KASPERSKY lab

Kaspersky Security 10 for Mobile

Manuel de l'administrateur

Version de l'application : 10 Service Pack 1 Maintenance Release 3

Cher utilisateur

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

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

Date de rédaction du document : 17/12/2015

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

Contenu

A propos de ce document

Le manuel de l'administrateur de Kaspersky Security for Mobile est destiné aux experts assurant l'installation et l'administration des applications mobiles Kaspersky Endpoint Security et Kaspersky Safe Browser, ainsi qu'aux experts assurant l'assistance technique auprès des entreprises utilisant Kaspersky Security for Mobile.

Ce manuel fournit des informations relatives à la configuration et à l'utilisation de la suite logicielle Kaspersky Security for Mobile.

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

Dans cette section

Dans ce document

Ce document contient les sections suivantes :

Sources d'informations sur l'application (cf. page 12)

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

Kaspersky Security for Mobile (cf. page 16)

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

Interface de l'application (à la page 26)

Cette section présente les principaux éléments de l'interface de l'application.

Licence de l'application (cf page 27)

Cette section présente les principales notions associées à la licence de Kaspersky Security for Mobile.

Lancement et arrêt de l'application (à la page 33)

Cette section explique comment lancer et arrêter l'application.

Stratégies de groupe pour l'administration des périphériques mobiles (cf. page 37)

Cette section contient des informations sur les stratégies à l'aide desquelles l'administrateur peut gérer les périphériques mobiles des utilisateurs de manière centralisée.

Administration des périphériques Android cf. page 40)

Cette section contient les instructions nécessaires à la configuration à distance des périphériques Android™ dotés de l'application Kaspersky Endpoint Security for Android.

Administration des périphériques iOS (cf. page 81)

Cette section contient les instructions nécessaires à la configuration à distance des périphériques iOS dotés de l'application Kaspersky Safe Browser for iOS.

Administration des périphériques Windows Phone (cf. page 86)

Cette section contient les instructions nécessaires à la configuration à distance des périphériques Windows Phone® dotés de l'application Kaspersky Safe Browser for Windows Phone.

Administration des périphériques EAS (cf. page 91)

Cette section contient les instructions sur la configuration des périphériques connectés au Serveur de périphériques mobiles Exchange ActiveSync®.

Administration des appareils MDM iOS (cf. page 98)

Cette section contient les instructions sur la configuration à distance des appareils MDM iOS connectés au serveur d'appareils mobiles MDM iOS.

Participation au Kaspersky Security Network (à la page 145)

Cette section reprend les informations sur l'interaction de l'application Kaspersky Endpoint Security avec Kaspersky Security Network.

Glossaire (cf. page 174)

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

Kaspersky Lab AO (cf. page 180)

Cette section contient des informations sur Kaspersky Lab AO.

Information sur le code tiers (cf. page 182)

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

Avis de marques déposées (cf. page 183)

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

Index (cf. page 196)

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 de texte	Description de la convention
Exemple :	Les exemples sont présentés sur un fond bleu sous le titre "Exemple".
La *mise à jour*, c'est... L'événement *Bases périmées* survient.	Les éléments de texte suivants sont en italique : • nouveaux termes; • noms des statuts et des événements de l'application.
Appuyez sur la touche **ENTER**. Appuyez en même temps sur les touches **ALT**+**F4**.	Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules. Des noms de touche unis par le caractère + (plus) représentent une combinaison de touches. Ces touches doivent être enfoncées simultanément.
Cliquez sur le bouton **Activer**.	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu et les boutons, sont en caractères mi-gras.
► *Pour planifier une tâche, procédez comme suit :*	Les phrases de saisie des instructions sont en italique et présentent l'icône "flèche".
Dans la ligne de commande, saisissez le texte `help` Le message suivant s'affiche: `Indiquez la date au format JJ:MM:AA.`	Les types de texte suivants apparaissent dans un style spécial : • texte de la ligne de commande; • texte des messages affichés sur l'écran par l'application; • données à saisir à l'aide du clavier.
<Nom d'utilisateur>	Les variables sont écrites entre chevrons. A la place de la variable, il convient d'indiquer la valeur correspondante en enlevant les chevrons.

Sources d'informations sur l'application

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

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

Dans cette section

Sources d'informations pour la recherche autonome

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

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

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

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

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

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

Page Kaspersky Security for Mobile dans la Base de connaissances

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

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

Les articles de la Base de connaissances peuvent répondre à des questions en rapport non seulement avec Kaspersky Security for Mobile, mais également avec d'autres applications de Kaspersky Lab. Les articles de la base de connaissances peuvent également contenir des informations du Support technique.

Aide électronique

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

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

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

Documentation

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

Discussion sur les applications de Kaspersky Lab sur le forum

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

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

Kaspersky Security for Mobile

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

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

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

- Plug-in d'administration de Kaspersky Endpoint Security 10 Service Pack 1, Maintenance Release 3 (plus loin "plug-in d'administration de Kaspersky Endpoint Security").

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

- Plug-in d'administration de Kaspersky Mobile Device Management 10 Service Pack 1, Maintenance Release 3 (plus loin "plug-in d'administration de Kaspersky Mobile Device Management").

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

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

Dans cette section

A propos de Kaspersky Endpoint Security for Android

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

Kaspersky Endpoint Security inclut les modules suivants :

- Anti-Virus. Ce module permet de détecter et de neutraliser les menaces sur l'appareil mobile à l'aide des bases antivirus de l'app et des services en nuage du Kaspersky Security Network. L'Anti-Virus présente les composants suivants :
    - Protection. La protection permet de découvrir les menaces dans les fichiers ouverts, d'analyser les nouvelles applications et de prévenir l'infection du périphérique en temps réel.
    - Analyse. L'analyse est lancée sur demande pour tout le système de fichiers, la mémoire vive ou un dossier. L'analyse complète permet de rechercher la présence éventuelle d'objets malveillants dans tout le système de fichiers du périphérique tandis que l'analyse personnalisée porte sur un dossier en particulier. L'analyse complète et l'analyse

personnalisée détectent les menaces dans les fichiers installés et non ouverts, ainsi que les menaces dans les fichiers qui sont ouverts à ce moment-là. L'analyse de la mémoire permet de détecter les menaces uniquement dans les fichiers ouverts à ce moment-là.

  - Mise à jour. La mise à jour permet de télécharger les nouvelles bases antivirus de l'app.

- Antivol. Ce composant protège les informations du périphérique contre tout accès non autorisé en cas de perte ou de vol du périphérique. Le module permet de bloquer l'appareil, de le localiser ou de supprimer à distance les données qui s'y trouvent à l'aide de commandes.

