous pouvez définir les critères de la vérification à la première étape de l'Assistant de création d'une règle de vérification.

La vérification de la conformité des appareils des utilisateurs à la stratégie de groupe peut être exécutée selon les critères suivants :

- **La protection en temps réel est activée**. L'application vérifie l'utilisation de la protection antivirus sur l'appareil mobile.
- **Les bases antivirus sont à jour**. L'application vérifie l'actualité des bases de l'application Kaspersky Endpoint Security for Android sur l'appareil mobile. Par défaut, la valeur seuil au-delà de laquelle les bases antivirus sont considérées comme dépassées est fixée à 10 jours.
- **Absence d'applications interdites**. L'application recherche la présence d'applications interdites sur l'appareil mobile. Vous pouvez composer une liste des applications interdites dans les propriétés de la stratégie, dans la section **Contrôle des applications**.
- **Absence d'applications de catégories interdites**. L'application recherche la présence d'applications appartenant à des catégories interdites sur l'appareil mobile. Vous pouvez composer une liste des catégories interdites dans les propriétés de la stratégie, dans la section **Contrôle des applications**.
- **Toutes les applications requises sont installées**. L'application vérifie la présence de toutes les applications obligatoires sur l'appareil mobile. Vous pouvez composer une liste des applications obligatoires dans les propriétés de la stratégie, dans la section **Contrôle des applications**.
- **La version du système d'exploitation est à jour**. L'application vérifie la version du système d'exploitation de l'appareil mobile. L'Assistant de création d'une règle de vérification permet d'indiquer la plage de versions de systèmes d'exploitation pouvant être utilisés sur l'appareil de l'utilisateur.
- **L'appareil se synchronise régulièrement**. L'application vérifie la régularité de la synchronisation de l'appareil avec le Serveur d'administration. Vous pouvez indiquer un intervalle maximal entre les synchronisations dans l'Assistant de création d'une règle d'analyse.
- **Système d'exploitation non piraté**. L'application vérifie l'intégrité du système d'exploitation de l'appareil.
- **Le mot de passe de l'appareil est conforme aux directives de l'entreprise**. L'application vérifie le nombre de caractères dans le mot de passe système de l'utilisateur. Vous pouvez indiquer le nombre minimal de caractères pour le mot de passe de l'utilisateur dans les propriétés de la stratégie, sous l'onglet **Gestion de l'appareil**.

Actions et restrictions temporaires

Vous pouvez restreindre l'utilisation des appareils mobiles non conformes aux critères de vérification et supprimer les données personnelles et professionnelles qui s'y trouvent. Pour ce faire, dans l'Assistant de création de règles de vérification, vous devez composer une liste des actions à exécuter sur les appareils et indiquer une restriction temporaire pour chacune d'entre elle. La restriction temporaire correspond à la durée suivant la vérification de l'appareil pendant laquelle l'utilisateur peut corriger lui-même les non conformités aux exigences. Si, à l'issue de cette période, l'utilisateur n'a pas corrigé les non conformités, l'application applique les actions que vous avez indiquées dans la règle de vérification.

Vous pouvez indiquer les actions suivantes :

- **Interdire l'accès à la messagerie de l'entreprise (TouchDown)**. L'application Kaspersky Endpoint Security for Android de l'appareil de l'utilisateur bloque le lancement du client de messagerie TouchDown et l'accès à la messagerie de l'entreprise.
- **Interdire le lancement de toutes les applications**. L'application Kaspersky Endpoint Security for Android bloque le lancement de toutes les applications mobiles sur l'appareil de l'utilisateur.
- **Verrouiller**. L'application Kaspersky Endpoint Security for Android bloque l'appareil de l'utilisateur.

- **Supprimer les données d'entreprise**. L'application Kaspersky Endpoint Security for Android supprime les données d'entreprise suivantes de l'appareil de l'utilisateur :
  - données des conteneurs ;
  - paramètres du réseau sans fil de l'entreprise ;
  - paramètres du point d'accès de l'entreprise (APN, VPN).
- **Supprimer toutes les données**. L'application Kaspersky Endpoint Security for Android supprime toutes les données de l'appareil de l'utilisateur (telles que les données de la carte mémoire ou des conteneurs, les certificats et les points d'accès Wi-Fi).

Si les mêmes actions sont prescrites dans plusieurs règles, l'application les exécute une fois seulement. Si différentes restrictions de durée sont indiquées pour une seule et même action, l'application applique la restriction de durée la plus basse. Si, suite à la deuxième vérification des appareils, les paramètres de ceux-ci satisfont aux critères, l'application lève les restrictions imposées.

DEFINITION DES REGLES DE VERIFICATION DE LA CONFORMITE

Pour définir une règle de vérification de la conformité des appareils par rapport à la stratégie de groupe de Kaspersky Endpoint Security for Mobile, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Contrôle de la conformité**.
3. Si vous souhaitez recevoir des notifications indiquant que des appareils non conformes à la stratégie ont été détectés, dans le groupe **Notifications sur la non-conformité**, cochez la case **Avertir l'administrateur**.

   Lorsque Kaspersky Endpoint Security détecte une irrégularité vis-à-vis de la stratégie, elle profite de la synchronisation de l'appareil mobile avec le Serveur d'administration pour générer le rapport **Non-conformité détectée : <nom du critère d'analyse>**. Ce rapport peut être consulté dans la Console d'administration du Kaspersky Security Center ou dans les propriétés locales du programme.
4. Si vous souhaitez notifier l'utilisateur à propos de la non conformité de son appareil mobile et des applications qu'il comporte, dans le groupe **Notifications sur la non-conformité**, cochez la case **Avertir l'utilisateur**.

   Lorsque Kaspersky Endpoint Security détecte une irrégularité de conformité à la stratégie, elle profite de la synchronisation de l'appareil mobile avec le Serveur d'administration pour avertir l'utilisateur dans la section **Etat** du groupe **Sécurité d'entreprise**.
5. Dans le groupe **Règles d'analyse**, composez la liste des règles de vérification de la conformité des appareils à la stratégie. Pour ce faire, procédez comme suit :
   a. Cliquez sur le bouton **Ajouter**.

      Lance l'Assistant de création des règles d'analyse.
   b. Suivez les instructions de l'Assistant pour la création des règles d'analyse.

      Une fois le travail de l'Assistant terminé, la nouvelle règle de vérification de la conformité de l'appareil vis-à-vis de la stratégie s'affiche dans le groupe **Règles d'analyse** de la liste des règles de vérification.

Vous pouvez modifier et supprimer les règles dans la liste des règles de vérification en cliquant sur les boutons **Modifier** et **Supprimer** de la partie supérieure de la liste.

6. Si vous souhaitez désactiver temporairement la règle créée, utilisez l'interrupteur en face de la règle sélectionnée.

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

Kaspersky Endpoint Security vérifie la conformité des appareils mobiles des utilisateurs par rapport à la stratégie lors de leur synchronisation au Serveur d'administration. S'il détecte une non conformité sur l'appareil mobile d'un utilisateur, il y applique les restrictions que vous avez définies dans la liste des règles de vérification.

CONFIGURATION DE L'ACTIVATION DE L'APPLICATION

Les paramètres de la stratégie vous permettent de configurer l'activation de l'application sur l'appareil mobile de l'utilisateur.

Pour configurer les paramètres d'activation de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Licence**.

3. Dans le groupe **Licence**, dans la liste déroulante **Clé**, sélectionnez la clé d'activation de l'application dans le stockage des clés du Serveur d'Administration du Kaspersky Security Center.

   Le champ ci-dessous affiche les informations sur l'application correspondant à la licence acquise, la durée de validité de la licence et son type.

4. Afin d'activer l'application sur l'appareil mobile de l'utilisateur, verrouillez la modification des paramètres.

5. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

L'application Kaspersky Endpoint Security sera ainsi activée sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DE L'ADMINISTRATION DES APPAREILS SAMSUNG

Cette section contient des informations sur la configuration des paramètres d'administration des appareils Android Samsung prenant en charge l'utilisation de Samsung KNOX. La configuration des paramètres est effectuée dans les propriétés de la stratégie de groupe appliquée aux appareils mobiles Samsung.

DANS CETTE SECTION

CONFIGURATION DES PARAMETRES GENERAUX POUR SAMSUNG KNOX

Afin de transmettre des données sur l'appareil mobile de l'utilisateur, il convient de configurer les paramètres du point d'accès (APN).

Pour pouvoir utiliser le point d'accès sur l'appareil mobile de l'utilisateur, l'appareil doit être doté d'une carte SIM. Les paramètres du point d'accès sont fournit par l'opérateur de téléphonie mobile. Une erreur de configuration du point d'accès pourrait entraîner des frais supplémentaires de communication mobile.

La configuration des paramètres du point d'accès (APN) est disponible pour les appareils Android Samsung prenant en charge l'utilisation de Samsung KNOX toutes versions confondues.

Pour configurer les paramètres du point d'accès (APN) pour l'appareil mobile de l'utilisateur, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Administration des appareils Samsung**.
3. Dans le groupe **Point d'accès (APN)**, cliquez sur le bouton **Configurer**.

   La fenêtre **Paramètres du point d'accès (APN)** s'ouvre.
4. Sous l'onglet **Paramètres principaux**, indiquez les paramètres suivants pour le point d'accès :
   a. Dans la liste déroulante **Type de point d'accès**, sélectionnez le type de point d'accès.
   b. Dans le champ **Nom du point d'accès**, indiquez le nom du point d'accès.
   c. Dans le champ **Adresse du serveur**, indiquez le nom de réseau du serveur de l'opérateur mobile fournissant l'accès aux services de transfert des données.
   d. Dans le champ **MCC**, indiquez le code mobile du pays (MCC).
   e. Dans le champ **MNC**, indiquez le code mobile du réseau (MNC).
   f. Si vous avez sélectionné **MMS** ou **Internet et MMS** comme type de point d'accès, indiquez les paramètres avancés pour les MMS :
      - Dans le champs **Serveur pour les MMS**, indiquez le nom de domaine complètement qualifié du serveur de l'opérateur mobile dédié à l'échange de MMS.
      - Dans le champ **Serveur proxy pour les MMS**, indiquez le nom réseau ou l'adresse IP et le numéro de port du serveur proxy de l'opérateur mobile dédié à l'échange de MMS.
5. Sous l'onglet **Avancé**, configurez les paramètres avancés du point d'accès (APN) :
   a. Dans la liste déroulante **Type d'autorisation**, sélectionnez le type d'autorisation de l'utilisateur de l'appareil mobile sur le serveur de l'opérateur mobile fournissant l'accès au réseau.
   b. Dans le champ **Adresse du serveur proxy**, indiquez le nom réseau ou l'adresse IP du serveur proxy et le numéro de port du serveur proxy de l'opérateur mobile fournissant l'accès au réseau.
   c. Dans le champ **Nom de l'utilisateur**, indiquez le nom de l'utilisateur pour l'autorisation sur le réseau mobile.

d. Dans le champ **Mot de passe**, indiquez le mot de passe pour l'autorisation de l'utilisateur sur le réseau mobile.

6. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Les paramètres généraux du point d'accès (APN) seront ainsi configurés sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DU PARE-FEU POUR SAMSUNG KNOX

Afin de contrôler les connexions réseau sur l'appareil mobile de l'utilisateur, il convient de configurer les paramètres du Pare-feu.

La configuration des paramètres du Pare-feu est disponible pour les appareils Android Samsung prenant en charge l'utilisation de Samsung KNOX toutes versions confondues.

Pour configurer le mode de fonctionnement du Pare-feu sur l'appareil mobile, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Administration des appareils Samsung** :

   - Si l'appareil mobile prend en charge l'utilisation de Samsung KNOX version 1, sélectionnez la section **Paramètres pour KNOX 1**.

   - Si l'appareil mobile prend en charge l'utilisation de Samsung KNOX version 2, sélectionnez la section **Paramètres pour KNOX 2**.

3. Dans le groupe **Pare-feu**, cliquez sur **Configurer**.

   La fenêtre **Mode de fonctionnement du Pare-feu** s'ouvre.

4. Sélectionnez le mode de fonctionnement du Pare-feu :

   - Si vous souhaitez autoriser toutes les connexions entrantes et sortantes sur l'appareil mobile, déplacez le curseur jusqu'à la position **Autoriser toutes**.

   - Si vous souhaitez que l'application bloque toute activité réseau, exceptée celle des applications de la liste des exclusions, déplacez le curseur jusqu'à la position **Bloquer toutes, sauf les exclusions**.

5. Si vous avez sélectionné le mode de fonctionnement du Pare-feu **Bloquer toutes, sauf les exclusions**, composez la liste des exclusions :

   a. Cliquez sur le bouton **Ajouter**.

      La fenêtre **Exclusion** s'ouvre.

      - Dans le champ **Nom de l'application**, saisissez le nom de l'application mobile.

      - Sélectionnez le nom système du paquet de l'application mobile dans le champ Nom du paquet.

   Vous pouvez modifier ou supprimer les applications mentionnées dans la liste des exclusions en cliquant sur les boutons **Modifier** et **Supprimer** de la partie supérieure de la liste.

6. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Les paramètres de filtrage des connexions réseau entrantes et sortantes seront ainsi configurés sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION D'UN RESEAU PRIVE VIRTUEL POUR SAMSUNG KNOX 1

Afin de connecter l'appareil mobile de l'utilisateur à un réseau privé virtuel en toute sécurité, il convient de configurer les paramètres de connexion de l'appareil à un réseau VPN.

Pour configurer la connexion VPN sur l'appareil mobile de l'utilisateur, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Administration des appareils Samsung**.

3. Sélectionnez la section **Paramètres pour KNOX 1**.

4. Dans le groupe **Réseau privé virtuel (VPN)**, cliquez sur le bouton **Configurer**.

   La fenêtre **Paramètres du réseau privé virtuel (VPN)** s'ouvre.

5. Dans la liste déroulante **Type de réseau**, sélectionnez le type de connexion VPN.

6. Saisissez le nom du tunnel VPN dans le champ **Nom**.

7. Dans le champ **Adresse du serveur**, saisissez le nom réseau ou l'adresse IP du serveur VPN.

8. Dans le champ **Domaine(s) de recherche DNS**, saisissez le domaine de recherche DNS qui sera automatiquement ajouté aux noms de serveur DNS.

   Vous pouvez saisir plusieurs domaines de recherche DNS en les séparant à l'aide d'un espace.

9. Dans le champ **Serveur(s) DNS**, saisissez le nom de domaine complètement qualifié ou l'adresse IP du serveur DNS.

   Vous pouvez saisir plusieurs serveurs DNS en les séparant à l'aide d'un espace.

10. Dans le champ **Redirection ICMP**, saisissez la plage d'adresses IP du réseau avec lesquelles s'effectue l'échange de données via la connexion VPN.

    Si le champ **Redirection ICMP** ne contient pas la plage des adresses IP, l'ensemble du trafic Internet passera par la connexion VPN.

11. Pour les types de réseau IPSEC_XAUTH_PSK et L2TP_IPSEC_PSK vous pouvez également configurer les paramètres suivants :

    a. Dans le champ **Clé IPSec partagée**, saisissez le mot de passe de la clé de sécurité IPSec préalablement installée.

    b. Dans le champ **Identifiant IPSec**, saisissez le nom de l'utilisateur de l'appareil mobile.

12. Pour le type de réseau L2TP_IPSEC_PSK, vous pouvez également indiquer le mot de passe pour la clé L2TP dans le champ **Clé L2TP**.

13. Pour le type de réseau PPTP, vous pouvez cocher la case **Utiliser le chiffrement** pour que l'application utilise la méthode de chiffrement MPPE afin d'assurer la sécurité du transfert de données lors de la connexion de l'appareil au serveur VPN.

14. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Les paramètres du réseau privé virtuel pour Samsung KNOX 1 seront ainsi configurés sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

Il convient de prendre en compte les exigences suivantes lors de l'utilisation d'un réseau privé virtuel :

- L'application utilisant la connexion VPN doit être autorisée dans les paramètres du Pare-feu (cf. section "Configuration du Pare-feu pour Samsung KNOX" à la page 87).
- Les paramètres du réseau privé virtuel définis dans la stratégie ne peuvent pas s'appliquer aux applications système. Pour les applications système, la connexion VPN doit être configurée manuellement.
- Certaines applications utilisant la connexion VPN requièrent une configuration complémentaire lors du premier lancement. Afin d'effectuer la configuration, la connexion VPN doit être autorisée dans les paramètres de l'application.

CONFIGURATION DE MICROSOFT EXCHANGE POUR SAMSUNG KNOX

Afin d'assurer une utilisation sécurisée de la messagerie professionnelle sur l'appareil mobile de l'utilisateur, il convient de configurer les paramètres du serveur de messagerie Microsoft Exchange.

La configuration des paramètres du serveur de messagerie Microsoft Exchange est disponible pour les appareils Android Samsung prenant en charge l'utilisation de Samsung KNOX toutes versions confondues.

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration de l'application mobile Kaspersky Endpoint Security (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils KES" à la page 63).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Administration des appareils Samsung**.
   - Si l'appareil mobile prend en charge l'utilisation de Samsung KNOX version 1, sélectionnez la section **Paramètres pour KNOX 1**.
   - Si l'appareil mobile prend en charge l'utilisation de Samsung KNOX version 2, sélectionnez la section **Paramètres pour KNOX 2**.
3. Dans le groupe **Serveur de messagerie Exchange**, cliquez sur le bouton **Configurer**.