- Filtre des appels et SMS. En fonction du mode de fonctionnement Filtre des appels et SMS sélectionné, celui-ci permet de bloquer les appels et SMS non sollicités. Le filtrage des SMS et des appels entrants s'effectue à l'aide des listes de contacts autorisés et interdits. Filtre des appels et SMS permet de bloquer ou de transmettre les SMS et les appels entrants provenant des contacts interdits ou autorisés. Selon le mode sélectionné, Filtre des appels et SMS permet également de transmettre les appels et SMS entrants provenant de tous les numéros du répertoire du périphérique (Contacts) ou de bloquer les appels et SMS entrants de tous les numéros comportant des lettres.

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

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

- Quarantaine. Place dans un stockage spécial et isolé les fichiers qui ont été détectés lors de l'analyse du périphérique ou au cours du fonctionnement normal de la protection. La quarantaine compacte les fichiers avant leur isolement afin de protéger votre appareil. Ce module " Quarantaine " permet de supprimer ou de restaurer les fichiers placés en quarantaine.
- Rapports. Permet de recevoir des informations sur le fonctionnement de l'Anti-Virus, du Filtre des appels et SMS et de la Protection Internet sur le périphérique mobile de l'utilisateur. Ce module regroupe les rapports dès leur création. Le rapport peut contenir jusqu'à 200 entrées sur les événements. Lorsque le nombre d'entrées dépasse 200, le module remplace les entrées les plus anciennes par les entrées les plus récentes.

A propos de Kaspersky Safe Browser for iOS

L'application mobile Kaspersky Safe Browser for iOS (ci-après "Kaspersky Safe Browser") est un navigateur sécurisé.

Kaspersky Safe Browser inclut les modules suivants :

- Protection Internet. Permet de bloquer les sites Internet malveillants dont le but est de diffuser un code nuisible. La Protection Internet bloque également les sites Internet de phishing qui servent à voler des données confidentielles des utilisateurs (mots de passe des banques en lignes ou des systèmes de paiement, par exemple) pour obtenir un accès à leurs comptes bancaires. La Protection Internet analyse les sites Internet avant leur ouverture à l'aide du service en nuage du Kaspersky Security Network. Selon les résultats de l'analyse, la Protection Internet autorise le chargement des sites Internet identifiés comme fiables et bloque les sites Internet identifiés comme malveillants. La Protection Internet prend également en charge le filtrage des sites Internet par catégorie, selon les catégories définies dans le service dans le nuage du Kaspersky Security Network. Cela permet à l'administrateur de limiter l'accès des utilisateurs à certaines catégories (les pages Internet des catégories " Jeux de hasard, loteries, tirages au sort " ou " Médias de communication Internet ", par exemple).
- Antivol. Permet de localiser l'appareil mobile à l'aide d'une commande en cas de perte ou de vol.
- Synchronisation. Assure la connexion de l'appareil mobile au Serveur d'administration. La synchronisation offre la possibilité de configurer à distance les paramètres de l'application, et de l'appareil mobile à l'aide de stratégies de groupe définies dans la Console d'administration Kaspersky Security Center.

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

A propos de Kaspersky Safe Browser for Windows Phone

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

Kaspersky Safe Browser inclut les modules suivants :

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

- Antivol. Permet de localiser l'appareil mobile à l'aide d'une commande en cas de perte ou de vol.

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

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

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

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

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

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

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

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

Nouveautés

Kaspersky Security for Mobile propose les nouveautés et les mises à jour suivantes :

- Prise en charge des périphériques mobiles tournant sous le système d'exploitation Android 6.0 Marshmallow.
- Prise en charge de l'administration de l'appareil à l'aide de Android for Work.
- Nouvelles catégories d'application pour le Contrôle des applications.
- Lancement de l'analyse antivirus sur le périphérique mobile après la mise à jour des bases antivirus.
- Déblocage du périphérique si l'utilisateur du périphérique mobile a oublié le mot de passe de déblocage de l'écran.
- Refonte des éléments graphique des applications mobiles Kaspersky Endpoint Security for Android, Kaspersky Safe Browser for iOS et Kaspersky Safe Browser for Windows Phone.
- Mise à jour de la liste de données qui peuvent être supprimées après la réception de la commande de suppression des données de l'entreprise.

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 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 for Android ;

- `kmlisten.exe` : utilitaire de distribution du paquet d'installation sur un périphérique mobile via une station de travail ;
- `kmlisten.ini` – fichier de configuration contenant les paramètres pour l'utilitaire de distribution du paquet d'installation ;
- `kmlisten.kpd` – fichier contenant la description de l'application.

- `klcfginst_fr.exe` — fichier d'installation du plug-in d'administration de Kaspersky Endpoint Security 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 for Android.
- `KSM_10_3_xx_ru.zip` : fichier d'installation de l'application mobile Kaspersky Safe Browser for iOS.
- `sms_utility_10.1.25fr.apk` : utilitaire Kaspersky SMS Broadcasting.
- `licutil.exe` : utilitaire d'activation de l'application mobile Kaspersky Endpoint Security sans utilisation de Kaspersky Security Center.
- paquet de documentation:
  - manuel de l'administrateur de Kaspersky Security for Mobile ;
  - manuel d'implantation de Kaspersky Security for Mobile ;
  - aide contextuelle du plug-in d'administration de Kaspersky Endpoint Security ;
  - aide contextuelle du plug-in d'administration de Kaspersky Mobile Device Management ;
  - aide contextuelle de l'application mobile Kaspersky Endpoint Security for Android.

Configurations logicielles et matérielles

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- type d'appareil : iPhone 4 ou modèle plus récent, iPad 2 ou modèle plus récent ;
- 35 Mo d'espace libre dans la mémoire principale de l'appareil ;

- système d'exploitation iOS 7, iOS 8 et iOS 9 ;
- connexion à Internet ;
- accès à la géolocalisation et à l'appareil photo de l'appareil.

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

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

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

Interface de l'application

Kaspersky Security for Mobile est une suite logiciel qui contient des plug-ins d'administration et un paquet d'applications mobiles. Les actions qui impliquent les plug-ins d'administration sont réalisées dans l'interface de la Console d'administration Kaspersky Security Center. Pour en savoir plus sur l'interface de Kaspersky Security Center, consultez la documentation de Kaspersky Security Center. Les actions qui impliquent les applications mobiles sont réalisées dans les interfaces respectives des applications pour les systèmes d'exploitation Android, iOS et Windows Phone. Pour en savoir plus sur les interfaces des applications mobiles, consultez la documentation de ces applications.

Licence de l'application

Cette section présente les principales notions associées à la licence de Kaspersky Security for Mobile.

Dans cette section

A propos du Contrat de licence

Le Contrat de licence utilisateur final est un accord juridique conclu entre vous et AO Kaspersky Lab qui stipule les conditions dans lesquelles vous pouvez utiliser Kaspersky Security for Mobile.

Lisez attentivement les conditions du Contrat de licence avant de commencer à utiliser Kaspersky Security for Mobile.

Vous pouvez prendre connaissance des conditions du Contrat de licence de l'une des manières suivantes :

- Pendant l'installation des modules de Kaspersky Security for Mobile.
- En lisant le document license.txt. Ce document figure dans le paquet d'installation de Kaspersky Security for Mobile.

Vous acceptez les conditions du Contrat de Licence Utilisateur Final, en confirmant votre accord avec le texte du contrat de licence lors de l'installation des modules de Kaspersky Security for Mobile. Si vous n'acceptez pas les dispositions du Contrat de Licence Utilisateur Final, vous devez interrompre l'installation des modules de Kaspersky Security for Mobile et vous ne pouvez pas les utiliser.

A propos de la licence

La *licence* est un droit d'utilisation limité dans le temps de la suite Kaspersky Security for Mobile qui est conféré sur la base du Contrat de Licence Utilisateur Final.

La licence vous donne droit aux types de service suivants :

- utilisation des applications sur les périphériques mobiles conformément aux dispositions du Contrat de Licence Utilisateur Final ;
- obtention du Support Technique.

Le volume de services offert et la durée d'utilisation des applications mobiles dépendent du type de licence utilisée pour activer l'application.

Les types suivants de licences sont prévus :

- *Evaluation* : une licence gratuite conçue pour découvrir Kaspersky Security for Mobile.

  La licence d'évaluation présente une courte durée de validité. Une fois que la licence d'évaluation de l'application mobile Kaspersky Endpoint Security arrive à échéance, toutes les fonctions de l'application sont désactivées. Pour continuer à utiliser Kaspersky Endpoint Security, vous devez acheter une licence commerciale.

- *Commerciale* : licence payante octroyée lors de l'achat de Kaspersky Security for Mobile.

  A l'expiration de la licence commerciale, l'application mobile continue à fonctionner, mais ses fonctionnalités sont limitées (par exemple, la mise à jour des bases de données de Kaspersky Endpoint Security n'est pas disponible). Pour pouvoir continuer à bénéficier de toutes les fonctionnalités du Kaspersky Endpoint Security, vous devez renouveler la licence commerciale.

Il est conseillé de renouveler la licence ou d'acheter une nouvelle licence avant sa date d'expiration afin de garantir la protection maximale de l'ordinateur contre toutes les menaces.

A propos de l'abonnement

L'abonnement à Kaspersky Security for Mobile constitue une commande pour l'utilisation de l'application mobile selon des paramètres sélectionnés (date d'expiration, nombre de périphériques mobiles protégés). Il est possible d'enregistrer un abonnement à Kaspersky Security for Mobile auprès d'un prestataire de services (par exemple, auprès d'un fournisseur Internet). L'abonnement peut être renouvelé manuellement ou automatiquement. Il peut également être refusé. L'administration de l'abonnement est accessible sur le site Internet du fournisseur de services.

L'abonnement peut être limité (par exemple, pour un an) ou illimité (sans date d'expiration). Pour prolonger l'action de Kaspersky Security for Mobile après la date d'expiration d'un abonnement limité, il est nécessaire de renouveler ce dernier. L'abonnement illimité est renouvelé automatiquement si le prépaiement au service client est effectué en temps et en heure.

Si l'abonnement est limité, une période de grâce de renouvellement vous est proposée après sa date d'expiration. Pendant cette période, l'application continue à fonctionner. C'est le fournisseur du service qui détermine l'existence et la durée de cette période de grâce.

Pour utiliser Kaspersky Security for Mobile sur abonnement, il est nécessaire d'entrer le code d'activation fourni par le prestataire de services. Quand le code d'activation a été appliqué, la clé correspondante à la licence d'utilisation de l'application selon un abonnement est installée.

> Le choix des possibilités de gestion de l'abonnement diffère selon les prestataires de services. Le prestataire de services peut ne pas proposer de période de grâce où l'application continue à fonctionner après la date d'expiration.

Les codes d'activation achetés par abonnement ne peuvent pas être utilisés pour l'activation de versions antérieures de Kaspersky Endpoint Security.

A propos de la clé

Une *clé* est une séquence de bits qui vous permet d'activer puis d'utiliser la suite Kaspersky Security conformément aux conditions du Contrat de licence. Elle est créée par les experts de Kaspersky Lab.

Vous pouvez ajouter une clé à l'application mobile à l'aide d'un fichier de clé ou un code d'activation :

- Si votre organisation a déployé la suite Kaspersky Security Center, il faut appliquer le fichier clé et le diffuser aux applications mobiles. La clé s'affiche dans l'interface de Kaspersky Security Center et dans l'interface de l'application mobile sous la forme d'une séquence alphanumérique unique.
- Si votre organisation n'utilise pas la suite Kaspersky Security Center, il faudra ajouter le code d'activation à la distribution de l'application mobile. Une fois ajoutée, elle s'affiche dans l'interface de l'application mobile sous la forme d'une séquence alphanumérique unique.

Une fois que les clés ont été ajoutées, vous pouvez les remplacer par d'autres.

Une clé peut être bloquée par Kaspersky Lab en cas de non-respect des conditions du Contrat de licence. Si une clé a été bloquée, vous devrez ajouter une autre clé pour utiliser les applications mobiles.

A propos du code d'activation

Le *code d'activation* est une suite unique de 20 caractères alphanumériques. Vous le saisissez pour ajouter la clé d'activation de Kaspersky Endpoint Security for Android. Vous recevez le code d'activation à l'adresse électronique que vous avez indiquée après l'achat de Kaspersky Security for Mobile ou après la commande d'une version d'évaluation de Kaspersky Security for Mobile.

Pour activer l'application mobile à l'aide de ce code, il faut un accès Internet pour se connecter aux serveurs d'activation de Kaspersky Lab.

En cas de perte du code d'activation après l'activation de l'application mobile, vous pouvez le restaurer. Le code d'activation peut vous être utile pour vous inscrire sur Kaspersky CompanyAccount, par exemple. Pour récupérer le code d'activation, il faut contacter le Support Technique de Kaspersky Lab.

A propos du fichier clé

Le *fichier clé* est un fichier doté d'une extension key qui vous est fourni par Kaspersky Lab. Le fichier clé permet d'ajouter une clé pour activer les applications mobiles.

Vous recevez le fichier clé à l'adresse email que vous avez indiquée après l'achat de la suite Kaspersky Security for Mobile ou après la commande d'une version d'évaluation de Kaspersky Security for Mobile.

Pour activer l'application à l'aide du fichier clé, il n'est pas nécessaire de se connecter aux serveurs d'activation de Kaspersky Lab.