   La fenêtre **Paramètres du serveur de messagerie Exchange** s'ouvre.
4. Dans le champ **Adresse du serveur**, saisissez l'adresse IP ou le nom DNS du serveur sur lequel se trouve le serveur de messagerie.
5. Dans le champ **Domaine Exchange ActiveSync**, saisissez le nom du domaine de l'utilisateur de l'appareil mobile sur le réseau de l'entreprise.
6. Dans la liste déroulante **Période de synchronisation**, sélectionnez la période souhaitée pour la synchronisation de l'appareil mobile avec le serveur Microsoft Exchange.
7. Si vous souhaitez utiliser le protocole de transfert de données SSL, cochez la case **Utiliser le chiffrement (SSL)**.
8. Si vous souhaitez utiliser des certificats numériques afin de protéger l'échange de messages entre l'appareil mobile et le serveur Microsoft Exchange, cochez la case **Vérifier le certificat du serveur**.
9. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Les paramètres du serveur de messagerie Microsoft Exchange seront ainsi configurés sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DE LA STRATEGIE DE GROUPE POUR L'ADMINISTRATION DES APPAREILS EAS

La stratégie d'administration permet de configurer les paramètres de fonctionnement des appareils EAS : la robustesse du mot de passe, la synchronisation avec le serveur Microsoft Exchange, la restriction des fonctionnalités de l'appareil mobile et les restrictions relatives au fonctionnement des applications. Les stratégies permettent de définir de façon centralisée les mêmes valeurs de paramètres de fonctionnement des appareils mobiles faisant partie du groupe d'administration.

Pour ouvrir la fenêtre des propriétés de la stratégie d'administration des appareils EAS afin de configurer les paramètres, procédez comme suit :

1. Dans l'arborescence de la Console d'administration du Kaspersky Security Center, sélectionnez le groupe d'administration pour lequel les paramètres de fonctionnement des appareils EAS doivent être configurés.

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

3. Dans la liste des stratégies, sélectionnez la stratégie d'administration des appareils EAS.

   Si nécessaire, vous pouvez créer une nouvelle stratégie de groupe à l'aide de l'Assistant de création d'une stratégie (cf. section "Stratégies de groupe pour l'administration des appareils mobiles" à la page 58).

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

La fenêtre **Propriétés : <nom de la stratégie>** s'ouvre. Cette fenêtre permet de configurer les paramètres de la stratégie de groupe.

RESTRICTION DES PRIVILEGES D'INSTALLATION

Les administrateurs du Kaspersky Security Center peuvent définir des privilèges d'accès des utilisateurs de la Console d'administration aux différentes fonctions de l'application selon leurs attributs dans l'entreprise.

Dans l'interface de la Console d'administration, la configuration des privilèges d'accès s'effectue dans les propriétés du Serveur d'administration, sous les onglets **Sécurité** et **Rôles des utilisateurs**. L'onglet **Rôles des utilisateurs** permet d'ajouter des rôles d'utilisateur types accompagnés d'un ensemble de privilèges définis. La section **Sécurité** permet de définir des privilèges pour un utilisateur ou pour un groupe d'utilisateurs et d'attribuer des rôles à un utilisateur ou à un groupe d'utilisateurs. Les privilèges des utilisateurs pour chaque application sont définis par *zone opérationnelle*.

Vous pouvez également définir les privilèges des utilisateurs par zone opérationnelle pour l'application Kaspersky Mobile Device Management. Le tableau ci-dessous reprend les zones opérationnelles pour l'administration des appareils EAS et les onglets de la stratégie qui figurent dans ces zones opérationnelles.

Tableau 3. Privilèges d'accès aux fonctions de l'application

ZONE OPERATIONNELLE	ONGLET DE LA STRATEGIE
Stratégie Exchange ActiveSync	Généraux, Mot de passe, Synchronisation, Restrictions des fonctions, Restrictions des applications

L'administrateur peut attribuer les privilèges d'accès suivants pour chaque zone opérationnelle :

- **Autorisation de la modification**. L'utilisateur de la Console d'administration peut modifier les paramètres de la stratégie dans la fenêtre des propriétés.

- **Interdiction de la modification**. L'utilisateur de la Console d'administration ne peut pas modifier les paramètres de la stratégie dans la fenêtre des propriétés. Les onglets de la stratégie qui figurent dans la zone opérationnelle pour laquelle ce privilège a été défini n'apparaissent pas dans l'interface.

Pour en savoir plus sur l'utilisation des privilèges et des rôles des utilisateurs dans la Console d'administration du Kaspersky Security Center, reportez-vous au *Manuel de l'administrateur du Kaspersky Security Center.*

CONFIGURATION DE LA ROBUSTESSE DU MOT DE PASSE POUR LE DEVERROUILLAGE

Afin de protéger les données de l'appareil EAS, il convient de mettre en place un mot de passe robuste pour le déverrouillage.

Par défaut, Kaspersky Mobile Device Management ne demande pas de saisir ou de définir un mot de passe pour le déverrouillage lors du démarrage de l'appareil mobile.

➧ *Pour configurer les paramètres de robustesse du mot de passe pour le déverrouillage de l'appareil EAS, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des appareils EAS (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils EAS" à la page 90).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Mot de passe**.

3. Dans le groupe **Paramètres du mot de passe**, cochez la case **Demander le mot de passe**.

4. Configurez les paramètres de robustesse du mot de passe pour le déverrouillage :

   - Si vous souhaitez que l'utilisateur intègre obligatoirement des lettres et des chiffres au mot de passe, cochez la case **Demander la saisie d'une valeur alphanumérique**. Dans le champ **Nombre minimal de jeux de caractères**, indiquez le niveau de complexité du mot de passe alpha-numérique. Valeurs possibles : de 1 à 4. La valeur 1 correspond au niveau de complexité le plus bas.

   - Si vous souhaitez permettre à l'utilisateur d'utiliser la fonctionnalité de restauration du mot de passe, cochez la case **Activer la restauration du mot de passe**.

   - Si vous souhaitez que les fichiers dans la mémoire de l'appareil EAS soient chiffrés, cochez la case **Demander le chiffrement sur l'appareil**.

   - Si vous souhaitez que les fichiers sur la carte mémoire de l'appareil EAS soient chiffrés, cochez la case **Demander le chiffrement sur la carte mémoire**.

   - Si vous souhaitez permettre à l'utilisateur d'utiliser un mot de passe simple composé de chiffres uniquement, cochez la case **Autoriser un mot de passe simple**.

   - Si vous souhaitez limiter le nombre de tentatives de saisie du mot de passe pour accéder à l'appareil, cochez la case **Nombre maximal de tentatives de saisie**. Dans le champ à droite de la case, indiquez le nombre maximal de tentatives de saisie du mot de passe dont dispose l'utilisateur pour déverrouiller l'appareil EAS. Si l'utilisateur n'a pas saisi le mot de passe correct après le nombre de tentatives autorisées, Kaspersky Mobile Device Management supprime toutes les données du périphérique.

   - Si vous souhaitez établir un nombre minimal de caractères dans le mot de passe de l'utilisateur, cochez la case **Nombre minimal de caractères**. Dans le champ à droite de la case, indiquez le nombre minimal de caractères dans le mot de passe. Valeurs possibles : de 4 à 16.

   - Si vous souhaitez que Kaspersky Mobile Device Management invite à saisir le mot de passe pour accéder à l'appareil après une période d'inactivité de l'utilisateur, cochez la case **Délai d'inactivité avant la saisie réitérée du mot de passe (min)**. Dans le champ à droite de la case, indiquez la durée d'inactivité de l'utilisateur (en minutes) au terme de laquelle l'application invite ce dernier à saisir le mot de passe.

- Si vous souhaitez limiter la durée de validité du mot de passe, cochez la case **Validité du mot de passe (jours)**. Dans le champ à droite de la case, indiquez la durée de validité du mot de passe. A l'issue de cette période, l'application propose à l'utilisateur de changer de mot de passe.

- Dans le champ **Historique du mot de passe**, indiquez le nombre de mots de passe précédents interdits.

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

Kaspersky Mobile Device Management vérifiera ainsi la présence d'un mot de passe sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée. Si le mot de passe pour le déverrouillage n'est pas indiqué, l'utilisateur sera invité à le définir. Le mot de passe doit être défini conformément aux paramètres indiqués dans la stratégie. Si le mot de passe pour le déverrouillage indiqué ne correspond pas aux exigences de la stratégie, l'utilisateur sera invité à le modifier.

CONFIGURATION DES PARAMETRES DE LA SYNCHRONISATION

Afin de permettre à l'utilisateur de l'appareil EAS d'accéder aux messages électroniques, aux événements du calendrier, aux contactes et aux tâches sur le serveur Microsoft Exchange, il convient de configurer les paramètres de la synchronisation. Au terme de la synchronisation, l'utilisateur peut travailler de manière autonome avec ces données.

Par défaut, les événements du calendrier et les messages électroniques sont conservés indéfiniment sur l'appareil EAS. L'utilisateur peut lancer la synchronisation avec le serveur Microsoft Exchange autant de fois qu'il le souhaite. Il est interdit de télécharger sur l'appareil mobile les pièces jointes accompagnant les messages électroniques.

➧ *Pour configurer les paramètres de synchronisation de l'appareil EAS avec le Serveur Microsoft Exchange, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des appareils EAS (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils EAS" à la page 90).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Synchronisation**.

3. Dans le groupe **Paramètres de synchronisation**, sélectionnez la durée de conservation des événements du calendrier sur l'appareil EAS dans la liste déroulante **Conserver les événements du calendrier**.

4. Dans la liste déroulante **Conserver les messages électroniques**, sélectionnez la durée de conservation des messages électroniques sur l'appareil EAS.

5. Si vous souhaitez limiter le volume de messages électroniques, cochez la case **Limiter la taille du courrier électronique (Ko)**. Dans le champ ci-dessous, indiquez le volume de messages électroniques autorisé en kilooctets.

6. Si vous souhaitez permettre à l'utilisateur de se synchroniser avec le serveur Microsoft Exchange en itinérance, à l'aide de la technologie Direct Push, cochez la case **Autoriser Direct Push en itinérance**.

7. Si vous souhaitez permettre à l'utilisateur de consulter sa messagerie électronique au format HTML, cochez la case **Autoriser la messagerie électronique au format HTML**.

8. Configurer le téléchargement des pièces jointes accompagnant les messages électroniques :

   a. Si vous souhaitez permettre à l'utilisateur de télécharger sur l'appareil EAS les fichiers joints aux messages électroniques, cochez la case **Autoriser le téléchargement des pièces jointes sur l'appareil**.

      La case **Taille maximale de la pièce jointe (KB)** devient alors disponible.

   b. Si vous souhaitez limiter la taille des pièces jointes aux messages électroniques entrants, cochez la case **Taille maximale de la pièce jointe (en Ko)**. Dans le champ ci-dessous, indiquez en kilooctets la taille des pièces jointes pouvant être téléchargées sur l'appareil.

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

Les paramètres de synchronisation avec le serveur Microsoft Exchange seront ainsi configurés sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DES RESTRICTIONS DE FONCTIONNALITES

Afin d'assurer la sécurité de l'appareil EAS, il convient de configurer les restrictions des fonctionnalités de l'appareil.

Par défaut, toutes les fonctionnalités de l'appareil EAS peuvent être utilisées sans restriction.

Pour configurer les restrictions des fonctionnalités sur l'appareil EAS, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des appareils EAS (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils EAS" à la page 90).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Restrictions des fonctionnalités.**

3. Dans le groupe **Paramètres de la restriction de fonctionnalités**, autorisez ou interdisez l'utilisation des fonctionnalités de l'appareil EAS :

   - Si vous souhaitez permettre à l'utilisateur de connecter une carte mémoire ou tout autre disque amovible à l'appareil EAS, cochez la case **Autoriser les supports amovibles**.

   - Si vous souhaitez permettre à l'utilisateur d'utiliser l'appareil photo de l'appareil EAS, cochez la case **Autoriser l'appareil photo**.

   - Si vous souhaitez permettre à l'utilisateur d'utiliser la connectivité Wi-Fi sur l'appareil EAS, cochez la case **Autoriser le réseau sans fil**.

   - Si vous souhaitez permettre à l'utilisateur d'utiliser le port infrarouge sur l'appareil EAS, cochez la case **Autoriser la connexion infrarouge**.

   - Si vous souhaitez permettre à l'utilisateur d'utiliser l'appareil EAS en tant que point d'accès au Wi-Fi pour la création d'un réseau sans fil, cochez la case **Autoriser l'utilisation de l'appareil comme point d'accès Wi-Fi**.

   - Si vous souhaitez permettre à l'utilisateur de l'appareil EAS de se connecter au bureau à distance, cochez la case **Autoriser la connexion au bureau à distance depuis l'appareil**.

   - Si vous souhaitez permettre à l'utilisateur d'utiliser le client Desktop ActiveSync sur l'appareil EAS, cochez la case **Autoriser la synchronisation du bureau**.

   - Dans la liste déroulante **Utilisation du Bluetooth**, autorisez ou interdisez l'utilisation du Bluetooth sur l'appareil EAS :

     - **Autoriser**. L'utilisation de Bluetooth est autorisée sur le périphérique mobile.

     - **Mains libres seulement**. L'utilisation du Bluetooth est autorisée lorsqu'un kit sans fil est connecté à l'appareil mobile.

     - **Interdire**. L'utilisation de Bluetooth est interdite sur le périphérique mobile.

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

Les restrictions de fonctionnalités de l'appareil EAS seront ainsi configurées sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DES RESTRICTIONS D'APPLICATIONS

Afin d'assurer la sécurité de l'appareil EAS, il convient de configurer les restrictions relatives au fonctionnement des applications (navigateur Internet, applications non signées).

Par défaut, les applications de l'appareil EAS peuvent être utilisées sans restriction.

Pour configurer les restrictions relatives au fonctionnement des applications sur l'appareil EAS, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des appareils EAS (cf. section "Configuration de la stratégie de groupe pour l'administration des appareils EAS" à la page 90).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Restrictions des applications**.

3. Dans le groupe **Paramètres de la restriction d'applications**, configurez les restrictions relatives au fonctionnement des applications :

   - Si vous souhaitez permettre à l'utilisateur d'utiliser le navigateur Internet, cochez la case **Autoriser l'utilisation du navigateur**.

   - Si vous souhaitez permettre à l'utilisateur de créer des comptes de messagerie personnels (POP3 ou IMAP4), cochez la case **Autoriser la messagerie de l'utilisateur**.

   - Si vous souhaitez permettre à l'utilisateur d'exécuter des applications ne disposant pas d'un certificat d'authenticité, cochez la case **Autoriser les applications non signées**.

   - Si vous souhaitez permettre à l'utilisateur d'installer des applications ne disposant pas d'un certificat d'authenticité, cochez la case **Autoriser les paquets d'installation non signés**.

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

Le fonctionnement des applications sera ainsi restreint sur l'appareil mobile de l'utilisateur conformément à la stratégie une fois celle-ci appliquée.

CONFIGURATION DE LA STRATEGIE DE GROUPE POUR L'ADMINISTRATION DES APPAREILS IOS MDM

La stratégie d'administration permet de configurer les paramètres de fonctionnement de l'appareil iOS MDM : les paramètres de sécurité, les restrictions, les réseaux VPN, les réseaux sans fil, les comptes utilisateur (messagerie, calendrier, LDAP) et autres. Les stratégies permettent de définir de façon centralisée les mêmes valeurs de paramètres de fonctionnement des appareils mobiles faisant partie du groupe d'administration.

Pour ouvrir la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM afin de configurer les paramètres, procédez comme suit :

1. Dans l'arborescence de la Console d'administration du Kaspersky Security Center, sélectionnez le groupe d'administration pour lequel les paramètres de fonctionnement des appareils iOS MDM doivent être configurés.

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

3. Dans la liste des stratégies, sélectionnez la stratégie d'administration des appareils iOS MDM.

   Si nécessaire, vous pouvez créer une stratégie de groupe à l'aide de l'Assistant de création d'une stratégie (cf. section "Création d'une stratégie de groupe" à la page 61).

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

La fenêtre **Propriétés : <nom de la stratégie>** s'ouvre. Cette fenêtre permet de configurer les paramètres de la stratégie de groupe.

RESTRICTION DES PRIVILEGES D'INSTALLATION

Les administrateurs du Kaspersky Security Center peuvent définir des privilèges d'accès des utilisateurs de la Console d'administration aux différentes fonctions de l'application selon leurs attributs dans l'entreprise.

Dans l'interface de la Console d'administration, la configuration des privilèges d'accès s'effectue dans les propriétés du Serveur d'administration, sous les onglets **Sécurité** et **Rôles des utilisateurs**. L'onglet **Rôles des utilisateurs** permet d'ajouter des rôles d'utilisateur types accompagnés d'un ensemble de privilèges définis. La section **Sécurité** permet de définir des privilèges pour un utilisateur ou pour un groupe d'utilisateurs et d'attribuer des rôles à un utilisateur ou à un groupe d'utilisateurs. Les privilèges des utilisateurs pour chaque application sont définis par *zone opérationnelle*.

Vous pouvez également définir les privilèges des utilisateurs par zone opérationnelle pour l'application Kaspersky Mobile Device Management. Le tableau ci-dessous reprend les zones opérationnelles pour l'administration des appareils iOS MDM et les onglets de la stratégie qui figurent dans ces zones opérationnelles.