En cas de suppression accidentelle du fichier clé, vous pouvez le restaurer. Vous aurez besoin du fichier clé pour ouvrir un Kaspersky CompanyAccount par exemple.

Pour restaurer un fichier clé, réalisez une des actions suivantes :

- Contacter le Support Technique de Kaspersky Lab ;
- Obtenir le fichier clé sur le site Internet de Kaspersky Lab (https://activation.kaspersky.com/fr/) à partir du code d'activation que vous possédez.

A propos de l'approvisionnement des données

En acceptant les conditions du Contrat de licence, vous acceptez de transférer de manière automatique les informations relatives aux sommes de contrôle des fichiers traités (MD5) ainsi que les informations requises pour définir la réputation des URL. Les informations obtenues ne contiennent aucune donnée personnelle ou autre donnée confidentielle. Kaspersky Lab protège les informations obtenues conformément aux dispositions juridiques en vigueur.

Dans le but de produit des documents marketing efficace et à fin d'améliorer le fonctionnement des applications de Kaspersky Lab, vous acceptez de fournir automatiquement au service Google Analytics™ les informations relatives aux éléments suivants :

- sur l'application, y compris la version de l'application, l'identifiant de l'application et l'identifiant de l'application dans le service Google Analytics ;
- sur l'identifiant de l'installation de l'application sur l'appareil et sur le mode d'installation utilisé ;
- région et version linguistique ;

- résolution de l'écran du périphérique ;
- navigation entre les fenêtres de l'application ;
- protocole d'envoi des données au service Google Analytics, sa version et l'identifiant de la méthode d'envoi des données ;
- licence de l'application ;
- intervalles de mise à jour des bases antivirus et synchronisation avec le Serveur d'administration Kaspersky Security Center.

Les données sont transmises à Google Analytics via un canal sécurisé. L'accès aux informations et la protection de celles-ci sont réglementés par les conditions d'utilisation du service Google Analytics.

Pour obtenir de plus amples informations sur le transfert, le traitement, le stockage et la destruction des informations recueillies lors de l'utilisation de Kaspersky Security for Mobile, lisez le texte du Contrat de Licence Utilisateur Final et la page du site Internet de Kaspersky Lab http://www.kaspersky.fr/privacy.

Lancement et arrêt de l'application

Kaspersky Security Center lance et arrête automatiquement les plug-ins d'administration de Kaspersky Endpoint Security et Kaspersky Mobile Device Management. Pour en savoir plus sur le lancement et l'arrêt de Kaspersky Security Center, consultez le *Manuel de l'administrateur du Kaspersky Security Center*.

Kaspersky Endpoint Security for Android se lance au démarrage du système d'exploitation et protège le périphérique mobile de l'utilisateur tout au long de la session de fonctionnement. L'utilisateur peut arrêter l'application en désactivant tous les composants de Kaspersky Endpoint Security. Vous pouvez configurer l'accès de l'utilisateur à l'administration des composants de l'application à l'aide de stratégies de groupe.

Kaspersky Safe Browser démarre lorsque vous cliquez sur l'icône de l'application. Pour quitter l'application, suivez la méthode traditionnelle pour la platerforme en question.

Stratégies de groupe pour l'administration des périphériques mobiles

Cette section fournit des informations sur la stratégie de groupe d'administration des périphériques mobiles, sur la création et la suppression de cette stratégie ainsi que sur la restriction des autorisations de configuration des stratégies de groupe pour les utilisateurs de la Console d'administration de Kaspersky Security Center.

Dans cette section

A propos de la stratégie de groupe

Une *stratégie de groupe* est un ensemble unique de paramètres pour l'administration des périphériques 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 de stratégie.

Une stratégie permet de configurer les paramètres de périphériques individuels ou de groupes. 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 périphérique en particulier, cette configuration s'effectue dans la fenêtre des paramètres locaux de l'application. Les paramètres d'administration définis spécifiquement pour un périphérique 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 périphériques mobiles lors de la synchronisation et sont considérées comme des paramètres actifs. 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.

Pour maintenir la sécurité d'entreprise des périphériques mobiles des utilisateurs à jour, vous pouvez contrôler leur conformité à la stratégie de groupe d'administration (cf. section "Contrôle de la conformité des périphérique mobiles à la stratégie de groupe", à la page 63).

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*.

Création d'une stratégie de groupe

Cette section décrit la création de stratégies de groupe pour les périphériques dotés des applications mobiles Kaspersky Endpoint Security ou Kaspersky Safe Browser et de stratégies pour les périphériques EAS et MDM iOS.

Les stratégies créées pour le groupe d'administration sont affichées dans l'espace de travail du groupe dans la console d'administration Kaspersky Security Center 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 chaque 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 d'administration de périphériques mobiles, procédez comme suit :*

1. Dans l'arborescence de la Console, sélectionnez le groupe d'administration pour lequel vous souhaitez créer une stratégie.
2. Dans l'espace 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.

Dans cette section

Etape 1. Définition du nom de la stratégie 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. Sélection de l'application pour la création de la stratégie 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 for Mobile Service Pack 1 Maintenance Release 3**, pour les appareils utilisant l'application mobile Kaspersky Endpoint Security ou Kaspersky Safe Browser.
- **Kaspersky Mobile Device Management 10 Service Pack 1 Maintenance Release 3**, pour les périphériques EAS et iOS MDM.

Il es possible de créer une stratégie pour des périphériques mobiles si le poste de travail de l'administrateur est doté du plug-in d'administration de Kaspersky Endpoint Security et du plug-in d'administration de Kaspersky Mobile Device Management. Si les plug-ins ne sont pas installés, le nom de l'application correspondante ne figure pas dans la liste des applications. Pour en savoir plus sur l'installation des plug-ins d'administration de Kaspersky Endpoint Security et Kaspersky Mobile Device Management, consultez le Manuel d'implantation de Kaspersky Security for Mobile.

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

Etape 3. Sélection de l'état de la stratégie

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 le périphérique dès la synchronisation suivante du périphérique 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.

Suppression d'une stratégie de groupe

► *Pour supprimer une stratégie de groupe, procédez comme suit :*

1. Dans l'arborescence, 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. Dans le menu contextuel de la stratégie, choisissez l'option **Supprimer**.

La stratégie de groupe sera ainsi supprimée. les périphériques 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.

Restriction des autorisations de configuration des stratégies de groupe

Les administrateurs du Kaspersky Security Center peuvent définir les autorisations d'accès des utilisateurs de la Console d'administration aux différentes fonctions de la suite logicielle Kaspersky Security for Mobile selon leurs fonctions 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 configurer les autorisations des utilisateurs par zone d'activité. Les informations relatives aux correspondances entre les zones d'activité et les onglets des stratégies sont reprises dans l'Appendice 1 (cf. section "Appendice 1. Autorisations de configuration des stratégies de groupe" à la page 150).