Tableau 4. Privilèges d'accès aux fonctions de l'application

ZONE OPERATIONNELLE	ONGLET DE LA STRATEGIE
Administration des paramètres des appareils iOS MDM	Généraux, Compte utilisateur unique, Protection Internet, Réseaux sans fil (Wi-Fi), Point d'accès (APN), Exchange ActiveSync, Courrier électronique, Paramètres de configuration
Restrictions et sécurité	Restrictions des fonctions, Restrictions des applications, Restrictions du contenu multimédia, Mot de passe, Réseaux privés virtuels (VPN), Proxy HTTP global, Certificats, SCEP
Synchronisation des contacts et des calendriers	LDAP, Calendrier, Contacts, Abonnements à un calendrier
Fonctionnalité complémentaire	Raccourci internet, Polices, AirPlay, AirPrint

L'administrateur peut attribuer les privilèges d'accès suivants pour chaque zone opérationnelle :

- **Autorisation de la modification**. L'utilisateur de la Console d'administration peut modifier les paramètres de la stratégie dans la fenêtre des propriétés.

- **Interdiction de la modification**. L'utilisateur de la Console d'administration ne peut pas modifier les paramètres de la stratégie dans la fenêtre des propriétés. Les onglets de la stratégie qui figurent dans la zone opérationnelle pour laquelle ce privilège a été défini n'apparaissent pas dans l'interface.

Pour en savoir plus sur l'utilisation des privilèges et des rôles des utilisateurs dans la Console d'administration du Kaspersky Security Center, reportez-vous au *Manuel de l'administrateur du Kaspersky Security Center.*

CONFIGURATION DE LA ROBUSTESSE DU MOT DE PASSE POUR LE DEVERROUILLAGE

Afin de protéger les données de l'appareil iOS MDM, il convient de configurer les exigences relatives à la robustesse du mot de passe pour le déverrouillage.

Par défaut, l'utilisateur peut utiliser un mot de passe simple. Un *mot de passe simple* peut contenir une suite ou une répétition de caractères, par exemple « abcd » ou « 2222 ». Il n'est pas nécessaire de saisir un mot de passe alpha-numérique contenant des caractères spéciaux. Par défaut, la durée de validité du mot de passe et le nombre de tentatives de saisie ne sont pas limités.

➧ *Pour configurer les paramètres de robustesse du mot de passe pour le déverrouillage de l'appareil iOS MDM, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Mot de passe**.

3. Dans le groupe **Paramètres du mot de passe**, cochez la case **Appliquer les paramètres à l'appareil**.

4. Configurez les paramètres de robustesse du mot de passe pour le déverrouillage :

   - Si vous souhaitez permettre à l'utilisateur d'utiliser un mot de passe simple, cochez la case **Autoriser un mot de passe simple**.

   - Si vous souhaitez que l'utilisateur intègre obligatoirement des lettres et des chiffres au mot de passe, cochez la case **Demander la saisie d'une valeur alphanumérique**.

   - Dans la liste **Nombre minimal de caractères**, sélectionnez la longueur minimale du mot de passe.

   - Dans la liste **Nombre minimal de caractères spéciaux**, sélectionnez le nombre minimal de caractères spéciaux dans le mot de passe (par exemple, "$", "&", "!").

- Dans le champ **Durée maximale d'utilisation**, indiquez la période, en jours, pendant laquelle le mot de passe reste actif. Kaspersky Mobile Device Management demande à l'utilisateur de modifier le mot de passe à l'issue de la période définie.

- Dans la liste **Activer le verrouillage automatique dans**, sélectionnez le temps d'activation du verrouillage automatique de l'appareil iOS MDM.

- Dans le champ **Historique des mots de passe**, indiquez la quantité de mots de passe utilisés (mot de passe actuel compris) que Kaspersky Mobile Device Management comparera avec le nouveau mot de passe lors du changement de celui-ci. Si les mots de passe sont identiques, le nouveau mot de passe n'est pas accepté.

- Dans la liste **Délai maximal pour le déverrouillage sans mot de passe**, sélectionnez la durée pendant laquelle l'utilisateur peut déverrouiller l'appareil iOS MDM sans saisir de mot de passe.

- Dans la liste **Nombre maximal de tentatives de saisie**, sélectionnez le nombre de tentatives de saisie du mot de passe dont dispose l'utilisateur pour déverrouiller l'appareil iOS MDM.

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

Kaspersky Mobile Device Management vérifiera ainsi la robustesse du mot de passe sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée. Si la robustesse du mot de passe pour le déverrouillage ne correspond pas à la stratégie, l'utilisateur sera invité à le modifier.

CONFIGURATION DES RESTRICTIONS POUR LES APPAREILS IOS MDM

Afin de répondre aux exigences en matière de sécurité de l'entreprise, il convient de configurer les restrictions relatives au fonctionnement de l'appareil iOS MDM.

Pour configurer les restrictions de l'appareil iOS MDM, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Restrictions des fonctionnalités**.

3. Dans le groupe **Paramètres des restrictions de fonctionnalités**, cochez la case **Appliquer les paramètres à l'appareil**.

4. Configurez les restrictions des fonctionnalités de l'appareil iOS MDM.

   Les restrictions sont décrites dans l'Appendice (cf. section "Appendice. Restrictions pour les appareils iOS MDM" à la page 133).

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

6. Sélectionnez la section **Restrictions des applications**.

7. Dans le groupe **Paramètres des restrictions d'applications**, cochez la case **Appliquer les paramètres à l'appareil**.

8. Configurez les restrictions pour les applications sur l'appareil iOS MDM.

   Les restrictions sont décrites dans l'Appendice (cf. section "Appendice. Restrictions pour les appareils iOS MDM" à la page 133).

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

10. Sélectionnez la section **Restrictions du contenu multimédia**.

11. Dans le groupe **Paramètres de la restriction du contenu multimédia**, cochez la case **Appliquer les paramètres à l'appareil**.

12. Configurez les restrictions pour le contenu multimédia sur l'appareil iOS MDM.

    Les restrictions sont décrites dans l'Appendice (cf. section "Appendice. Restrictions pour les appareils iOS MDM" à la page 133).

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

Les restrictions relatives aux fonctionnalités, aux applications et au contenu multimédia seront ainsi configurées sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DU PROXY HTTP GLOBAL

Afin d'assurer la sécurité du trafic Internet de l'utilisateur, il convient de configurer la connexion de l'appareil iOS MDM à Internet via un serveur proxy.

La connexion automatique à Internet via un serveur proxy n'est disponible que pour les appareils contrôlés.

Pour configurer le proxy HTTP global sur l'appareil iOS MDM, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Proxy HTTP global**.

3. Dans le groupe **Paramètres du proxy HTTP global**, cochez la case **Appliquer les paramètres à l'appareil**.

4. Sélectionnez le type de configuration du proxy HTTP global.

   Par défaut, le type de configuration manuel est sélectionné pour le proxy HTTP global et il est interdit à l'utilisateur de se connecter aux réseaux via portail captif sans connexion au serveur proxy. *Réseaux via portail captif* : réseaux sans fil exigeant une authentification préalable sur l'appareil mobile sans connexion au serveur proxy.

   - Si vous souhaitez saisir manuellement les paramètres de connexion au serveur proxy, procédez comme suit :

     a. Dans la liste déroulante **Type de configuration**, sélectionnez **Manuelle**.

     b. Dans le champ **Adresse du serveur proxy et port**, indiquez le nom de l'hôte ou l'adresse IP du serveur proxy et le numéro de port du serveur proxy.

     c. Dans le champ **Nom de l'utilisateur**, indiquez le nom du compte utilisateur pour l'autorisation sur le serveur proxy. Vous pouvez utiliser les macros de la liste déroulante **Ajouter un macro**.

     d. Dans le champ **Mot de passe**, indiquez le mot de passe du compte utilisateur pour l'autorisation sur le serveur proxy.

     e. Si vous souhaitez permettre à l'utilisateur d'accéder aux réseaux via portail captif, cochez la case **Autoriser l'accès aux réseaux via portail captif sans connexion au serveur proxy**.

   - Si vous souhaitez configurer les paramètres de connexion au serveur proxy à l'aide d'un fichier PAC (Proxy Auto Configuration) prédéfini, procédez comme suit :

     a. Dans la liste déroulante **Type de configuration**, sélectionnez **Automatique**.

b. Dans le champ **URL du fichier PAC**, indiquez l'URL du fichier PAC (par exemple, http://www.example.com/filename.pac).

c. Si vous souhaitez permettre à l'utilisateur de connecter l'appareil mobile au réseau sans fil sans passer par le serveur proxy lorsque le fichier PAC est inaccessible, cochez la case **Autoriser la connexion directe si le fichier PAC est inaccessible**.

d. Si vous souhaitez permettre à l'utilisateur d'accéder aux réseaux via portail captif, cochez la case **Autoriser l'accès aux réseaux via portail captif sans connexion au serveur proxy**.

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

L'utilisateur de l'appareil mobile se connectera ainsi à Internet via le serveur proxy une fois la stratégie appliquée.

CONFIGURATION DES PARAMETRES DU COMPTE UTILISATEUR UNIQUE

Afin d'utiliser le système d'entreprise de la technologie d'authentification unique, il convient de configurer un compte utilisateur unique sur l'appareil iOS MDM. Le technologie d'authentification unique permet d'accéder aux applications et services de l'entreprise en saisissant une seule fois les données de compte de l'utilisateur. La technologie d'authentification unique utilise le système d'authentification Kerberos.

Par défaut, l'utilisation de la technologie d'authentification unique pour les sites Internet et les applications n'est pas limitée.

Pour configurer le compte unique de l'utilisateur de l'appareil iOS MDM, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Compte utilisateur unique**.

3. Dans le groupe **Paramètres du compte utilisateur unique**, cochez la case **Appliquer les paramètres à l'appareil**.

4. Dans le champ **Nom du compte utilisateur**, saisissez le nom du compte utilisateur pour l'autorisation sur le serveur Kerberos. Vous pouvez utiliser les macros de la liste déroulante **Ajouter un macro**.

5. Dans le champ **Nom d'utilisateur Kerberos**, saisissez le principal nom du compte de l'utilisateur de l'appareil iOS MDM sur le serveur Kerberos.

   Le nom principal doit respecter la casse lors de la saisie au format principal/instance@zone d'action (primary/instanse@realm). Par exemple : mycompany/admin@EXAMPLE ou mycompany@EXAMPLE.

   Vous pouvez utiliser les macros de la liste déroulante **Ajouter un macro**.

6. Dans le champ **Espace de travail Kerberos**, saisissez le nom du réseau regroupant les serveurs Kerberos et les appareils iOS MDM. L'espace de travail Kerberos doit être indiqué en majuscules.

7. Si vous souhaitez que l'utilisateur utilise le compte unique sur les sites Internet ajoutés à la liste des URL autorisées uniquement, procédez comme suit :

   a. Cochez la case **Limiter l'utilisation du compte utilisateur pour les URL**.

   b. Cliquez sur le bouton **Configuration** à droite de la case.

      La fenêtre **URL autorisées** s'ouvre.

   c. Créez la liste des sites Internet pour lesquels l'autorisation automatique est permise par le biais de la technologie de compte utilisateur unique.

Si la liste des modèles d'URL est vide, l'utilisateur peut appliquer le compte utilisateur unique pour tous les sites Internet de la zone d'action de la technologie d'authentification unique.

d. Cliquez sur le bouton **OK** pour enregistrer la liste des sites Internet.

8. Si vous souhaitez que l'utilisateur utilise le compte unique dans les applications ajoutées à la liste des identifiants d'applications uniquement, procédez comme suit :

   a. Cochez la case **Limiter l'utilisation du compte utilisateur pour les applications**.

   b. Cliquez sur le bouton **Configuration** à droite de la case.

   c. La fenêtre **Identifiants d'applications** s'ouvre.

   d. Dans la fenêtre **Identifiants d'applications** qui s'ouvre, créez la liste des applications pour lesquelles l'autorisation automatique est permise via la technologie de compte utilisateur unique.

      Si la liste des modèles d'identifiants d'applications est vide, l'utilisateur peut appliquer le compte utilisateur unique pour toutes les applications de la zone d'action de la technologie d'authentification unique.

   e. Cliquez sur le bouton **OK** pour enregistrer la liste des applications.

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

Le compte utilisateur unique sera ainsi configuré sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DE L'ACCES AUX SITES INTERNET

Afin de contrôler l'accès de l'utilisateur de l'appareil iOS MDM aux sites Internet, il convient de configurer les paramètres de la Protection Internet. La Protection Internet contrôle l'accès de l'utilisateur aux sites Internet sur la base des listes de sites autorisés et interdits que vous créez. La Protection Internet permet également d'ajouter des onglets de sites Internet à la barre d'onglets de Safari.

Par défaut, l'accès aux sites Internet n'est pas limité.

La configuration de la Protection Internet est disponible uniquement pour les appareils contrôlés.

Pour configurer l'accès aux sites Internet sur l'appareil iOS MDM, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Protection Internet**.

3. Dans le groupe **Paramètres de la Protection Internet**, cochez la case **Appliquer les paramètres à l'appareil**.

4. Afin de bloquer l'accès aux sites interdits et de permettre l'accès aux sites autorisés, procédez comme suit :

   a. Dans la liste déroulante **Mode de filtrage des sites Internet**, sélectionnez le mode **Restreindre l'accès au contenu "pour adultes"**.

   b. Dans le groupe **Sites Internet autorisés**, créez la liste des sites Internet autorisés.

      L'adresse du site Internet doit commencer par "http://" ou "https://". Kaspersky Mobile Device Management autorise l'accès à tous les sites Internet du domaine. Par exemple, si vous avez ajouté http://www.example.com dans la liste des sites Internet autorisés, l'accès à http://pictures.example.com ou http://www.example.com/movies est également autorisé. Si la liste des sites Internet autorisés est vide, l'application autorise l'accès à tous les sites Internet, excepté à ceux apparaissant dans la liste des sites interdits.

c. Dans le groupe **Sites Internet interdits**, créez la liste des sites Internet interdits.

L'adresse du site Internet doit commencer par "http://" ou "https://". Kaspersky Mobile Device Management interdit l'accès à tous les sites Internet du domaine.

5. Pour bloquer l'accès à tous les sites Internet, exceptés les sites Internet autorisés de la liste des onglets, procédez comme suit :

a. Dans la liste déroulante **Mode de filtrage des sites Internet**, sélectionnez le mode **Autoriser uniquement les sites Internet figurant dans la liste des onglets**.

b. Dans le groupe **Onglets**, créez la liste des onglets des sites Internet autorisés.

L'adresse du site Internet doit commencer par "http://" ou "https://". Kaspersky Mobile Device Management autorise l'accès à tous les sites Internet du domaine. Si la liste des onglets est vide, l'application autorise l'accès à tous les sites Internet. Kaspersky Mobile Device Management ajoute les sites Internet depuis la liste des onglets à la barre d'onglets de Safari sur l'appareil mobile de l'utilisateur.

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

Le filtrage des sites Internet sera ainsi configuré sur l'appareil mobile de l'utilisateur conformément au mode sélectionné et aux listes crées une fois la stratégie appliquée.

CONNEXION AU RESEAU SANS FIL

Afin de connecter automatiquement l'appareil iOS MDM à un réseau sans fil disponible et de garantir la sécurité des données, il convient de configurer les paramètres de connexion.

Pour configurer la connexion de l'appareil iOS MDM à un réseau sans fil, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Réseaux sans fil (Wi-Fi)**.

3. Dans le groupe **Paramètres des réseaux sans fil**, cliquez sur le bouton **Ajouter**.

La fenêtre **Réseau sans fil** s'ouvre.

4. Dans le champ **Identificateur du réseau SSID**, saisissez le nom du réseau sans fil contenant le point d'accès (SSID).

5. Si vous souhaitez que l'appareil iOS MDM se connecte automatiquement au réseau sans fil, cochez la case **Connexion automatique**.

6. Si vous souhaitez que le réseau sans fil n'apparaisse pas dans la liste des réseaux disponibles sur l'appareil iOS MDM, cochez la case **Réseau masqué**.

Dans ce cas, pour se connecter au réseau l'utilisateur devra saisir manuellement sur l'appareil mobile l'identifiant du réseau SSID défini dans les paramètres du routeur Wi-Fi.

7. Dans la liste déroulante **Protection du réseau**, sélectionnez le type de protection de la connexion au réseau sans fil :

- **Désactivée**. L'authentification de l'utilisateur n'est pas requise.
- **WEP**. Le réseau est protégé par le protocole de chiffrement WEP (Wireless Encryption Protocol).
- **WPA/WPA2 particulier**. Le réseau est protégé par le protocole de chiffrement WPA / WPA2 (Wi-Fi Protected Access).

- **Tout (personnel)**. Le réseau est protégé par le protocole de chiffrement WEP ou WPA / WPA2 en fonction du type de directeur Wi-Fi. Une clé de chiffrement spécifique à chaque utilisateur est utilisée pour l'authentification.

- **WEP dynamique**. Le réseau est protégé par le protocole de chiffrement WEP avec une clé dynamique.

- **WPA/WPA2 d'entreprise**. Le réseau est protégé par le protocole de chiffrement WPA / WPA2 avec une seule clé de chiffrement pour l'ensemble des utilisateurs.

- **Tout (d'entreprise)**. Le réseau est protégé par le protocole de chiffrement WEP ou WPA / WPA2 en fonction du type de directeur Wi-Fi. L'authentification utilise une seule clé de chiffrement pour tous les utilisateurs.

Si dans la liste **Protection du réseau**, vous avez sélectionné **WEP dynamique**, **WPA/WPA2 d'entreprise** ou **Quelconque (entreprise)**, vous pouvez sélectionner les types de protocoles EAP (Extensible Authentication Protocol) pour l'identification de l'utilisateur sur le réseau sans fil dans le groupe **Protocoles**.

Dans le groupe **Certificats de confiance**, vous pouvez également créer une liste des certificats de confiance pour l'authentification de l'utilisateur de l'appareil iOS MDM sur les serveurs de confiance.

8. Configurez le compte utilisateur pour l'authentification de l'utilisateur lors de la connexion de l'appareil iOS MDM au réseau sans fil :

   a. Cliquez sur le bouton **Configuration** dans le groupe **Authentification**.

      La fenêtre **Authentification** s'ouvre.

   b. Dans le champ **Nom d'utilisateur**, saisissez le nom du compte utilisateur pour l'authentification de l'utilisateur lors de la connexion au réseau sans fil.

   c. Si vous souhaitez que l'utilisateur saisisse manuellement le mot de passe du compte utilisateur lors de la connexion au réseau sans fil, cochez la case **Demander le mot de passe lors de chaque connexion**.

   d. Dans le champ **Mot de passe**, saisissez le mot de passe du compte utilisateur pour l'authentification sur le réseau sans fil.

   e. Dans la liste déroulante **Certificat pour l'authentification**, sélectionnez le certificat pour l'authentification de l'utilisateur sur le réseau sans fil. Si la liste ne contient pas les certificats, vous pouvez les ajouter dans la section **Certificats** (cf. section "**Ajout de certificats de sécurité**" à la page 121).

   f. Dans le champ **Identifiant de l'utilisateur**, saisissez l'identifiant de l'utilisateur qui s'affichera à la place de son vrai nom pour la transmission des données lors du processus d'authentification.

      L'identificateur vise à élever le niveau de sécurité du processus d'authentification. En effet, il n'affiche pas le nom de l'utilisateur, qui apparaît lui-même dans le tunnel TLS chiffré.

   g. Cliquez sur le bouton **OK**.

   Les paramètres du compte utilisateur pour l'authentification de l'utilisateur lors de la connexion au réseau sans fil seront ainsi configurés sur l'appareil iOS MDM.

9. Configurez (si nécessaire) les paramètres de connexion au réseau sans fil via le serveur proxy :

   a. Dans le groupe **Serveur proxy**, cliquez sur le bouton **Configuration**.

   b. Dans la fenêtre **Serveur proxy** qui s'ouvre, sélectionnez le mode de configuration du serveur proxy et indiquez les paramètres de connexion.

   c. Cliquez sur le bouton **OK**.

   Les paramètres de connexion de l'appareil au réseau sans fil via le serveur proxy seront ainsi configurés sur l'appareil iOS MDM.

10. Cliquez sur le bouton **OK**.

    Le nouveau réseau Wi-Fi s'affichera dans la liste.

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

La connexion au réseau Wi-Fi sera ainsi configurée sur l'appareil iOS MDM de l'utilisateur une fois la stratégie appliquée. L'appareil mobile de l'utilisateur se connectera automatiquement à un réseau sans fil disponible. La protection des données lors de la connexion au réseau Wi-Fi est assurée par la technologie d'authentification.

CONFIGURATION DE LA PROTECTION DES DONNEES DE L'UTILISATEUR A L'AIDE DES PROTOCOLES EAP

Si dans la liste **Protection du réseau**, vous avez sélectionné la valeur **WEP dynamique**, **WPA/WPA2 d'entreprise** ou **Tout (d'entreprise)** (cf. section "**Connexion à un réseau sans fil**" à la page 101), il est recommandé de configurer la protection des données de l'utilisateur à l'aide des protocoles EAP (Extensible Authentication Protocol).

Afin de configurer la protection des données de l'utilisateur à l'aide des protocoles EAP, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Réseau sans fil (Wi-Fi)**.
3. Dans le groupe **Paramètres des réseaux sans fil**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Réseau sans fil** s'ouvre.
4. Dans le groupe **Protocoles**, cliquez sur le bouton **Configuration**.

   La fenêtre **Protocoles** s'ouvre.
5. Dans le groupe **Types d'EAP**, sélectionnez les types de protocoles EAP :
   - **TLS**. Protocole de sécurité au niveau transport.
   - **TTLS**. Protocole de sécurité au niveau transport via un tunnel TLS chiffré.
   - **LEAP**. Protocole d'authentification extensible léger. Ce protocole est utilisé pour l'exploitation des périphériques Cisco® Aironet®.
   - **PEAP**. Protocole extensible sécurisé via tunnel TLS.
   - **EAP-FAST**. Protocole extensible via tunnel protégé.
   - **EAP-SIM**. Protocole d'identification par carte SIM d'appareil mobile.
   - **EAP-AKA**. Protocole d'identification par carte USIM.
6. Dans le groupe **EAP-FAST**, configurez les paramètres du protocole d'authentification via tunnel protégé :
   - Si vous souhaitez utiliser une clé cryptographique PAC (Protected Access Credential) pour l'identification de l'utilisateur, cochez la case **Utiliser Protected Access Credential (PAC)**.
   - Si vous souhaitez préparer une clé PAC pour l'identification de l'utilisateur selon le protocole EAP-FAST, cochez la case **Autoriser l'approvisionnement automatique du PAC**.
   - Si vous souhaitez préparer une clé PAC anonyme pour l'identification de l'utilisateur selon le protocole EAP-FAST, cochez la case **Autoriser l'utilisation anonyme du PAC**.
7. Cliquez sur le bouton **OK**.

L'identification de l'utilisateur à l'aide des protocoles EAP sera ainsi configurée sur l'appareil iOS MDM.

CONSTITUTION D'UNE LISTE DES CERTIFICATS DE CONFIANCE

Si dans la liste **Protection du réseau**, vous avez sélectionné la valeur **WEP dynamique**, **WPA/WPA2 d'entreprise** ou **Tout (d'entreprise)** (cf. section "**Connexion à un réseau sans fil**" à la page 101), il est recommandé de créer une liste des certificats de confiance pour l'authentification de l'utilisateur de l'appareil iOS MDM sur les serveurs de confiance. Le certificat de confiance est un certificat dont l'authenticité est confirmée dans le centre de certification.

Pour composer une liste des certificats de confiance, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Réseaux sans fil (Wi-Fi)**.
3. Dans le groupe **Paramètres des réseaux sans fil**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Réseau sans fil** s'ouvre.
4. Dans le groupe **Certificats de confiance**, cliquez sur le bouton **Configuration**.
5. La fenêtre **Certificats de confiance** s'ouvre.
6. Dans le groupe **Certificats de confiance**, créez la liste des certificats de confiance.
7. Dans le groupe **Noms des certificats de confiance** créez la liste des serveurs qui nécessitent une authentification par certificat de confiance.

   Vous pouvez indiquer le nom complet du serveur, par exemple server.mycompany.com ou seulement une partie de son nom, par exemple *.mycompany.com.
8. Cliquez sur le bouton **OK**.

La liste des certificats de confiance pour l'authentification de l'utilisateur sur les serveurs de confiance sera ainsi créée sur l'appareil iOS MDM.

CONFIGURATION DE LA CONNEXION VPN

Afin de connecter l'appareil iOS MDM à un réseau privé virtuel et de garantir la sécurité des données lors de la connexion à un réseau VPN, il convient de configurer les paramètres de connexion à un réseau privé virtuel.

Pour configurer la connexion VPN sur l'appareil iOS MDM, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Réseaux privés virtuels (VPN)**.
3. Dans le groupe **Paramètres des réseaux privés virtuels**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Paramètres des réseaux privés virtuels (VPN)** s'ouvre.
4. Indiquez le nom pour le tunnel VPN dans le champ **Nom du réseau**.
5. Dans la liste déroulante **Type de connexion**, sélectionnez le type de connexion VPN :

   - **L2TP** (Layer 2 Tunneling Protocol). La connexion prend en charge l'authentification de l'utilisateur du périphérique mobile iOS MDM à l'aide de mots de passe MS-CHAP v2, de l'authentification à deux facteurs et de l'authentification automatique à l'aide d'une clé commune.

- **PPTP** (Point-to-Point Tunneling Protocol). La connexion prend en charge l'authentification de l'utilisateur du périphérique mobile iOS MDM à l'aide de mots de passe MS-CHAP v2 et de l'authentification à deux facteurs.

- **IPSec (Cisco)**. La connexion prend en charge l'authentification de l'utilisateur du périphérique mobile iOS MDM à l'aide de mots de passe et de l'authentification automatique à l'aide d'une clé commune.

- **Cisco AnyConnect**. La connexion prend en charge le pare-feu Cisco® Adaptive Security Appliance (ASA) version 8.0(3).1 ou supérieure. La configuration de la connexion VPN requiert l'installation sur le périphérique mobile iOS MDM de l'application Cisco® AnyConnect® depuis l'App Store.

- **Juniper SSL**. La connexion prend en charge la passerelle Juniper Networks™ SSL VPN série SA version 6.4 ou suivante avec le paquet Juniper Networks IVE version 7.0 ou suivante. La configuration de la connexion VPN requiert l'installation sur le périphérique mobile iOS MDM de l'application JUNOS™ depuis l'App Store.

- **F5 SSL**. La connexion prend en charge les solutions F5® BIG-IP® Edge Gateway™, Access Policy Manager® et Fire SSL VPN. La configuration de la connexion VPN requiert l'installation sur le périphérique mobile iOS MDM de l'application F5 BIG-IP Edge Client® depuis l'App Store.

- **SonicWALL Mobile Connect**. La connexion prend en charge les appareils SonicWALL Aventail E-Class Secure Remote Access version 10.5.4 et suivantes, les appareils SonicWALL SRA version 5.5 et suivantes ainsi que les appareils SonicWALL Next-Generation Firewall, y compris TZ, NSA, E-Class NSA avec SonicOS version 5.8.1.0 et suivantes. La configuration de la connexion VPN requiert l'installation sur le périphérique mobile iOS MDM de l'application SonicWALL™ Mobile Connect depuis l'App Store.

- **Aruba VIA**. La connexion prend en charge les contrôleurs d'accès mobile Aruba Networks®. Pour les configurer, il faut installer sur le périphérique mobile iOS MDM l'application Aruba Networks VIA depuis l'App Store.

- **Custom SSL**. L'application prend en charge l'authentification de l'utilisateur du périphérique mobile iOS MDM à l'aide de mots de passe et de certificats, ainsi que de l'authentification à deux facteurs.

6. Dans le champ **Adresse du serveur**, saisissez le nom réseau ou l'adresse IP du serveur VPN.

7. Dans le champ **Nom du compte utilisateur**, saisissez le nom du compte utilisateur pour l'autorisation sur le serveur VPN. Vous pouvez utiliser les macros de la liste déroulante **Ajouter un macro**.

8. Configurez les paramètres de sécurité pour la connexion VPN conformément au type de réseau privé virtuel sélectionné. Vous trouverez plus bas dans cette section des instructions détaillées concernant la configuration de la connexion VPN.

9. Configurez (si nécessaire) les paramètres de connexion au réseau privé virtuel via le serveur proxy :

   a. Sélectionnez l'onglet **Paramètres du serveur proxy**.

   b. Sélectionnez le mode de configuration du serveur proxy et indiquez les paramètres de connexion.

   c. Cliquez sur le bouton **OK**.

   Les paramètres de connexion de l'appareil au réseau VPN via le serveur proxy seront ainsi configurés sur l'appareil iOS MDM.

10. Cliquez sur le bouton **OK**.

    Le nouveau réseau privé virtuel s'affichera dans la liste.

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

La connexion au réseau VPN sera ainsi configurée sur l'appareil iOS MDM de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DE LA CONNEXION L2TP

Pour configurer les paramètres de sécurité pour la connexion L2TP du réseau VPN, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Réseaux privés virtuels (VPN)**.
3. Dans le groupe **Paramètres des réseaux privés virtuels**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Paramètres des réseaux privés virtuels (VPN)** s'ouvre.
4. Dans la liste déroulante **Type de connexion**, sélectionnez **L2TP**.
5. Dans le groupe **Type d'authentification**, sélectionnez la méthode d'authentification de l'utilisateur de l'appareil iOS MDM sur le réseau privé virtuel :

   - **RSA SecureID**. Authentification à deux facteurs de l'utilisateur du périphérique mobile iOS MDM à l'aide d'un token RSA SecureID et d'une clé commune. L'authentification de l'utilisateur requiert la définition de la clé dans le champ **Secret partagé**.
   - **Mot de passe**. Authentification de l'utilisateur du périphérique mobile iOS MDM à l'aide d'un mot de passe. Pour authentifier l'utilisateur, il faut définir le mot de passe dans le champ ci-dessous.
6. Dans le champ **Clé partagée**, indiquez le mot de passe pour la clé de sécurité IPSec préalablement installée.
7. Si vous souhaitez que l'ensemble du trafic sortant passe par la connexion VPN, même si un autre service réseau est utilisé (par exemple, AirPort ou Ethernet), cochez la case **Envoyer l'ensemble du trafic via la connexion VPN**.
8. Cliquez sur le bouton **OK**.

CONFIGURATION DE LA CONNEXION PPTP

Pour configurer les paramètres de sécurité pour la connexion PPTP du réseau VPN, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Réseaux privés virtuels (VPN)**.
3. Dans le groupe **Paramètres des réseaux privés virtuels**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Paramètres des réseaux privés virtuels (VPN)** s'ouvre.
4. Dans la liste déroulante **Type de connexion**, sélectionnez **PPTP**.
5. Dans le groupe **Type d'authentification**, sélectionnez la méthode d'authentification de l'utilisateur de l'appareil iOS MDM sur le réseau privé virtuel :

   - **RSA SecureID**. Authentification à deux facteurs de l'utilisateur du périphérique mobile iOS MDM à l'aide d'un token RSA SecureID et d'une clé commune.
   - **Mot de passe**. Authentification de l'utilisateur du périphérique mobile iOS MDM à l'aide d'un mot de passe. Pour authentifier l'utilisateur, il faut définir le mot de passe dans le champ ci-dessous.
6. Dans la liste déroulante **Niveau de chiffrement**, sélectionnez le niveau de chiffrement des données transmises via la connexion VPN à l'aide du protocole PPTP :

- **Aucun**. Le chiffrement est désactivé.
- **Automatique**. Kaspersky Mobile Device Management définit automatiquement l'algorithme de chiffrement des données.
- **128 bits maximum**. L'algorithme de chiffrement des données utilisé repose sur une clé qui ne dépasse pas 128 bits.

7. Si vous souhaitez que l'ensemble du trafic sortant passe par la connexion VPN, même si un autre service réseau est utilisé (par exemple, AirPort ou Ethernet), cochez la case **Envoyer l'ensemble du trafic via la connexion VPN**.
8. Cliquez sur le bouton **OK**.

CONFIGURATION DE LA CONNEXION IPSEC (CISCO)

Pour configurer les paramètres de sécurité pour la connexion IPSec (Cisco®) du réseau VPN, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Réseaux privés virtuels (VPN)**.
3. Dans le groupe **Paramètres des réseaux privés virtuels**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Paramètres des réseaux privés virtuels (VPN)** s'ouvre.
4. Dans la liste déroulante **Type de connexion**, sélectionnez **IPSec (Cisco)**.
5. Dans le groupe **Type d'authentification**, sélectionnez le type d'authentification de l'utilisateur de l'appareil iOS MDM sur le réseau privé virtuel :
   - **Clé partagée/Nom du groupe** : authentification de l'utilisateur appartenant au groupe à l'aide d'une clé commune.
   - **Certificat** : authentification de l'utilisateur à l'aide d'un certificat.
6. Si le type d'authentification sélectionné est **Clé partagée/Nom du groupe**, configurez les paramètres suivants :
   - **Nom du groupe ;**
   - **Clé partagée ;**
   - **Utiliser une authentification hybride ;**
   - **Demander la saisie du mot de passe sur l'appareil.**
7. Si le type d'authentification sélectionné est **Certificat**, configurez les paramètres suivants :
   - Sous l'onglet **Généraux**, cochez/décochez la case **Demander le code PIN**.
   - Sous l'onglet **Paramètres avancés** :
     - **Certificats ;**
     - **Activer le VPN lors de la connexion des domaines ;**
     - **Durée d'inactivité avant déconnexion.**
8. Cliquez sur le bouton **OK**.

CONFIGURATION DE LA CONNEXION CISCO ANYCONNECT

Pour configurer les paramètres de sécurité pour la connexion Cisco® AnyConnect® du réseau VPN, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Réseaux privés virtuels (VPN)**.
3. Dans le groupe **Paramètres des réseaux privés virtuels**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Paramètres des réseaux privés virtuels (VPN)** s'ouvre.
4. Dans la liste déroulante **Type de connexion**, sélectionnez **Cisco AnyConnect**.
5. Dans le champ **Groupe**, saisissez le pseudonyme du groupe de mise en tunnel pour les clients Cisco® AnyConnect® lors de la connexion au réseau VPN.
6. Sélectionnez l'onglet **Paramètres avancés**.
7. Dans la liste déroulante **Authentification de l'utilisateur**, sélectionnez le type d'authentification de l'utilisateur de l'appareil mobile iOS MDM lors de la connexion au réseau VPN via le protocole Cisco® AnyConnect® :
   - **Mot de passe** : authentification de l'utilisateur à l'aide d'un mot de passe. Pour authentifier l'utilisateur sur le réseau privé virtuel, indiquez le mot de passe dans le champ **Mot de passe**.
   - **Certificat** : authentification de l'utilisateur à l'aide d'un certificat. Pour authentifier l'utilisateur sur le réseau privé virtuel, configurez les paramètres suivants sous l'onglet **Paramètres avancés** :
     - **Certificats** ;
     - **Activer le VPN lors de la connexion des domaines** ;
     - **Durée d'inactivité avant déconnexion**.
8. Cliquez sur le bouton **OK**.