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.*

Administration des périphériques Android

Pour pouvoir administrer des périphériques Android, l'application Kaspersky Endpoint Security for Android doit être installée sur le périphérique mobile. Pour en savoir plus sur l'installation de Kaspersky Endpoint Security for Android, consultez le *Manuel d'implantation de Kaspersky Security for Mobile*.

L'administration des périphériques Android s'opère à l'aide de stratégies de groupe. Les stratégies de groupe permettent de configurer les paramètres du périphérique mobile ainsi que les paramètres de l'application Kaspersky Endpoint Security for Android installé sur celui-ci.

► *Pour configurer la stratégie de groupe pour l'administration des périphériques Android, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration auquel appartiennent les périphériques dont vous souhaitez configurer les paramètres.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Sélectionnez la stratégie pour Kaspersky Endpoint Security 10 for Mobile Service Pack 1 Maintenance Release 3 dan,s la liste des stratégies.

   Si nécessaire, vous pouvez créer une nouvelle 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 35).
4. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.

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

Dans cette section

Configuration des paramètres 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.

Par défaut, les périphériques 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 périphériques mobiles avec le Serveur d'administration, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).

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

3. Sélectionnez la fréquence de lancement de la synchronisation dans la liste déroulante **Lancer la synchronisation**.

   > Il est impossible d'interdire la synchronisation des périphériques Android en itinérance. La sélection ou non de la case **Désactiver la synchronisation en itinérance** n'influence pas le fonctionnement du périphérique mobile.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Configuration de la protection antivirus

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

Dans cette section

Configuration de l'analyse du périphérique

Afin de réaliser l'analyse antivirus et de rechercher la présence éventuelle d'autres programmes malveillants, il convient de configurer l'analyse du périphérique mobile de l'utilisateur.

Par défaut, l'application Kaspersky Endpoint Security analyse uniquement les fichiers exécutables enregistrés sur le périphérique 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 du périphérique mobile, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).

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

3. Configurez les paramètres d'analyse dans le groupe **Paramètres d'analyse du périphérique** :

   - Pour que l'application analyse tous les fichiers enregistrés sur le périphérique et sur la carte mémoire, décochez la case **Analyser seulement les fichiers exécutables**.

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

   - Pour que l'application tente de répare les objets malveillants découverts, 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 du périphérique. Pour ce faire, appuyez sur **Programmation** et dans la fenêtre **Programmation** qui s'ouvre, définissez la fréquence et l'heure d'exécution de l'analyse complète.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Configuration de la protection du système de fichiers

Afin de pouvoir détecter les menaces à temps, il faut configurer la protection du système de fichiers du périphérique mobile.

La protection est activée par défaut. les périphériques mobiles 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 applications qui pourraient être exploitées par des individus malintentionnés pour nuire au périphérique 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 du périphérique mobile, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).

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 du périphérique mobile :

   - Pour activer la protection en temps réel contre les menaces sur le périphérique mobile de l'utilisateur, cochez la case **Activer la protection**.

     Kaspersky Endpoint Security analysera uniquement les nouvelles applications.

   - Pour activer le mode de protection étendu du périphérique mobile de l'utilisateur contre les menaces, cochez la case **Mode de protection étendu**.

     Kaspersky Endpoint Security for Android analysera tous les fichiers que l'utilisateur ouvre, modifie, transfère, copie, lance et sauvegarde sur le périphérique, ainsi que les applications mobiles juste après leur installation.

   - Pour activer l'analyse complémentaire des nouvelles applications avant leur premier lancement sur le périphérique de l'utilisateur à l'aide du service cloud Kaspersky Security Network, cochez la case **Activer la protection cloud**.

- Pour bloquer les logiciels publicitaires et les applications pouvant être exploitées par des individus malintentionnés pour nuire au périphérique ou aux données de l'utilisateur, cochez la case **Publicité, numéroteur et autres**.

4. Pour 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 le bouton **Appliquer** pour enregistrer les modifications apportées.

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Configuration de la mise à jour

Pour garantir l'actualité de la protection du périphérique mobile, il faut configurer les paramètres de mise à jour des bases antivirus.

La mise à jour des bases antivirus est désactivée par défaut lorsque le périphérique est en itinérance. La mise à jour planifiée des bases antivirus n'a pas lieu.

► *Pour configurer les paramètres de mise à jour des bases antivirus de l'application, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Mise à jour**.
3. Pour que Kaspersky Endpoint Security télécharge la mise à jour des bases de données selon une programmation quand le périphérique est en itinérance cochez la case **Autoriser la mise à jour en itinérance** dans le groupe **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.

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 **Mise à jour programmée**, configurez le lancement automatique de la mise à jour des bases antivirus sur le périphérique de l'utilisateur. Pour ce faire, appuyez sur **Programmation** et dans la fenêtre **Programmation** qui s'ouvre, définissez la fréquence et l'heure d'exécution de la mise à jour.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Configuration de la protection contre l'accès non autorisé

Cette section contient des informations sur la configuration des paramètres de la protection du périphérique mobile contre l'accès non autorisé en cas de perte ou de vol.

Dans cette section

Configuration de l'Antivol

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

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 des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Antivol**.
3. Si vous souhaitez que l'application envoie, en cas de remplacement de la carte SIM, le nouveau numéro de téléphone du périphérique à l'adresse électronique ou au numéro de téléphone indiqué :
   a. Cochez la case **Activer la surveillance SIM**.
   b. Dans le champ **Envoyer le SMS vers un numéro de téléphone**, indiquez le numéro de téléphone du destinataire du message.
4. Si vous souhaitez que l'application bloque le périphérique en cas de remplacement de la carte SIM ou de l'allumage du périphérique sans carte SIM :
   a. Cochez la case **Verrouiller l'appareil en cas de remplacement de la carte SIM**.
   b. Dans le champ **Texte en cas de verrouillage**, indiquez le texte du message qui sera affiché sur l'écran du périphérique mobile verrouillé.
5. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Envoi des commandes de l'Antivol au périphérique mobile

Afin de protéger les données stockées sur le périphérique de l'utilisateur en cas de perte ou de vol du périphérique, il faut configurer l'envoi des commandes de l'Antivol au périphérique.

Par défaut, l'envoi de commandes au périphérique mobile est désactivé.

► *Pour envoyer les commandes de l'Antivol au périphérique mobile, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).

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

3. Dans le groupe **Envoi des instructions**, cliquez sur le lien **Envoyer des instructions à partir de la stratégie** pour ouvrir la fenêtre de sélection des commandes.

4. Sélectionnez les commandes de l'Antivol que vous souhaitez envoyer au périphérique mobile :

   - Pour obtenir les coordonnées géographiques de l'appareil, cochez la case **Géolocalisation**.

   - Pour verrouiller le périphérique, cochez la case **Verrouillage**.

     Pour déverrouiller le périphérique, l'utilisateur devra saisir le code à usage unique pour le déverrouillage du périphérique (cf. section "Création d'un mot de passe à usage unique pour le déverrouillage du périphérique" à la page 49).

   - Pour supprimer les données personnelles et celles de l'entreprise sur le périphérique, cochez la case **Suppression des données d'entreprise**.

     Les données de l'entreprise désignent les données dans les stockages, les paramètres de connexion au réseau sans fil de l'entreprise, au réseau VPN, le point d'accès (APN)n le profil TouchDown, le profil de travail Android for Work, Samsung KNOX 2 ainsi que la clé de KNOX License Manager.

   - Pour supprimer toutes les données du périphérique, cochez la case **Suppression de toutes les données**.

5. Appuyez sur **OK**.

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

Le périphérique mobile recevra la commande de l'Antivol après la synchronisation suivante avec le Serveur d'administration. Vous pouvez consulter le résultat de l'exécution de la commande dans la Console d'administration, dans la fenêtre des résultats de l'exécution des commandes dans les paramètres du périphérique.

Création d'un mot de passe à usage unique pour le déverrouillage du périphérique

Afin de déverrouiller le périphérique 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 unique pour chaque appareil mobile.

► *Pour créer un code à usage unique pour le déverrouillage du périphérique mobile, procédez comme suit :*

1. Dans l'arborescence de la console, dans le dossier **Gestion des appareils mobiles**, sélectionnez le sous-dossier **Appareils mobiles**.
2. Sélectionnez le périphérique mobile pour lequel vous souhaitez recevoir un code de déverrouillage à usage unique.
3. Double-cliquez pour ouvrir la fenêtre des propriétés du périphérique mobile.
4. Choisissez la section **Applications**.
5. Choisissez l'application Kaspersky Endpoint Security Service Pack 1, Maintenance Release 3, puis appuyez sur le bouton **Propriétés**.
6. Choisissez la section **Antivol**.
7. Dans le groupe **Code à usage unique pour le déverrouillage de l'appareil**, 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.
8. Envoyez le code à usage unique à l'utilisateur via n'importe quelle méthode disponible afin que celui-ci puisse déverrouiller le périphérique mobile.

Configuration des paramètres de la Protection Internet

Afin de protéger les données personnelles de l'utilisateur du périphérique 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 Protection Internet fonctionne uniquement dans le navigateur Google Chrome™ et ne fonctionne pas dans les autres navigateurs.

La Protection Internet est activée par défaut : l'accès aux sites Internet des catégories **Phishing** et **Applications malveillantes** 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 des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Protection Internet**.
3. Cochez la case **Activer la Protection Internet**.
4. Si vous souhaitez que l'application limite l'accès de l'utilisateur aux sites Internet en fonction de leur contenu, procédez comme suit :
   a. sélectionnez l'option **Sites Internet interdits des catégories sélectionnées** dans le groupe **Protection Internet**.
   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.
5. Si vous souhaitez que l'application autorise l'utilisateur à accéder uniquement aux sites Internet désignés par l'administrateur, procédez comme suit :
   a. sélectionnez l'option **Seuls les sites Internet répertoriés sont autorisés** dans le groupe **Protection Internet**.

b. Composez la liste des sites Internet en ajoutant les adresses des sites auxquels l'application ne bloquera pas l'accès. Vous pouvez indiquer l'adresse complète du site Internet (par exemple, pictures.example.com) ou utiliser des expressions rationnelles. Pour de plus amples informations sur l'utilisation des expressions rationnelles, consultez la documentation java.util.regex.pattern http://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html.

6. Si vous souhaitez que l'application limite l'accès à n'importe quel site Internet, sélectionnez l'option **Tous les sites Internet sont interdits** dans le groupe **Protection Internet**.

7. 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**.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Administration des applications mobiles tierces

Cette section décrit les modes d'installation d'applications tierces employées à des fins professionnelles sur les périphériques mobiles des utilisateurs.

Dans cette section

Présentation des conteneurs

Vous pouvez utiliser des conteneurs afin de contrôler l'activité des applications mobiles lancées sur le périphérique 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 le périphérique.

Vous pouvez placer uniquement 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 53). Dans ce cas, la distribution de l'application dans le conteneur est placée automatiquement sur le serveur Internet de Kaspersky Security Center.

Les conteneurs ne peuvent être utilisés que sur des appareils Android.

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

- Possibilité de chiffrer automatiquement les données de l'application dans le conteneur sur le périphérique 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 :

  - Nom d'utilisateur et mot de passe de domaine. Lors du lancement de l'application dans le conteneur sur l'appareil, l'utilisateur saisit son nom 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 le périphérique 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.
- Contrôle des requêtes adressées par l'application dans le conteneur.

Vous pouvez utiliser une des méthodes suivantes pour installer l'application dans le conteneur sur le périphérique 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 du périphérique mobile avec le Serveur d'administration, la distribution de l'application figurant dans le conteneur est automatiquement copiée sur le périphérique de l'utilisateur.

Création 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 la fenêtre de l'Assistant **Paramètres** , sélectionnez dans le champ **Sélectionnez une application** la distribution de l'application mobile (extension apk).
6. Cochez la case **Créer un conteneur avec l'application sélectionnée**.

   Le programme 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**.

7. Pour envoyer le lien à l'utilisateur directement par email pour qu'il télécharge l'application dans le conteneur de son périphérique mobile, appuyez sur le bouton **Envoyer par e-mail**.

8. Pour enregistrer l'application dans le conteneur localement sur votre poste de travail ou sur le réseau, appuyez sur le bouton **Enregistrer sous**.

Configuration de l'administration du périphérique

Cette section contient les informations sur la configuration des paramètres d'administration du périphérique mobile.

Dans cette section

Configuration du mot de passe système

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

Par défaut, Kaspersky Endpoint Security ne demande pas de saisir ou de définir un mot de passe système lors du démarrage du périphérique 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 des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Gestion de l'appareil**.

3. Si vous souhaitez que l'application recherche l'existence d'un mot de passe système au démarrage du périphérique, 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 le périphérique, 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 le bouton **Appliquer** pour enregistrer les modifications apportées.

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Configuration des restrictions pour les périphériques Android

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

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

► *Pour configurer les restrictions au niveau de l'utilisation du Wi-Fi, de l'appareil photo et du Bluetooth sur le périphérique mobile, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Gestion de l'appareil**.

3. Dans le groupe **Restrictions**, configurez l'utilisation du module Wi-Fi, du périphérique photo et du Bluetooth :

   - Pour désactiver le module Wi-Fi sur le périphérique mobile de l'utilisateur, cochez la case **Interdire l'utilisation du Wi-Fi**.