CONFIGURATION DE LA CONNEXION JUNIPER SSL

Pour configurer les paramètres de sécurité pour la connexion Juniper SSL du réseau VPN, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Réseaux privés virtuels (VPN)**.
3. Dans le groupe **Paramètres des réseaux privés virtuels**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Paramètres des réseaux privés virtuels (VPN)** s'ouvre.
4. Dans la liste déroulante **Type de connexion**, sélectionnez **Juniper SSL**.
5. Dans le champ **Zone d'action**, saisissez le nom du réseau où se trouvent les serveurs VPN et les appareils mobiles iOS MDM pour la connexion VPN via Juniper SSL.
6. Dans le champ **Rôle**, saisissez le nom du rôle d'utilisateur selon lequel l'utilisateur obtient l'accès aux ressources à l'aide de Juniper SSL.

Un rôle peut regrouper plusieurs utilisateurs qui exercent des fonctions identiques.

7. Sélectionnez l'onglet **Paramètres avancés**.
8. Dans la liste déroulante **Authentification de l'utilisateur**, sélectionnez le type d'authentification de l'utilisateur de l'appareil mobile iOS MDM lors de la connexion au réseau VPN via le protocole Juniper SSL :
   - **Mot de passe** : authentification de l'utilisateur à l'aide d'un mot de passe. Pour authentifier l'utilisateur sur le réseau privé virtuel, indiquez le mot de passe dans le champ **Mot de passe**.
   - **Certificat** : authentification de l'utilisateur à l'aide d'un certificat. Pour authentifier l'utilisateur sur le réseau privé virtuel, configurez les paramètres suivants :
     - **Certificats** ;
     - **Activer le VPN lors de la connexion des domaines** ;
     - **Durée d'inactivité avant déconnexion**.
9. Cliquez sur le bouton **OK**.

CONFIGURATION DE LA CONNEXION F5 SSL

Pour configurer les paramètres de sécurité pour la connexion F5 SSL du réseau VPN, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Réseaux privés virtuels (VPN)**.
3. Dans le groupe **Paramètres des réseaux privés virtuels**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Paramètres des réseaux privés virtuels (VPN)** s'ouvre.
4. Dans la liste déroulante **Type de connexion**, sélectionnez **F5 SSL**.
5. Sélectionnez l'onglet **Paramètres avancés**.
6. Dans la liste déroulante **Authentification de l'utilisateur**, sélectionnez le type d'authentification de l'utilisateur de l'appareil mobile iOS MDM lors de la connexion au réseau VPN via le protocole F5 SSL :
   - **Mot de passe** : authentification de l'utilisateur à l'aide d'un mot de passe. Pour authentifier l'utilisateur sur le réseau privé virtuel, indiquez le mot de passe dans le champ **Mot de passe**.
   - **Certificat** : authentification de l'utilisateur à l'aide d'un certificat. Pour authentifier l'utilisateur sur le réseau privé virtuel, configurez les paramètres suivants :
     - **Certificats** ;
     - **Activer le VPN lors de la connexion des domaines** ;
     - **Durée d'inactivité avant déconnexion**.
   - **Mot de passe + Certificat** : authentification de l'utilisateur à l'aide d'un mot de passe et d'un certificat.
7. Cliquez sur le bouton **OK**.

CONFIGURATION DE LA CONNEXION SONICWALL MOBILE CONNECT

Pour configurer les paramètres de sécurité pour la connexion SonicWALL Mobile Connect du réseau VPN, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Réseaux privés virtuels (VPN)**.
3. Dans le groupe **Paramètres des réseaux privés virtuels**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Paramètres des réseaux privés virtuels (VPN)** s'ouvre.
4. Dans la liste déroulante **Type de connexion**, sélectionnez **SonicWALL Mobile Connect**.
5. Dans le champ **Domaine ou Groupe**, saisissez le nom de domaine du serveur SSL VPN (par exemple, vpn.société.com) ou le nom du groupe d'utilisateur SonicWALL Mobile Connect.
6. Sélectionnez l'onglet **Paramètres avancés**.
7. Dans la liste déroulante **Authentification de l'utilisateur**, sélectionnez le type d'authentification de l'utilisateur de l'appareil mobile iOS MDM lors de la connexion au réseau VPN via le protocole SonicWALL Mobile Connect :
   - **Mot de passe** : authentification de l'utilisateur à l'aide d'un mot de passe. Pour authentifier l'utilisateur sur le réseau privé virtuel, indiquez le mot de passe dans le champ **Mot de passe**.
   - **Certificat** : authentification de l'utilisateur à l'aide d'un certificat. Pour authentifier l'utilisateur sur le réseau privé virtuel, configurez les paramètres suivants :
     - **Certificats** ;
     - **Activer le VPN lors de la connexion des domaines** ;
     - **Durée d'inactivité avant déconnexion**.
8. Cliquez sur le bouton **OK**.

CONFIGURATION DE LA CONNEXION ARUBA VIA

Pour configurer les paramètres de sécurité pour la connexion Aruba VIA du réseau VPN, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Réseaux privés virtuels (VPN)**.
3. Dans le groupe **Paramètres des réseaux privés virtuels**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Paramètres des réseaux privés virtuels (VPN)** s'ouvre.
4. Dans la liste déroulante **Type de connexion**, sélectionnez **Aruba VIA**.
5. Sélectionnez l'onglet **Paramètres avancés**.
6. Dans la liste déroulante **Authentification de l'utilisateur**, sélectionnez le type d'authentification de l'utilisateur de l'appareil iOS MDM lors de la connexion au réseau VPN via le protocole Aruba VIA :

- **Mot de passe** : authentification de l'utilisateur à l'aide d'un mot de passe. Pour authentifier l'utilisateur sur le réseau privé virtuel, indiquez le mot de passe dans le champ **Mot de passe**.
- **Certificat** : authentification de l'utilisateur à l'aide d'un certificat. Pour authentifier l'utilisateur sur le réseau privé virtuel, configurez les paramètres suivants :
  - **Certificats ;**
  - **Activer le VPN lors de la connexion des domaines ;**
  - **Durée d'inactivité avant déconnexion.**

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

CONFIGURATION DE LA CONNEXION CUSTOM SSL

Pour configurer les paramètres de sécurité pour la connexion Custom SSL du réseau VPN, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Réseaux privés virtuels (VPN)**.
3. Dans le groupe **Paramètres des réseaux privés virtuels**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Paramètres des réseaux privés virtuels (VPN)** s'ouvre.
4. Dans la liste déroulante **Type de connexion**, sélectionnez **Custom SSL**.
5. Dans le champ **Identificateur (entrée DNS inversée)**, saisissez le nom DNS de l'appareil mobile iOS MDM pour la connexion VPN Custom SSL (par exemple, com.example.vpn).
6. Dans le groupe **Données de configuration**, créez la liste des paires clé/valeur avec les paramètres avancés pour la connexion Custom SSL.
7. Sélectionnez l'onglet **Paramètres avancés**.
8. Dans la liste déroulante **Authentification de l'utilisateur**, sélectionnez le type d'authentification de l'utilisateur de l'appareil mobile iOS MDM lors de la connexion au réseau VPN via le protocole Custom SSL :
   - **Mot de passe** : authentification de l'utilisateur à l'aide d'un mot de passe. Pour authentifier l'utilisateur sur le réseau privé virtuel, indiquez le mot de passe dans le champ **Mot de passe**.
   - **Certificat** : authentification de l'utilisateur à l'aide d'un certificat. Pour authentifier l'utilisateur sur le réseau privé virtuel, configurez les paramètres suivants :
     - **Certificats** ;
     - **Activer le VPN lors de la connexion des domaines** ;
     - **Durée d'inactivité avant déconnexion**.
9. Cliquez sur le bouton **OK**.

Connexion aux appareils AirPlay

Afin de diffuser sans fil de la musique, des photos et des vidéos depuis un appareils iOS MDM vers un appareil AirPlay, il convient de configurer la connexion automatique aux appareils AirPlay. Pour pouvoir utiliser la technologie AirPlay, l'appareil mobile et l'appareil AirPlay doivent être connectés au même réseau sans fil. Les périphériques AirPlay regroupent les appareils Apple TV (de deuxième et troisième génération), les périphériques AirPort Express, et les enceintes ou récepteurs prenant en charge AirPlay.

La connexion automatique aux appareils AirPlay n'est disponible que pour les appareils contrôlés.

Pour configurer la connexion de l'appareil iOS MDM aux appareils AirPlay, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **AirPlay**.
3. Dans le groupe **Paramètres AirPlay**, cochez la case **Appliquer les paramètres à l'appareil**.
4. Dans le groupe **Mots de passe**, cliquez sur le bouton **Ajouter**.

   Une ligne vierge sera ajoutée au tableau des mots de passe.
5. Dans la colonne **Nom de l'appareil**, saisissez le nom de l'appareil AirPlay sur le réseau sans fil.
6. Dans la colonne **Mot de passe**, saisissez le mot de passe de l'appareil AirPlay.
7. Si vous souhaitez restreindre la connexion de l'appareil iOS MDM aux appareils AirPlay, créez la liste des appareils autorisés dans le groupe **Appareils autorisés**. Pour ce faire, ajoutez les adresses MAC des appareils AirPlay à la liste des appareils autorisés.

   L'accès aux appareils AirPlay ne figurant pas dans la liste des appareils autorisés est interdit. Si la liste des appareils autorisés est laissée vide, Kaspersky Mobile Device Management autorise l'accès à tous les appareils AirPlay.
8. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

L'appareil mobile de l'utilisateur se connectera ainsi automatiquement aux appareils AirPlay pour la diffusion sans fil de contenu multimédia une fois la stratégie appliquée.

Connexion a une imprimante AirPrint

Afin d'imprimer des documents depuis l'appareil iOS MDM à l'aide de la technologie sans fil AirPrint, il convient de configurer la connexion automatique aux imprimantes AirPrint. Pour pouvoir utiliser la technologie AirPrint, l'appareil mobile et l'imprimante doivent être connectés au même réseau sans fil. Un accès partagé pour tous les utilisateurs doit être configuré sur l'imprimante AirPrint.

Pour configurer la connexion de l'appareil iOS MDM à une imprimante AirPrint, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **AirPrint**.
3. Dans le groupe **Imprimantes**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Imprimante** s'ouvre.

4. Saisissez l'adresse IP de l'imprimante AirPrint dans le champ **Adresse IP**.
5. Saisissez le chemin d'accès à l'imprimante AirPrint dans le champ **Chemin d'accès à la ressource**.

   Le chemin d'accès à l'imprimante est conforme à la clé rp (resourse path) du protocole Bonjour. Par exemple :

   - printers/Canon_MG5300_series ;
   - ipp/print ;
   - Epson_IPP_Printer.
6. Cliquez sur le bouton **OK**.

   L'imprimante AirPrint ajoutée s'affichera dans la liste.
7. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

L'utilisateur de l'appareil mobile pourra ainsi imprimer des documents sur une imprimante AirPrint via une connexion sans fil une fois la stratégie appliquée.

AJOUT D'UN COMPTE UTILISATEUR DE MESSAGERIE ELECTRONIQUE

Afin de permettre à l'utilisateur de l'appareil iOS MDM d'utiliser sa messagerie électronique, il convient d'ajouter un compte utilisateur de messagerie électronique.

Par défaut, le compte utilisateur de messagerie électronique est ajouté avec les paramètres suivants :

- protocole de messagerie électronique : IMAP ;
- l'utilisateur peut transférer des messages électroniques d'un compte à un autre et synchroniser les adresses de ses comptes utilisateur ;
- l'utilisateur peut utiliser n'importe quel client de messagerie (sans se limiter à Mail) ;
- les messages électroniques sortants de l'appareil de l'utilisateur ne sont pas chiffrés selon le protocole S/MIME ;
- le transfert des messages ne passe pas par une connexion SSL.

Vous pouvez modifier les paramètres établis lors de l'ajout d'un compte utilisateur.

Pour ajouter un compte utilisateur de messagerie électronique pour l'utilisateur de l'appareil iOS MDM, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Messagerie électronique**.
3. Dans le groupe **Comptes utilisateur de messagerie électronique**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Compte utilisateur de messagerie électronique** s'ouvre.
4. Dans le champ **Description du compte utilisateur**, saisissez la description du compte de messagerie électronique de l'utilisateur.

5. Sélectionnez le protocole de messagerie électronique :

   - **POP** ;
   - **IMAP**.

6. Si nécessaire, indiquez le préfixe du chemin IMAP dans le champ **Préfixe du chemin IMAP**.

   Le préfixe du chemin IMAP doit être indiqué en majuscules (par exemple, GMAIL pour Google Mail™). Champ disponible si le protocole de compte utilisateur IMAP a été sélectionné.

7. Dans le champ **Nom de l'utilisateur à afficher dans les messages**, saisissez le nom de l'utilisateur qui sera affiché dans le champ **De :** de tous les messages sortants.

8. Dans le champ **Adresse de messagerie électronique**, saisissez l'adresse électronique de l'utilisateur de l'appareil iOS MDM.

9. Configurez les paramètres avancés du compte utilisateur de messagerie électronique :

   - Si vous souhaitez que l'utilisateur puisse transférer les messages électroniques d'un de ses comptes utilisateur à un autre, cochez la case **Autoriser le transfert de messages entre les comptes utilisateur**.
   - Si vous souhaitez que les adresses utilisées se synchronisent entre les comptes de l'utilisateur, cochez la case **Autoriser la synchronisation des dernières adresses utilisées**.
   - Si vous souhaitez que l'utilisateur utilise uniquement le client de messagerie iOS standard, cochez la case **Autoriser l'utilisation de Mail uniquement**.
   - Si vous souhaitez utiliser le protocole S/MIME pour le chiffrement des messages sortants, cochez la case **Utiliser S/MIME**.

10. Dans les groupes **Serveur de messagerie entrante** et **Serveur de messagerie sortante**, cliquez sur **Configuration** et configurez les paramètres de connexion aux serveurs :

    - **Adresse du serveur et port** : noms des hôtes ou adresses IP des serveurs du courrier entrant et sortant et numéros des ports des serveurs.
    - **Nom du compte utilisateur** : nom du compte de l'utilisateur pour l'autorisation d'accès au serveur du courrier entrant et sortant.
    - **Type d'authentification** : type d'authentification du compte de l'utilisateur de messagerie électronique sur les serveurs du courrier entrant et sortant.
    - **Mot de passe** : mot de passe du compte utilisateur pour l'autorisation d'accès au serveur du courrier entrant et sortant protégé par la méthode d'authentification sélectionnée.
    - **Utiliser une connexion SSL** : utilisation du protocole de transport SSL (Secure Sockets Layer) pour le transfert de données. Ce protocole applique le chiffrement et l'authentification sur la base de certificats pour la protection du transfert de données.

11. Cliquez sur le bouton **OK**.

    Le nouveau compte utilisateur de messagerie électronique s'affichera dans la liste.

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

Les comptes utilisateur de messagerie électronique seront ainsi ajoutés sur l'appareil mobile de l'utilisateur à partir de la liste créée une fois la stratégie appliquée.

AJOUT D'UN COMPTE UTILISATEUR EXCHANGE ACTIVESYNC

Afin de permettre à l'utilisateur de l'appareil iOS MDM de travailler avec la messagerie électronique, le calendrier, les contacts, les notes et les tâches de l'entreprise, il convient d'ajouter un compte utilisateur Exchange ActiveSync sur le serveur Microsoft Exchange.

Par défaut, le compte utilisateur est ajouté sur le serveur Microsoft Exchange avec les paramètres suivants :

- la messagerie est synchronisée une fois par semaine ;
- l'utilisateur peut transférer des messages d'un compte à un autre et synchroniser les adresses de ses comptes utilisateur ;
- l'utilisateur peut utiliser n'importe quel client de messagerie (sans se limiter à Mail) ;
- les messages électroniques sortants de l'appareil de l'utilisateur ne sont pas chiffrés selon le protocole S/MIME ;
- le transfert des messages ne passe pas par une connexion SSL.

Vous pouvez modifier les paramètres établis lors de l'ajout d'un compte utilisateur Exchange ActiveSync.

Pour ajouter un compte utilisateur Exchange ActiveSync pour l'utilisateur de l'appareil iOS MDM, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Exchange ActiveSync**.
3. Dans le groupe **Comptes utilisateur Exchange ActiveSync**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Compte utilisateur Exchange ActiveSync** s'ouvre à l'onglet **Généraux**.
4. Dans le champ **Nom du compte utilisateur**, saisissez le nom du compte utilisateur pour l'autorisation sur le serveur Microsoft Exchange. Vous pouvez utiliser les macros de la liste déroulante **Ajouter un macro**.
5. Dans le champ **Adresse du serveur**, saisissez le nom réseau ou l'adresse IP du serveur Microsoft Exchange.
6. Si vous souhaitez utiliser le protocole de transfert de données SSL afin de protéger le transfert de données, cochez la case **Utiliser une connexion SSL**.
7. Dans le champ **Domaine**, saisissez le nom de domaine de l'utilisateur de l'appareil iOS MDM. Vous pouvez utiliser les macros de la liste déroulante **Ajouter un macro**.
8. Dans le champ **Utilisateur du compte**, saisissez le nom de l'utilisateur de l'appareil iOS MDM.

   Si ce champ est laissé vide, Kaspersky Mobile Device Management demandera le nom de l'utilisateur lors de l'application de la stratégie sur l'appareil iOS MDM. Vous pouvez utiliser les macros de la liste déroulante **Ajouter un macro**.
9. Dans le champ **Adresse de messagerie électronique**, saisissez l'adresse électronique de l'utilisateur de l'appareil iOS MDM. Vous pouvez utiliser les macros de la liste déroulante **Ajouter un macro**.
10. Dans le champ **Mot de passe**, saisissez le mot de passe du compte utilisateur Exchange ActiveSync pour l'autorisation sur le serveur Microsoft Exchange.
11. Sélectionnez l'onglet **Paramètres avancés** et configurez-y les paramètres avancés du compte utilisateur Exchange ActiveSync :

- **Synchroniser le courrier pour la période ;**
- **Type d'authentification ;**
- **Autoriser le déplacement des messages entre les comptes ;**
- **Autoriser la synchronisation des dernières adresses utilisées ;**
- **Autoriser l'utilisation de Mail uniquement ;**
- **Utiliser S/MIME ;**
- **Certificat de signature ;**
- **Certificat de chiffrement.**

12. Cliquez sur le bouton **OK**.

    Le nouveau compte utilisateur Exchange ActiveSync s'affichera dans la liste.

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

Les comptes utilisateur Exchange ActiveSync seront ainsi ajoutés sur l'appareil mobile de l'utilisateur à partir de la liste créée une fois la stratégie appliquée.

AJOUT D'UN COMPTE UTILISATEUR LDAP

Afin que l'utilisateur de l'appareil iOS MDM puisse accéder aux contacts de l'entreprise sur le serveur LDAP, il convient d'ajouter un compte utilisateur LDAP.

Pour ajouter un compte utilisateur LDAP pour l'utilisateur de l'appareil iOS MDM, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés <nom de la stratégie>** qui s'ouvre, sélectionnez la section **LDAP**.
3. Dans le groupe **Comptes utilisateur LDAP**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Compte utilisateur LDAP et paramètres de la recherche** s'ouvre.

4. Dans le champ **Description du compte utilisateur**, saisissez la description du compte LDAP de l'utilisateur. Vous pouvez utiliser les macros de la liste déroulante **Ajouter un macro**.
5. Dans le champ **Nom du compte utilisateur**, saisissez le nom du compte utilisateur pour l'autorisation sur le serveur LDAP. Vous pouvez utiliser les macros de la liste déroulante **Ajouter un macro**.
6. Dans le champ **Mot de passe**, saisissez le mot de passe du compte utilisateur LDAP pour l'autorisation sur le serveur LDAP.
7. Dans le champ **Adresse du serveur**, saisissez le nom de domaine du serveur LDAP. Vous pouvez utiliser les macros de la liste déroulante **Ajouter un macro**.
8. Si vous souhaitez utiliser le protocole de transfert de données SSL afin de protéger le transfert de messages, cochez la case **Utiliser une connexion SSL**.

9. Créez la liste des recherches pour l'accès de l'utilisateur de l'appareil iOS MDM aux dossiers comportant des données d'entreprise sur le serveur LDAP :

   a. Dans le groupe **Paramètres de la recherche**, cliquez sur le bouton **Ajouter**.

      Une ligne vierge apparaîtra dans le tableau des recherches.

   b. Dans la colonne **Nom**, saisissez le nom de la recherche sélectionnée.

   c. Dans la colonne **Profondeur de la recherche**, sélectionnez le niveau d'imbrication du dossier pour la recherche de données d'entreprise sur le serveur LDAP :

      - **Racine de l'arborescence** : recherche dans le dossier de base du serveur LDAP.
      - **Un niveau** : recherche dans les dossiers du premier niveau d'imbrication à partir du dossier de base.
      - **Sous-arbre** : recherche dans les dossiers de tous les niveaux d'imbrication à partir du dossier de base.

   d. Dans la colonne **Base de la recherche**, indiquez le chemin d'accès sur le serveur LDAP au dossier à partir duquel la recherche commence (par exemple, "ou=people", "o=example corp").

   e. Répétez les points a à d pour toutes les recherches que vous souhaitez ajouter à l'appareil iOS MDM.

10. Cliquez sur le bouton **OK**.

    Le nouveau compte utilisateur LDAP s'affichera dans la liste.

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

Les comptes utilisateur LDAP seront ainsi ajoutés sur l'appareil mobile de l'utilisateur à partir de la liste créée une fois la stratégie appliquée. L'utilisateur peut accéder aux contacts professionnels dans les applications standard Contacts, Messages et Mail d'iOS.

AJOUT D'UN COMPTE UTILISATEUR POUR LE CALENDRIER

Afin que l'utilisateur de l'appareil iOS MDM puisse utiliser ses événements du calendrier sur le serveur CalDAV, il convient d'ajouter un compte utilisateur sur CalDAV. La synchronisation avec CalDAV permettra à l'utilisateur de créer et d'accepter des invitations, de recevoir les mises à jour des événements et de synchroniser les tâches avec l'application Rappels.

Pour ajouter un compte utilisateur CalDAV pour l'utilisateur de l'appareil iOS MDM, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Calendrier**.

3. Dans le groupe **Comptes utilisateur CalDAV**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Compte utilisateur CalDAV** s'ouvre.

4. Dans le champ **Description du compte utilisateur**, saisissez la description du compte CalDAV de l'utilisateur. Vous pouvez utiliser les macros de la liste déroulante **Ajouter un macro**.

5. Dans le champ **Adresse du serveur et port**, indiquez le nom de l'hôte ou l'adresse IP du serveur CalDAV et le numéro de port du serveur CalDAV.

6. Dans le champ **URL principale**, indiquez l'URL du compte CalDAV de l'utilisateur de l'appareil iOS MDM sur le serveur CalDAV (par exemple, http://example.com/caldav/users/mycompany/user).

   L'URL doit commencer par "http://" ou "https://".

7. Dans le champ **Nom du compte utilisateur**, indiquez le nom du compte utilisateur pour l'autorisation sur le serveur CalDAV. Vous pouvez utiliser les macros de la liste déroulante **Ajouter un macro**.

8. Dans le champ **Mot de passe du compte utilisateur**, indiquez le mot de passe du compte utilisateur CalDAV pour l'autorisation sur le serveur CalDAV.

9. Si vous souhaitez utiliser le protocole de transfert de données SSL afin de protéger le transfert de données sur les événements entre le serveur CalDAV et l'appareil mobile, cochez la case **Utiliser une connexion SSL**.

10. Cliquez sur le bouton **OK**.

    Le nouveau compte utilisateur CalDAV s'affichera dans la liste.

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

Les comptes utilisateur CalDAV seront ainsi ajoutés sur l'appareil mobile de l'utilisateur à partir de la liste créée une fois la stratégie appliquée.

AJOUT D'UN COMPTE UTILISATEUR POUR LES CONTACTS

Afin que l'utilisateur de l'appareil iOS MDM puisse synchroniser ses contacts avec le serveur CardDAV, il convient d'ajouter un compte utilisateur CardDAV. La synchronisation avec le serveur CardDAV permettra à l'utilisateur d'avoir accès aux données des contacts depuis n'importe quel appareil.

Pour ajouter un compte utilisateur CardDAV pour l'utilisateur de l'appareil iOS MDM, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Contacts**.

3. Dans le groupe **Comptes utilisateur CardDAV**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Compte utilisateur CardDAV** s'ouvre.

4. Dans le champ **Description du compte utilisateur**, saisissez la description du compte CardDAV de l'utilisateur. Vous pouvez utiliser les macros de la liste déroulante **Ajouter un macro**.

5. Dans le champ **Adresse du serveur et port**, indiquez le nom de l'hôte ou l'adresse IP du serveur CardDAV et le numéro de port du serveur CardDAV.

6. Dans le champ **URL principale**, indiquez l'URL du compte CardDAV de l'utilisateur de l'appareil iOS MDM sur le serveur CardDAV (par exemple, http://example.com/carddav/users/mycompany/user).

   L'URL doit commencer par "http://" ou "https://".

7. Dans le champ **Nom du compte utilisateur**, indiquez le nom du compte utilisateur pour l'autorisation sur le serveur CardDAV. Vous pouvez utiliser les macros de la liste déroulante **Ajouter un macro**.

8. Dans le champ **Mot de passe du compte utilisateur**, indiquez le mot de passe du compte utilisateur CardDAV pour l'autorisation sur le serveur CardDAV.

9. Si vous souhaitez utiliser le protocole de transfert de données SSL afin de protéger le transfert de contacts entre le serveur CardDAV et l'appareil mobile, cochez la case **Utiliser une connexion SSL**.

10. Cliquez sur le bouton **OK**.

    Le nouveau compte utilisateur CardDAV s'affichera dans la liste.

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

Les comptes utilisateur CardDAV seront ainsi ajoutés sur l'appareil mobile de l'utilisateur à partir de la liste créée une fois la stratégie appliquée.

CONFIGURATION DE L'ABONNEMENT A UN CALENDRIER

Afin que l'utilisateur de l'appareil iOS MDM puisse ajouter à son calendrier les événements de calendriers tiers (tels que le calendrier de l'entreprise), il est nécessaire d'ajouter un abonnement au calendrier. Les *calendriers tiers* sont des calendriers appartenant à d'autres utilisateurs possédant un compte CalDAV, des calendriers iCal et d'autres calendriers publics.

Pour ajouter un abonnement à un calendrier, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Abonnement à un calendrier**.

3. Dans le groupe **Paramètres des abonnements**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Abonnement à un calendrier** s'ouvre.

4. Saisissez une description de l'abonnement au calendrier dans le champ **Description**. Vous pouvez utiliser les macros de la liste déroulante **Ajouter un macro**.

5. Dans le champ **URL**, indiquez l'URL du calendrier tiers.

   Ce champ peut servir à indiquer l'URL principale du compte CalDAV de l'utilisateur sur le calendrier pour lequel l'abonnement est créé. Vous pouvez également indiquer l'URL du calendrier iCal ou d'un autre calendrier public.

6. Dans le champ **Nom d'utilisateur**, saisissez le nom du compte utilisateur pour l'autorisation sur le serveur du calendrier tiers. Vous pouvez utiliser les macros de la liste déroulante **Ajouter un macro**.

7. Dans le champ **Mot de passe**, saisissez le mot de passe de l'abonnement au calendrier pour l'autorisation d'accès au serveur du calendrier tiers.

8. Si vous souhaitez utiliser le protocole de transfert de données SSL afin de protéger le transfert de données sur les événements entre le serveur CalDAV et l'appareil mobile, cochez la case **Utiliser une connexion SSL**.

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

   Le nouvel abonnement au calendrier s'affichera dans la liste.

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

Les événements des calendriers tiers seront ainsi ajoutés au calendrier de l'appareil mobile de l'utilisateur à partir de la liste créée une fois la stratégie appliquée.

AJOUT DE RACCOURCIS INTERNET

Un raccourci Internet est une application qui ouvre un site Internet depuis l'écran principal de l'appareil mobile. En cliquant sur l'icône des raccourcis Internet sur l'écran principal de l'appareil, l'utilisateur peut rapidement ouvrir des sites Internet (tels que le site de l'entreprise). Vous pouvez ajouter des raccourcis Internet sur les appareils des utilisateurs et configurer l'apparence de l'icône du raccourci affichée sur l'écran.

Par défaut, les restrictions suivantes s'appliquent à l'utilisation des raccourcis Internet :

- L'utilisateur ne peut pas supprimer lui-même les raccourcis Internet de l'appareil mobile.
- Les sites Internet qui s'ouvrent en cliquant sur l'icône du raccourci Internet ne s'affichent pas en plein écran.
- Des effets graphiques d'arrondissement des coins, d'ombre et de brillance s'appliquent à l'icône du raccourci Internet sur l'écran.

Pour ajouter un raccourci Internet à l'appareil iOS MDM de l'utilisateur, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Raccourcis Internet**.
3. Dans le groupe **Paramètres des raccourcis Internet**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Raccourcis Internet** s'ouvre.
4. Dans le champ **Nom**, saisissez le nom du raccourci Internet qui s'affichera sur l'écran principal de l'appareil iOS MDM.
5. Dans le champ **URL**, saisissez l'adresse du site Internet qui s'ouvrira si vous cliquez sur l'icône du raccourci Internet. L'adresse doit commencer par "http://" ou "https://".
6. Si vous souhaitez permettre à l'utilisateur de supprimer un raccourci Internet de l'appareil iOS MDM, cochez la case **Autoriser la suppression**.
7. Cliquez sur le bouton **Sélectionner** et indiquez le fichier contenant l'image pour l'icône du raccourci Internet.

   L'icône s'affichera sur l'écran principal de l'appareil iOS MDM. L'image doit remplir les conditions suivantes :

   - taille de 400 x 400 pixels maximum ;
   - format de fichier GIF, JPEG ou PNG ;
   - taille du fichier de 1 Mo maximum.

   Vous pouvez accéder à un aperçu de l'icône du raccourci Internet dans le champ **Icône**. Si vous ne sélectionnez pas d'image pour le clip Internet, l'icône apparaîtra sous la forme d'un carré blanc.
8. Si vous souhaitez que l'icône du raccourci Internet s'affiche sans effet graphique particulier (arrondissement des coins de l'icône et effet de brillance), cochez la case **Raccourci Internet sans effet graphique**.
9. Si vous souhaitez qu'en cas de pression sur l'icône le site Internet s'ouvre sur toute la surface de l'écran de l'appareil iOS MDM, cochez la case **Raccourci Internet en plein écran**.
10. Cliquez sur le bouton **OK**.

    Le nouveau raccourci Internet s'affichera dans la liste.
11. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

Les icônes des raccourcis Internet seront ainsi ajoutés à l'écran principal de l'appareil mobile de l'utilisateur à partir de la liste créée une fois la stratégie appliquée.

AJOUT DE POLICES D'ECRITURE

Pour ajouter une police d'écriture à l'appareil iOS MDM de l'utilisateur, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Polices**.
3. Dans le groupe **Paramètres des polices**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Police** s'ouvre.
4. Dans le champ **Nom du fichier**, indiquez le chemin d'accès au fichier de la police (fichier à l'extension ttf ou otf).

   Les polices présentant l'extension ttc ou otc ne sont pas prises en charge.

   Les polices sont identifiées par le nom PostScript. N'installez pas de polices présentant un nom PostScript identique, même si leur contenu diffère. L'installation de polices présentant un nom PostScript identique entraîne une erreur inconnue.
5. Cliquez sur le bouton **Ouvrir**.

   La nouvelle police s'affichera dans la liste.
6. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

Il sera ainsi proposé à l'utilisateur d'installer les polices sur l'appareil mobile à partir de la liste créée une fois la stratégie appliquée.

AJOUT DE CERTIFICATS DE SECURITE

Afin de faciliter l'authentification de l'utilisateur et d'assurer la sécurité des données, il convient d'ajouter des certificats à l'appareil iOS MDM de l'utilisateur. La signature des données à l'aide d'un certificat empêche leur altération pendant l'échange en réseau. Le chiffrement des données à l'aide d'un certificat offre un niveau de sécurité de l'information encore plus élevé. Le certificat peut également être utilisé pour l'authentification de l'utilisateur.

Kaspersky Mobile Device Management prend en charge les standards de certificats suivants :

- **PKCS#1** : chiffrement avec clé publique sur la base des algorithmes RSA.
- **PKCS#12** : stockage et transfert du certificat et de la clé privée.

Pour ajouter un certificat de sécurité à l'appareil iOS MDM de l'utilisateur, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Certificats**.
3. Dans le groupe **Paramètres des certificats**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Certificat** s'ouvre.
4. Indiquez le chemin d'accès au certificat dans le champ **Nom du fichier** :

Les fichiers des certificats PKCS#1 possèdent une extension cer, crt ou der. Les fichiers des certificats PKCS#12 possèdent une extension p12 ou pfx.

5. Cliquez sur le bouton **Ouvrir**.

   Si le certificat est protégé par un mot de passe, celui-ci devra être saisi. Le nouveau certificat s'affichera ensuite dans la liste.

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

Il sera ainsi proposé à l'utilisateur d'installer les certificats sur l'appareil mobile à partir de la liste créée une fois la stratégie appliquée.

CONFIGURATION DU PROFIL SCEP

Afin de permettre à l'utilisateur de l'appareil iOS MDM de recevoir automatiquement par Internet les certificats depuis le Centre de certification, il convient d'ajouter un profil SCEP. Un profil SCEP permet de prendre en charge le protocole simple d'enregistrement de certificats.

Par défaut, le profil SCEP est ajouté avec les paramètres suivants :

- L'enregistrement de certificats n'utilise pas de nom de sujet alternatif.
- Trois tentatives de requête sont envoyées au serveur SCEP avec un intervalle de 10 s entre chaque tentative. Si toutes les tentatives de signature du certificat se sont avérées infructueuses, il est nécessaire de créer une nouvelle requête de signature du certificat.
- Il est interdit d'utiliser le certificat obtenu pour la signature ou le chiffrement des données.

Vous pouvez modifier les paramètres établis lors de l'ajout d'un profil SCEP.

Pour ajouter un profil SCEP, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **SCEP**.
3. Dans le groupe **Profils SCEP**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Profil SCEP** s'ouvre.
4. Dans le champ **URL**, saisissez l'URL du serveur SCEP sur lequel le Centre de certification est déployé.

   L'URL peut comporter l'adresse IP ou le nom de domaine complet (FQDN), par exemple http://10.10.10.10/certserver/companyscep.
5. Dans le champ **Nom**, saisissez le nom du Centre de certification déployé sur le serveur SCEP.
6. Dans le champ **Sujet**, saisissez la ligne contenant les attributs de l'utilisateur de l'appareil iOS MDM qui seront contenus dans le certificat X.500.