   - Pour désactiver l'appareil photo sur le périphérique mobile de l'utilisateur, cochez la case **Interdire l'utilisation de la caméra**.

- Pour désactiver la fonction Bluetooth sur le périphérique mobile de l'utilisateur, cochez la case **Interdire l'utilisation du Bluetooth**.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Configuration de TouchDown

Afin d'assurer une utilisation sécurisée de la messagerie professionnelle sur le périphérique 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 des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Gestion de l'appareil**.

3. Dans le groupe **Profil TouchDown**, définissez les paramètres du client de messagerie TouchDown :

   - Dans le champ **Adresse du serveur**, saisissez l'adresse IP ou le nom DNS du serveur sur lequel se trouve le serveur de messagerie.

   - Indiquez le nom du domaine Active Directory dans lequel le compte de l'utilisateur est enregistré dans le champ **Domaine**.

4. Pour définir un certificat dans le client de messagerie TouchDown, cochez la case **Ne pas vérifier le certificat serveur**.

   Il faut au préalable ajouter ce certificat au périphérique de l'utilisateur dans la Console d'administration Kaspersky Security Center à l'entrée **Comptes utilisateur**.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Configuration des paramètres avancés

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 le périphérique mobile de l'utilisateur, il convient de configurer les paramètres du Filtre des appels et des SMS.

A cause des restrictions techniques de Android versions 4.4 et suivantes, la fonctionnalité du filtrage des appels et des SMS liée à l'envoi et à la réception des SMS peut fonctionner incorrectement.

► *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 des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Paramètres avancés**.
3. Cochez la case **Autoriser le filtrage des appels et SMS**.
4. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration. 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 paramètres de suppression de Kaspersky Endpoint Security

Pour supprimer Kaspersky Endpoint Security du périphérique mobile, il convient de configurer les paramètres de suppression de l'application. Par défaut, l'utilisateur n'a pas la possibilité de supprimer lui-même l'application du périphérique mobile.

► *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 des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Paramètres avancés**.
3. Dans le groupe **Suppression de l'application**, configurez les paramètres de suppression de l'application sur le périphérique Android :
   - Pour autoriser l'utilisateur à supprimer lui-même l'application du périphérique mobile, cochez la case **Autoriser la suppression de Kaspersky Endpoint Security for Android**.
   - Pour 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 le bouton **Appliquer** pour enregistrer les modifications apportées.

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Connexion au réseau sans fil

► *Pour connecter un périphérique mobile à un réseau sans fil, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Réseaux sans fil (Wi-Fi)**.

3. Dans le groupe **Réseaux sans fil**, cliquez sur **Ajouter**.

   La fenêtre **Réseau sans fil** s'ouvre.

4. Dans le champ **SSID réseau**, indiquez le nom du réseau sans fil contenant le point d'accès (SSID).

5. 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).

6. Saisissez dans le champ **Mot de passe** le mot de passe d'accès au réseau si vous aviez sélectionné un réseau sécurisé à l'étape précédente.

7. Saisissez dans le champ **Adresse et port du serveur proxy** l'adresse IP ou le nom DNS du serveur proxy ainsi que son numéro de port, le cas échéant.

   Le réseau sans fil ajouté apparaît dans la liste **Réseaux sans fil**.

   > 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.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration. L'utilisateur pourra ainsi se connecter au réseau sans fil ajouté sans avoir à indiquer les paramètres du réseau après que la stratégie aura été appliquée sur le périphérique mobile de l'utilisateur.

Configuration du Contrôle des applications

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

Dans cette section

Configuration des paramètres de lancement des applications

Pour garantir la sécurité du périphérique mobile de l'utilisateur, il est indispensable de configurer les paramètres de lancement des applications sur ce périphérique.

► *Pour définir les paramètres de lancement des applications sur le périphérique mobile, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).
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 le périphérique mobile de l'utilisateur :
   - Pour autoriser l'utilisateur du périphérique mobile à lancer toutes les applications, à l'exception de celles reprises dans la liste des catégories ou marquées comme interdites, sélectionnez le mode **Applications bloquées**.
   - Pour autoriser l'utilisateur du périphérique mobile à lancer uniquement les applications reprises dans la liste des catégories et celles marquées comme autorisées, recommandées ou obligatoires, sélectionnez le mode **Applications autorisées**.
4. Pour que Kaspersky Endpoint Security compose un rapport sur les applications interdites installées sur le périphérique mobile de l'utilisateur, sans pour autant les bloquer, cochez la case **Ne pas bloquer les applications interdites, rapport uniquement**.

Kaspersky Endpoint Security génère alors le rapport **Une application interdite est installée** lors de la synchronisation du périphérique mobile de l'utilisateur avec le Serveur d'administration. Le rapport est accessible dans le dossier **Rapports et notifications** de l'arborescence de la console ou dans les propriétés locales de l'application.

5. Pour que Kaspersky Endpoint Security bloque l'exécution des applications système sur le périphérique mobile de l'utilisateur en mode **Applications autorisées**, cochez la case **Bloquer les applications système**.
6. Composez la liste des catégories et des applications pour configurer le lancement des applications.

   Pour en savoir plus sur les catégories d'applications, consultez l'Appendice 3 (cf. section "Appendice 3. Catégories d'applications" à la page 171).

   La liste des applications qui appartiennent à chaque catégorie peut être consultée sur le site de Kaspersky Lab http://whitelist.kaspersky.com/catalogue.
7. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Installation d'applications tierces sur le périphérique

Conformément aux exigences relatives à la sécurité de l'entreprise, les applications mobiles tierces peuvent être installées sur les périphériques des utilisateurs en tant qu'applications autorisées, recommandées ou obligatoires pour le travail. Vous pouvez télécharger sur le périphérique des paquets d'applications mobiles créés au préalable dans Kaspersky Security Center. En outre, vous pouvez placer une application mobile tierce dans le conteneur et la télécharger sur le périphérique mobile de l'utilisateur (cf. section "Création de conteneurs" à la page 53) afin d'assurer la protection des données de l'entreprise.

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

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).

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 des applications mobiles** qui s'ouvre, sélectionnez le paquet de l'application mobile.

   - Indiquez manuellement le paquet d'applications mobiles :

     - **Nom du paquet** ;
     - **Nom de l'application** ;
     - **Lien vers la distribution.**

5. Dans la liste **Type d'application**, sélectionnez l'option **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**.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration. Les listes des applications obligatoires et recommandées seront transmises au périphérique mobile de l'utilisateur. L'utilisateur sera invité à installer les applications tierces. Une fois que l'utilisateur a confirmé l'installation, l'application tierce est installée sur le périphérique mobile de l'utilisateur.