   Les caractéristiques peuvent contenir des informations sur le pays (C), l'entreprise (O) et le nom public de l'utilisateur (CN). Par exemple, /C=RU/O=MyCompany/CN=User/. Vous pouvez également utiliser d'autres caractéristiques prévues dans RFC 5280.

7. Dans la liste déroulante **Type de nom alternatif du sujet**, sélectionnez le type de nom alternatif du sujet du serveur SCEP :

   - **Aucun** : l'identification par un nom alternatif n'est pas utilisée.
   - **Nom RFC 822** : identification en fonction de l'adresse de messagerie électronique. L'adresse de messagerie électronique doit être conforme à RFC 822.
   - **Nom DNS** : identification en fonction du nom de domaine.
   - **URI** : identification par adresse IP ou une adresse au format FQDN.

   Vous pouvez utiliser un nom de sujet alternatif pour l'identification de l'utilisateur de l'appareil mobile iOS MDM.

8. Dans le champ **Nom alternatif du sujet**, saisissez le nom alternatif du sujet du certificat X.500. La valeur du nom alternatif du sujet dépend du type du sujet : adresse de messagerie électronique de l'utilisateur, domaine ou URL.

9. Dans le champ **Nom du sujet NT**, saisissez le nom DNS de l'utilisateur de l'appareil mobile iOS MDM sur le réseau Windows NT.

   Le nom du sujet NT est repris dans la demande de certificat sur le serveur SCEP.

10. Dans le champ **Nombre de tentatives de requête auprès du serveur SCEP**, indiquez le nombre maximal de tentatives de requête auprès du serveur SCEP pour la signature d'un certificat.

11. Dans le champ **Intervalle entre les tentatives (en secondes)**, indiquez l'intervalle en secondes entre les tentatives de requête auprès du serveur SCEP pour la signature d'un certificat.

12. Dans le champ **Demande d'enregistrement**, saisissez la clé d'enregistrement préalablement publiée.

    Avant de signer le certificat, le serveur SCEP demande une clé à l'utilisateur de l'appareil mobile. Si ce champ reste vide, le serveur SCEP ne demande pas de clé.

13. Dans la liste déroulante **Taille de la clé**, sélectionnez la taille en octets de la clé d'enregistrement : 1024 ou 2048.

14. Si vous souhaitez permettre à l'utilisateur d'utiliser le certificat obtenu depuis le serveur SCEP en tant que certificat pour la signature, cochez la case **Utiliser pour la signature**.

15. Si vous souhaitez permettre à l'utilisateur d'utiliser le certificat obtenu depuis le serveur SCEP pour le chiffrement des données, cochez la case **Utiliser pour le chiffrement**.

    Il est interdit d'utiliser un certificat du serveur SCEP servant à la fois de certificat de signature des données et de certificat de chiffrement.

16. Dans le champ **Empreinte du certificat**, saisissez l'empreinte unique du certificat pour la vérification de l'authenticité de la réponse du Centre d'authentification. Vous pouvez utiliser les empreintes des certificats avec un algorithme de mise en cache SHA-1 ou MD5. Vous pouvez copier manuellement l'empreinte du certificat ou sélectionner le certificat à l'aide du bouton **Créer à partir du certificat**. Si vous créez l'empreinte à l'aide du bouton **Créer à partir du certificat**, l'empreinte sera automatiquement ajoutée au champ.

    L'empreinte du certificat doit indiquer si l'échange de données entre l'appareil mobile et le Centre de certification s'effectue selon le protocole HTTP.

17. Cliquez sur le bouton **OK**.

    Le nouveau profil SCEP s'affichera dans la liste.

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

La réception automatique par Internet du certificat depuis le Centre de certification sera ainsi configurée sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

CONFIGURATION DU POINT D'ACCES (APN)

Afin de permettre à l'utilisateur de l'appareil iOS MDM de se connecter aux services de transfert de données sur le réseau mobile, il convient de configurer le point d'accès (APN).

Pour configurer le point d'accès sur l'appareil iOS MDM de l'utilisateur, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des appareils iOS MDM (cf. section "Configuration d'une stratégie de groupe pour l'administration des appareils iOS MDM" à la page 94).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Point d'accès (APN)**.
3. Dans le groupe **Paramètres du point d'accès**, cochez la case **Appliquer les paramètres à l'appareil**.
4. Dans le champ **Nom du point d'accès**, indiquez le nom du point d'accès.
5. Dans le champ **Nom de l'utilisateur**, saisissez le nom de l'utilisateur pour l'autorisation sur le réseau mobile.
6. Dans le champ **Mot de passe**, saisissez le mot de passe pour l'autorisation de l'utilisateur sur le réseau mobile.
7. Dans le champ **Adresse du serveur proxy et port**, indiquez le nom de l'hôte, le domaine ou l'adresse IP du serveur proxy et le numéro de port du serveur proxy.
8. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

Le point d'accès (APN) sera ainsi configuré sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

SUPPRESSION D'UNE STRATEGIE DE GROUPE

Pour supprimer une stratégie de groupe, procédez comme suit :

1. Dans l'arborescence de la Console du Kaspersky Security Center, sélectionnez le groupe d'administration pour lequel vous souhaitez supprimer une stratégie.
2. Dans la zone de travail du groupe d'administration, sous l'onglet **Stratégies**, sélectionnez la stratégie que vous souhaitez supprimer.
3. Supprimez la stratégie d'une des manières suivantes :
   - Dans le menu contextuel de la stratégie, choisissez l'option **Supprimer**.
   - En suivant le lien **Supprimer la stratégie** situé dans la zone de travail à droite, dans le groupe de travail de la stratégie sélectionnée.

La stratégie de groupe sera ainsi supprimée. Les appareils mobiles appartenant au groupe d'administration continueront de fonctionner avec les paramètres définis dans la stratégie supprimée jusqu'à ce qu'une nouvelle stratégie de groupe soit appliquée.

SUPPRESSION DES APPLICATIONS MOBILES KASPERSKY ENDPOINT SECURITY DES APPAREILS

Cette section reprend les informations sur la suppression des applications mobiles Kaspersky Endpoint Security 10 des appareils des utilisateurs.

DANS CETTE SECTION

SUPPRESSION DE L'APPLICATION MOBILE KASPERSKY ENDPOINT SECURITY FOR ANDROID

L'utilisateur peut supprimer lui-même Kaspersky Endpoint Security for Android de son appareil si cette possibilité n'a pas été bloquée par la stratégie de groupe.

Si la suppression de l'application est autorisée par la stratégie de groupe, l'utilisateur peut supprimer lui-même Kaspersky Endpoint Security for Android de l'appareil à l'aide de l'interface de l'application ou des paramètres de l'appareil Android.

Si la stratégie interdit de supprimer l'application Kaspersky Endpoint Security for Android de l'appareil, l'utilisateur doit s'adresser à l'administrateur. Vous pouvez soit supprimer l'application à distance à l'aide du Kaspersky Security Center, soit permettre de supprimer l'application de l'appareil via les propriétés locales de l'application ou via la stratégie appliquée à l'appareil.

PERMETTRE AUX UTILISATEURS DE SUPPRIMER L'APPLICATION

Vous pouvez permettre aux utilisateurs de supprimer l'application Kaspersky Endpoint Security for Android des appareils en utilisant la stratégie de groupe. Vous pouvez permettre ou non à l'utilisateur d'un appareil de supprimer Kaspersky Endpoint Security for Android de son appareil via les paramètres locaux de l'application dans la Console d'administration.

Si vous souhaitez autoriser la suppression de l'application sur tous les appareils du groupe, vous pouvez autoriser cette action dans les propriétés de la stratégie de groupe établie auparavant.

Si vous souhaitez autoriser la suppression de l'application uniquement de certains appareils du groupe, vous devez configurer une nouvelle stratégie de groupe et l'appliquer aux appareils appropriés. Au cours de la prochaine synchronisation des appareils mobiles avec le Serveur d'administration, l'application sera accessible pour une auto-suppression.

Pour permettre la suppression de Kaspersky Endpoint Security for Android sur plusieurs appareils, procédez comme suit :

1. Dans l'arborescence de la Console d'administration du Kaspersky Security Center, sélectionnez le Serveur d'administration auquel sont connectés les appareils mobiles.

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

3. Dans le dossier **Ordinateurs administrés** choisissez le groupe où se trouvent les appareils sur lesquels les utilisateurs pourront supprimer l'application.

4. Vous pouvez créer un nouveau sous-groupe d'une des manières suivantes :

   - dans le menu contextuel du dossier **Ordinateurs administrés** de l'arborescence de la console ou dans le menu contextuel du sous-dossier, choisissez l'option **Créer → Groupe**;

   - dans l'espace de travail du dossier, choisissez l'onglet **Groupes** et ouvrez la fenêtre en cliquant sur le lien **Créer un sous-groupe**.

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

6. Lancez la procédure d'ajout à ce groupe d'appareils pour lesquels vous souhaitez autoriser la suppression de l'application par l'un des procédés suivants :

   - via le lien **Ajouter des ordinateurs dans le groupe** situé dans la zone de travail de la fenêtre principale de la Console d'administration, sous l'onglet **Groupes** ;

   - via le lien **Ajouter des ordinateurs** situé dans la zone de travail de la fenêtre principale de la Console d'administration, sous l'onglet **Ordinateurs**.

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

7. Dans la zone de travail du groupe créé, sélectionnez l'onglet **Stratégies** et lancez l'assistant de la création de la politique en suivant le lien **Créer stratégie**.

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

   - A l'étape **Sélection de l'application pour la création de la stratégie de groupe**, sélectionnez Kaspersky Endpoint Security 10 Service Pack 1 pour les appareils mobiles.

   - A l'étape **Paramètres avancés** du groupe **Administration de l'application** cochez la case **Autoriser la suppression de Kaspersky Endpoint Security for Android**.

   - A l'étape **Création de la stratégie de groupe**, dans le groupe de paramètres **Etat de la stratégie**, choisissez l'option **Stratégie active**.

La stratégie créée sera alors active pour le groupe d'administration sélectionné. Suite à la synchronisation des appareils mobiles de ce groupe avec le Serveur d'administration, l'application Kaspersky Endpoint Security for Android peut être supprimée par les utilisateurs.

Pour permettre la suppression de Kaspersky Endpoint Security for Android sur un appareil en particulier, procédez comme suit :

1. Dans l'arborescence de la Console d'administration du Kaspersky Security Center, sélectionnez le Serveur d'administration auquel sont connectés les appareils mobiles.

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

3. Dans le dossier **Ordinateurs administrés**, choisissez le groupe d'appareils dans lequel vous envisagez d'autoriser la suppression de l'application.

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

5. Dans la liste des objets, sélectionnez la stratégie active qui vous permet de gérer les appareils du groupe sélectionné.

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

7. Dans la fenêtre **Propriétés <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Paramètres avancés**.

8. Dans le groupe **Administration de l'application**, assurez-vous que le cadenas a l'aspect suivant  , ce qui signifie que les paramètres de ce groupe peuvent être modifiés dans les paramètres locaux de l'application.

   Le cas échéant, cliquez sur le bouton  pour pouvoir modifier les paramètres du groupe **Administration de l'application** dans les paramètres locaux de l'application.

9. Dans la zone de travail du groupe d'administration, choisissez l'onglet **Ordinateurs**.

10. Choisissez l'appareil de l'utilisateur dans la liste des appareils administrés.

11. Double-cliquez sur l'appareil sélectionné pour ouvrir la fenêtre de ses propriétés.

12. Dans la fenêtre **Propriétés : <nom de l'appareil>** qui s'ouvre, choisissez le groupe **Applications**.

13. Dans le groupe **Applications**, choisissez **Kaspersky Endpoint Security 10 Service Pack 1 for Mobile**.

14. Double-cliquez sur l'application sélectionnée pour ouvrir la fenêtre de ses propriétés.

15. Dans la section **Paramètres avancés** du groupe **Administration de l'application**, cochez la case **Autoriser la suppression de Kaspersky Endpoint Security for Android**.

Suite à la prochaine synchronisation de cet appareil mobile avec le Serveur d'administration, l'application Kaspersky Endpoint Security for Android pourra être supprimée par l'utilisateur.

SUPPRESSION DES DONNEES DE L'APPAREIL

Vous pouvez effectuer la suppression à distance de Kaspersky Endpoint Security for Android des appareils mobiles des utilisateurs connectés au Serveur d'administration Kaspersky Security Center.

Si vous souhaitez supprimer l'application sur tous les appareils du groupe, vous pouvez utiliser les propriétés de la stratégie créée au préalable pour ce groupe.

Si vous souhaitez autoriser la suppression de l'application uniquement de certains appareils, vous devez configurer une nouvelle stratégie de groupe et l'appliquer aux appareils appropriés. Lors de la prochaine synchronisation des appareils mobiles avec le Serveur d'administration, cette application sera supprimée.

Afin de supprimer Kaspersky Endpoint Security de quelques appareils mobiles sans participation de l'utilisateur, procédez comme suit:

1. Dans l'arborescence de la Console d'administration du Kaspersky Security Center, sélectionnez le Serveur d'administration auquel sont connectés les appareils mobiles.

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

3. Dans le dossier **Ordinateurs administrés**, choisissez le groupe d'appareils sur lesquels vous envisagez de supprimer l'application.

4. Vous pouvez créer un nouveau sous-groupe d'une des manières suivantes :

   - dans le menu contextuel du dossier **Ordinateurs administrés** de l'arborescence de la console ou dans le menu contextuel du sous-dossier, choisissez l'option **Créer → Groupe**;

   - dans l'espace de travail du dossier, choisissez l'onglet **Groupes** et ouvrez la fenêtre en cliquant sur le lien **Créer un sous-groupe**.

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

6. Lancez la procédure d'ajout dans le groupe d'appareils sur lesquels vous voulez supprimer l'application par l'un des procédés suivants :

   - via le lien **Ajouter des ordinateurs dans le groupe** situé dans la zone de travail de la fenêtre principale de la Console d'administration, sous l'onglet **Groupes** ;

   - via le lien **Ajouter des ordinateurs** situé dans la zone de travail de la fenêtre principale de la Console d'administration, sous l'onglet **Ordinateurs**.

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

7. Dans la zone de travail du groupe choisissez l'onglet **Stratégies** et lancez l'assistant de la création de stratégie en cliquant sur le lien **Créer une stratégie**.

   L'assistant de création de la stratégie va se lancer. Il faut suivre ses indications. Pour la stratégie destinée à la suppression de l'application, modifiez les paramètres aux étapes suivantes :

   - A l'étape **Sélection de l'application pour la création de la stratégie de groupe**, sélectionnez Kaspersky Endpoint Security 10 Service Pack 1 pour les appareils mobiles.

   - A l'étape **Paramètres avancés** du groupe **Administration de l'application** cochez la case **Supprimer Kaspersky Endpoint Security for Android de l'appareil**.

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

   - A l'étape **Création de la stratégie de groupe pour l'application**, dans le bloc des paramètres **Statut de la stratégie**, choisissez l'option **Stratégie active**.

La stratégie créée sera alors active pour le groupe d'administration sélectionné. Suite à la synchronisation des appareils mobiles de ce groupe avec le Serveur d'administration, l'application Kaspersky Endpoint Security for Android peut être supprimée par les utilisateurs. Si l'utilisateur accepte, l'application Kaspersky Endpoint Security for Android sera supprimée de l'appareil mobile. Si l'utilisateur refuse, une demande de confirmation de suppression de Kaspersky Endpoint Security for Android s'affiche sur l'écran de l'appareil mobile à chaque synchronisation avec le serveur d'administration.

Pour supprimer Kaspersky Endpoint Security for Android d'un appareil mobile, procédez comme suit :

1. Dans l'arborescence de la Console d'administration du Kaspersky Security Center, sélectionnez le Serveur d'administration auquel sont connectés les appareils mobiles.

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

3. Dans le dossier **Ordinateurs administrés** sélectionnez le groupe auquel appartient l'appareil sur lequel vous souhaitez supprimer l'application.

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

5. Dans la liste des objets, sélectionnez la stratégie active qui vous permet de gérer les appareils du groupe sélectionné.

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

7. Dans la fenêtre **Propriétés <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Paramètres avancés**.

8. Dans le groupe **Administration de l'application**, assurez-vous que le cadenas a l'aspect suivant  , ce qui signifie que les paramètres de ce groupe peuvent être modifiés dans les paramètres locaux de l'application.

   Le cas échéant, cliquez sur le bouton  pour pouvoir modifier les paramètres du groupe **Administration de l'application** dans les paramètres locaux de l'application.

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

10. Choisissez l'appareil de l'utilisateur dans la liste des appareils administrés.

11. Double-cliquez sur l'appareil sélectionné pour ouvrir la fenêtre de ses propriétés.

12. Dans la fenêtre **Propriétés : <nom de l'appareil>** qui s'ouvre, choisissez le groupe **Applications**.

13. Dans le groupe **Applications**, choisissez **Kaspersky Endpoint Security 10 Service Pack 1 for Mobile**.

14. Double-cliquez sur l'application sélectionnée pour ouvrir la fenêtre de ses propriétés.

15. Dans la section **Paramètres avancés** du groupe **Administration de l'application**, cochez la case **Supprimer Kaspersky Endpoint Security for Android de l'appareil**.

Suite à la synchronisation de cet appareil mobile avec le Serveur d'administration, l'application Kaspersky Endpoint Security for Android demande à l'utilisateur de confirmer la suppression. Si l'utilisateur confirme, l'application Kaspersky Endpoint Security for Android sera supprimée de l'appareil mobile. Si l'utilisateur refuse de confirmer, une demande de confirmation de suppression de Kaspersky Endpoint Security for Android s'affiche sur l'écran de l'appareil mobile à chaque synchronisation avec le serveur d'administration.

SUPPRESSION DE L'APPLICATION MOBILE KASPERSKY SAFE BROWSER FOR IOS

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

- *Pour supprimer l'application Kaspersky Safe Browser for iOS de l'appareil iOS,*

  cliquez sur l'icône de l'application sur l'écran de l'appareil et maintenez-la enfoncée jusqu'à ce qu'elle commence à clignoter, puis appuyez sur la croix.

SUPPRESSION DE L'APPLICATION MOBILE KASPERSKY SAFE BROWSER FOR WINDOWS PHONE

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

- *Pour supprimer l'application Kaspersky Safe Browser for Windows Phone de l'appareil, l'utilisateur doit procéder comme suit :*

  1. Appuyer et maintenir enfoncée l'icône de l'application sur l'écran de l'appareil mobile.

  2. Dans le menu qui s'affiche, sélectionner **Supprimer**.

     Une demande de confirmation apparaît à l'écran.

  3. Appuyer sur **Oui**.

ECHANGE DES INFORMATIONS AVEC KASPERSKY SECURITY NETWORK

Le cloud de Kaspersky Security Network est un service en ligne de Kaspersky Lab qui contient des informations sur la fiabilité des fichiers, des logiciels, des applications mobiles et des ressources Internet. Kaspersky Endpoint Security 10 for Mobile utilise le cloud de Kaspersky Security Network lors de l'utilisation des modules suivants :

- Analyse : les applications mobiles Kaspersky Endpoint Security effectuent une analyse supplémentaire des applications installées avant leur premier lancement. Une analyse est effectuée à la recherche de nouvelles menaces dont les informations n'ont pas encore été ajoutées aux bases antivirus.

- Protection Internet : les applications mobiles Kaspersky Endpoint Security exécutent une analyse supplémentaire des sites Internet avant leur ouverture.

L'Accord de licence détaille la nature des données transmises à Kaspersky Lab lorsque le cloud est utilisé parallèlement aux applications mobiles Kaspersky Endpoint Security sur les appareils des utilisateurs. En acceptant les termes de l'Accord de licence, vous consentez à transmettre les informations suivantes:

- Les sommes de contrôle des fichiers traités (MD5 et SHA256).

- Les noms des paquets d'applications mobiles lancés sur les appareils des utilisateurs en vue de définir les catégories des applications.

- Les données sur les applications à installer afin de vérifier la sécurité des applications. La fonction de transmission automatique des données sur les applications à installer peut être activée ou désactivée au cours du fonctionnement de Kaspersky Endpoint Security ;

- L'adresse du site Internet en cours de consultation par l'utilisateur, en vue de définir la réputation de l'URL ;

- Les paramètres du point d'accès Wi-Fi utilisé ;

- Les données sur les configurations matérielle et logicielle de l'appareil mobile ;

- Les données statistiques sur les menaces détectées.

Les informations transmises dans le Cloud ne contiendront pas de données personnelles ni d'autres informations confidentielles de l'utilisateur.

Les informations obtenues par le service Cloud de Kaspersky Security Network sont protégées par Kaspersky Lab conformément à la législation en vigueur. Kaspersky Lab utilise les informations obtenues uniquement sous forme de statistiques. Les données générales des statistiques sont automatiquement formées à partir des informations d'origine obtenues et ne contiennent pas de données personnelles ou d'autres informations confidentielles. Les informations d'origine obtenues sont enregistrées sous forme chiffrée et sont supprimées au fur et à mesure de leur accumulation (deux fois par an). Les données des statistiques générales sont conservées de manière illimitée.

Pour en savoir plus sur le cloud de Kaspersky Security Network, reportez-vous au site Internet http://support.kaspersky.com/fr/.

CONTACTER LE SUPPORT TECHNIQUE

Cette section contient des informations sur les modes et les conditions d'obtention de l'assistance technique.

DANS CETTE SECTION

A PROPOS DE L'ASSISTANCE TECHNIQUE

Si vous ne trouvez pas la solution à votre problème dans la documentation ou dans les autres sources d'informations relatives à l'application (cf. section « Sources d'information sur l'application » à la page 11), nous vous invitons à contacter le Support Technique de Kaspersky Lab. Les experts du Service de Support Technique répondront à vos questions sur l'installation et l'utilisation de l'application.

L'assistance technique est uniquement proposée aux utilisateurs ayant acheté une licence commerciale pour l'application. Les utilisateurs ayant obtenu une licence d'évaluation n'ont pas accès à l'assistance technique.

Avant de contacter le Support Technique, il est recommandé de prendre connaissance des règles d'octroi de l'assistance technique (http://support.kaspersky.com/fr/support/rules).

Vous pouvez contacter les experts du Service de Support Technique d'une des manières suivantes:

- appeler le Support Technique de Kaspersky Lab par téléphone ;
- envoyer une requête au Support Technique de Kaspersky Lab via le service en ligne Kaspersky CompanyAccount.

SUPPORT TECHNIQUE PAR TELEPHONE

Si le problème est urgent, vous pouvez téléphoner aux experts du Support Technique de Kaspersky Lab (http://support.kaspersky.com/fr/support/contacts).

Avant de contacter le Support Technique, il est conseillé de prendre connaissance des règles d'octroi de l'assistance technique (http://support.kaspersky.com/fr/support/rules). Ces règles vous indiquent les heures auxquelles vous pouvez contacter les experts du Support Technique de Kaspersky Lab par téléphone, ainsi que les données dont ces derniers pourraient avoir besoin afin de vous venir en aide.

Assistance technique via Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) est un service en ligne offert aux entreprises qui utilisent les applications de Kaspersky Lab. Le service en ligne Kaspersky CompanyAccount est conçu pour permettre une interaction entre les utilisateurs et les experts de Kaspersky Lab via des requêtes électroniques. Le service en ligne Kaspersky CompanyAccount permet un suivi du traitement par les experts de Kaspersky Lab des requêtes électroniques et propose un historique de celles-ci.

Vous pouvez inscrire tous les collaborateurs de votre société sous un même compte utilisateur Kaspersky CompanyAccount. Un compte utilisateur vous permet de gérer de manière centralisée les requêtes électroniques envoyées à Kaspersky Lab par les collaborateurs inscrits et d'administrer les privilèges de ces collaborateurs dans Kaspersky CompanyAccount.

Le service en ligne Kaspersky CompanyAccount est disponible dans les langues suivantes :

- anglais ;
- espagnol ;
- italien ;
- allemand ;
- polonais ;
- portugais ;
- russe ;
- français ;
- japonais.

Pour plus d'informations sur Kaspersky CompanyAccount, rendez-vous sur le site Internet du Support Technique (http://support.kaspersky.fr/faq/companyaccount_help).

Demande électronique de signature Certificate Signing Request

Vous pouvez envoyer une demande électronique de signature Certificate Signing Request (demande CSR) au Service de Support Technique.

Pour ce faire, vous devez indiquer dans le formulaire de la demande électronique le fichier de demande CSR http://support.kaspersky.com/fr/9245.

Après le traitement automatique de votre demande électronique, vous recevrez un fichier de demande CSR signé par Kaspersky Lab pour le transférer à Apple.

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

APPENDICE. RESTRICTIONS POUR LES APPAREILS IOS MDM

Kaspersky Mobile Device Management prend en charge l'administration des paramètres des appareils iOS MDM qui peuvent être configurés selon la stratégie de sécurité de l'entreprise.

Restrictions des fonctions :

- **Autoriser l'utilisation de la caméra**
- **Autoriser FaceTime**
- **Autoriser les captures d'écran**
- **Autoriser AirDrop** (uniquement pour les appareils contrôlés)
- **Autoriser iMessage** (uniquement pour les appareils contrôlés)
- **Autoriser la numérotation vocale**
- **Autoriser l'utilisation de Siri**
- **Autoriser le filtre d'expressions vulgaires** (uniquement pour les appareils contrôlés)
- **Autoriser quand l'appareil est verrouillé**
- **Afficher les données de l'utilisateur** (uniquement pour les appareils contrôlés)
- **Autoriser iBooks Store** (uniquement pour les appareils contrôlés)
- **Autoriser l'installation des applications**
- **Autoriser la suppression d'applications** (uniquement pour les appareils contrôlés)
- **Autoriser les Achats intégrés**
- **Demander le mot de passe lors de chaque achat sur iTunes Store**
- **Autoriser la sauvegarde dans iCloud**
- **Autoriser la conservation des documents et des données dans iCloud**
- **Autoriser le Trousseau iCloud**
- **Autoriser l'accès partagé aux photos dans iCloud**
- **Autoriser My Photo Stream**
- **Autoriser la synchronisation automatique en itinérance**
- **Activer le chiffrement des copies de sauvegarde**
- **Limiter le suivi de la publicité**
- **Autoriser l'utilisation des certificats TLS non approuvés**
- **Autoriser la mise à jour automatique des certificats de confiance**
- **Autoriser l'installation des profils de configuration** (uniquement pour les appareils contrôlés)
- **Autoriser la modification des paramètres du compte utilisateur** (uniquement pour les appareils contrôlés)

- **Autoriser la modification des paramètres de la fonction Trouver mes amis** (uniquement pour les appareils contrôlés)
- **Autoriser les connexions tierces**
- **Autoriser la transmission de documents à partir des applications administrées vers des applications non-administrées**
- **Autoriser la transmission de documents à partir d'applications non-administrées vers des applications administrées**
- **Autoriser l'envoi à Apple de données concernant le diagnostic et l'utilisateur**
- **Autoriser Touch ID pour déverrouiller l'appareil**
- **Exiger un mot de passe pour la première connexion AirPlay**
- **Autoriser Passbook à afficher les notifications sur un écran verrouillé**
- **Afficher le Centre de contrôle sur l'écran verrouillé**
- **Afficher le Centre de notification quand l'écran est verrouillé**
- **Afficher "Aujourd'hui" sur l'écran verrouillé**

Restrictions des applications :

- **Autoriser l'utilisation de YouTube**
- **Autoriser l'utilisation de iTunesStore**
- **Autoriser l'utilisation de Game Center**
- **Autoriser l'ajout des amis**
- **Autoriser le mode "Multi-joueurs"**
- **Autoriser l'utilisation de Safari**
- **Activer le remplissage automatique des champs**
- **Activer la notification concernant les sites Internet suspects**
- **Activer JavaScript**
- **Bloquer les fenêtres surgissantes**
- **Appliquer les fichiers cookies**

Restrictions du contenu multimédia :

- **Région**
- **Films**
- **Emissions TV**
- **Applications**
- **Autoriser la lecture de clips vidéo, de podcasts et de contenu iTunes U comportant du contenu explicite**
- **Autoriser le contenu pour adultes dans l'iBook Store**

GLOSSAIRE

A

Administrateur d'appareil

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

Appareil EAS

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

Appareil controle

Appareil iOS dont la configuration est contrôlée dans l'application pour la configuration de groupe des appareils iOS Apple Configurator. L'appareil contrôlé possède l'état supervised dans Apple Configurator. A chaque connexion de l'appareil contrôlé à l'ordinateur, Apple Configurator vérifie la conformité de la configuration de l'appareil aux paramètres définis et les configure, le cas échéant. L'appareil contrôlé ne peut être synchronisé avec une version d'Apple Configurator installée sur un autre ordinateur.

Un appareil contrôlé offre plus de paramètres pour la configuration à l'aide d'une stratégie Kaspersky Mobile Device Management qu'un appareil non contrôlé. Il est, par exemple, possible de configurer sur l'appareil contrôlé un proxy HTTP pour le contrôle du trafic Internet sur l'appareil dans les limites du réseau de l'entreprise. Par défaut, aucun appareil mobile n'est contrôlé.

Appareil iOS MDM

Un appareil mobile fonctionnant avec iOS et administré par le Serveur des appareils mobiles iOS MDM.

Application tierce

Application élaborée par une entreprise tierce (par exemple, client de messagerie pour l'appareil mobile).

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 appareils mobiles iOS MDM peut administrer les appareils iOS.

Conteneur

Une enveloppe spéciale pour applications mobiles qui permet de contrôler les activités de l'application dans le conteneur afin de protéger les données personnelles et d'entreprise stockées dans l'appareil. Le conteneur utilisé sur un appareil iOS est signé par le même certificat que Kaspersky Endpoint Security pour les appareils iOS.

Controle de la conformite

Vérification de la conformité des appareils mobiles des utilisateurs à la stratégie de groupe. Ce contrôle permet également de s'assurer de la conformité des paramètres des appareils mobiles aux exigences à la sécurité corporative.

E

Extension d'une application tierce

Module pour application tierce qui permet de configurer les paramètres de l'application tierce dans la Console d'administration du Kaspersky Security Center.

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 appareils iOS pour chercher, télécharger et installer des applications depuis un serveur Internet.

G

Groupe d'administration

Ensemble d'appareils administrés, notamment des appareils mobiles, réunis suivant leurs fonctionnalités et les applications dont ils sont équipés. Les appareils administrés sont regroupés pour assurer une gestion unifiée. Par exemple, le groupe d'administration peut regrouper les appareils 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 appareils qui font partie d'un groupe.

K

Kaspersky Security Network (KSN)

Infrastructure des services en ligne et des services 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 inconnues, augmente l'efficacité de fonctionnement de certains modules de la protection et réduit la possibilité de faux positifs.

P

Paquet autonome

Fichier d'installation de l'application mobile Kaspersky Endpoint Security for Android, contenant les paramètres de connexion de l'application au Serveur d'administration. Ce fichier est créé depuis le paquet d'installation pour cette application et fait partie intégrante du 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 spéciaux faisant partie de la distribution de l'application. Il contient les paramètres nécessaires à l'installation de l'application et assure le fonctionnement de l'application après son installation. 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 appareils des utilisateurs.

PROFIL IOS MDM

Profil comportant tout un ensemble de paramètres pour la connexion des appareils 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 appareils mobiles iOS MDM et d'obtenir un diagnostic étendu sur les appareils mobiles. Vous devez envoyer le lien vers le profil iOS MDM à l'utilisateur pour permettre au serveur de gestion des appareils 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 appareils mobiles iOS. Le profil provisioning comporte des informations sur la licence et est rattaché à une application en particulier.

R

REQUETE 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 APPAREILS MOBILES EXCHANGE ACTIVESYNC

Module de Kaspersky Endpoint Security installé sur un poste client qui permet de connecter les appareils mobiles Exchange ActiveSync au Serveur d'administration.

SERVEUR DES APPAREILS MOBILES IOS MDM

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

STRATEGIE

Ensemble de paramètres pour le fonctionnement de l'application et des applications mobiles Kaspersky Endpoint Security sur tous les appareils du groupe d'administration ou sur des appareils 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.

SYNCHRONISATION

Processus de mise en place de la connexion entre l'appareil mobile et le système d'administration à distance. Il permet également le transfert des données entre ces deux entités. Lors de la synchronisation, l'appareil reçoit les paramètres de Kaspersky Endpoint Security définis par l'administrateur. L'appareil envoie au système d'administration à distance les rapports sur le fonctionnement des modules de l'application mobile.

T

TACHE DE GROUPE

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

U

UTILITAIRE KASPERSKY SMS BROADCASTING

Utilitaire installé sur l'appareil iOS de l'administrateur afin de pouvoir envoyer des SMS aux appareils Android des utilisateurs.

KASPERSKY LAB ZAO

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

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

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

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

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

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

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

TECHNOLOGIES. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est donc pas un hasard si le moteur logiciel de Kaspersky Anti-Virus est intégré aux logiciels de plusieurs autres éditeurs : citons notamment SafeNet (E-U), Alt-N Technologies (E-U), Blue Coat Systems (E-U), Check Point Software Technologies (Israël), Clearswift (R-U), CommuniGate Systems (E-U), Openwave Messaging (Irlande), D-Link (Taïwan), M86 Security (E-U), GFI Software (Malte), IBM (E-U), Juniper Networks (E-U), LANDesk (E-U), Microsoft (E-U), Netasq+Arkoon (France), NETGEAR (E-U), Parallels (E-U), SonicWALL (E-U), WatchGuard Technologies (E-U), ZyXEL Communications (Taïwan). 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 2010, Kaspersky Antivirus a obtenu plusieurs hautes distinctions Advanced+ à l'issue de tests réalisés par le célèbre laboratoire antivirus autrichien AV-Comparatives. Mais la récompense la plus importante de Kaspersky Lab, c'est la fidélité de ses utilisateurs à travers le monde. Les produits et les technologies de la société protègent plus de 300 millions d'utilisateurs. Elle compte également plus de 200 000 entreprises parmi ses clients.

Site de Kaspersky Lab :	http://www.kaspersky.com/fr
Encyclopédie des virus :	http://www.securelist.com/fr/
Laboratoire d'étude des virus :	newvirus@kaspersky.com (uniquement pour l'envoi d'objets suspects sous forme d'archive)
Forum de Kaspersky Lab :	http://forum.kaspersky.fr

INFORMATIONS SUR LE CODE TIERS

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

Pour les appareils fonctionnant avec Android, les informations du fichier legal_notices.txt sont affichées dans la fenêtre **Avancé** dans la section **Info logiciel**.

AVERTISSEMENT RELATIF AUX MARQUES

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

Apple, iPhone, Mac OS sont des marques déposées d'Apple Inc.

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

Android et Google 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.

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

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

La marque déposée Symbian appartient à Symbian Foundation Ltd.

INDEX

A

C

F

G

K

M

P

R

S

Z