Configuration du rapport sur les applications installées

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

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

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).
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 du périphérique mobile de l'utilisateur avec le Serveur d'Administration. Un rapport est généré à chaque modification apportée à la liste des applications installées sur le périphérique 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 le périphérique mobile de l'utilisateur une fois la stratégie appliquée. Le rapport généré est accessible dans le dossier **Rapports et notifications** dans l'arborescence de la console ou dans les propriétés locales de l'application (cf. *Manuel de l'administrateur de Kaspersky Security Center*).

Contrôle de la conformité des périphériques mobiles à la stratégie de groupe

Cette section fournit des informations sur l'utilisation du module Contrôle de la conformité.

Vous pouvez vérifier la conformité des périphériques mobiles à la stratégie de groupe à l'aide du module Contrôle de la conformité. Le Contrôle de la conformité assure que les périphériques mobiles sont conformes à la stratégie et, si nécessaire, modifie leurs paramètres de fonctionnement à l'aide des règles d'analyse (cf. section "Présentation du Contrôle de la conformité" à la page 64). Vous pouvez vérifier régulièrement la conformité des périphériques mobiles des utilisateurs vis-à-vis de la stratégie de groupe. Les résultats de la vérification sont consignés dans un rapport.

Dans cette section

Présentation du Contrôle de la conformité

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

- Les critères de conformité du périphérique à la stratégie de groupe. Un critère est un paramètre défini de la stratégie de groupe.
- Les actions que l'application exécute sur le périphérique 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 du périphérique pendant laquelle l'utilisateur peut corriger lui-même les non conformités à la stratégie de groupe décelées sur le périphérique. Pendant la période de restriction temporaire, l'application n'exécute pas l'action indiquée dans la règle sur le périphérique.

La règle de vérification des périphériques 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 35). Vous pouvez activer ou désactiver la règle de vérification créée dans la section **Contrôle de conformité**, dans le groupe **Règles d'analyse** (cf. section "**Définition des règles d'analyse de la conformité**" à la page 67). Vous pouvez activer une ou plusieurs règles de vérification. L'activation de la règle de vérification s'effectue à chaque synchronisation des périphériques mobiles avec le Serveur d'administration.

Critères de vérification des périphériques

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 périphériques des utilisateurs à la stratégie de groupe peut être exécutée selon les critères suivants :

- **La protection en temps réel est activée**. Vérification de l'utilisation de la protection antivirus sur le périphérique mobile.
- **Les bases antivirus sont à jour**. Vérification de l'actualité des bases antivirus de l'application Kaspersky Endpoint Security for Android sur le périphérique 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**. Vérification de la présence éventuelle d'applications interdites su le périphérique. 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**. Vérification de la présence éventuelle sur le périphérique d'applications issues de catégories interdites. 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**. Vérification de la présence sur le périphérique de toutes les applications requises. 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**. Vérification de la version du système d'exploitation du périphérique mobile. L'Assistant de création d'une règle de vérification permet d'indiquer les versions de systèmes d'exploitation pouvant être utilisés sur le périphérique de l'utilisateur.
- **L'appareil se synchronise régulièrement**. Vérification de la régularité de la synchronisation du périphérique mobile 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**. Vérification de l'intégrité du système d'exploitation du périphérique.

- **Le mot de passe de l'appareil est conforme aux directives de l'entreprise**. Vérification du nombre de caractères dans le mot de passe système de l'utilisateur. Vous pouvez indiquer le nombre minimal admis de caractères pour le mot de passe de l'utilisateur dans la section **Gestion de l'appareil** des propriétés de la stratégie.

- **Installation de la version actuelle de Kaspersky Endpoint Security for Android**. Vérification de la version de l'application mobile Kaspersky Endpoint Security for Android. L'Assistant de création d'une règle de vérification permet d'indiquer la version minimale de l'application qui peut être utilisée sur le périphérique de l'utilisateur.

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, Kaspersky Endpoint Security applique au périphérique les actions que vous avez indiquées dans la règle de vérification.

Vous pouvez indiquer les actions suivantes :

- **Interdire l'accès au courrier de l'entreprise (TouchDown)**. L'application Kaspersky Endpoint Security for Android du périphérique 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 le périphérique de l'utilisateur.

- **Verrouiller**. L'application Kaspersky Endpoint Security for Android bloque le périphérique de l'utilisateur.

- **Supprimer les données d'entreprise**. L'application Kaspersky Endpoint Security for Android supprime les données d'entreprise suivantes du périphérique de l'utilisateur :

- données des conteneurs ;
- paramètres du réseau sans fil de l'entreprise ;
- paramètres du point d'accès de l'entreprise (APN, VPN) ;
- paramètres du profil TouchDown ;
- paramètre du profil de travail Android for Work ;
- paramètres de Samsung KNOX 2 ;
- clé KNOX License Manager.

- **Supprimer toutes les données**. L'application Kaspersky Endpoint Security for Android supprime toutes les données du périphérique 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 temporaires sont indiquées pour une seule et même action, l'application applique la restriction temporaire la plus basse. Si, suite à la deuxième vérification des périphériques, les paramètres de ceux-ci satisfont aux critères, l'application lève les restrictions imposées.

Définition des règles de vérification de la conformité

► *Pour créer une règle de vérification de conformité des périphériques à la stratégie de groupe, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Contrôle de conformité**.
3. Pour obtenir les notification sur les périphériques qui ne sont pas conformes à la stratégie, cochez la case **Avertir l'administrateur** dans le groupe **Notifications de non-conformité**.

Si le périphérique ne correspond pas à la stratégie, Kaspersky Endpoint Security génère le rapport **Non-conformité détectée : <nom du critère de vérification>** lors de la synchronisation du périphérique avec le Serveur d'administration Kaspersky Endpoint Security. Ce rapport est accessible dans le dossier **Rapports et notifications** de l'arborescence de la console ou dans les propriétés locales de l'application.

4. Pour signaler à l'utilisateur du périphérique que ce dernier ne correspond pas à la stratégie, cochez la case **Avertir l'utilisateur** dans le groupe **Notifications de non-conformité**.

   Si le périphérique ne correspond pas à la stratégie, lors de la synchronisation du périphérique avec le Serveur d'administration, Kaspersky Endpoint Security prévient l'utilisateur dans la section **Etat** du groupe **Sécurité corporative**.

5. Dans le groupe **Règles d'analyse**, composez la liste des règles de vérification de la conformité des périphériques 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 s'affiche dans le groupe **Règles d'analyse** de la liste des règles de vérification.

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

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration. Si le périphérique de l'utilisateur ne correspond pas aux règles, le périphérique est soumis aux restrictions définies dans la liste des règles de vérification.

Administration d'Android for Work

Android for Work est une plateforme de gestion de l'infrastructure mobile d'entreprise et qui fournit aux employés de l'entreprise un environnement professionnel pour périphériques mobiles. Pour plus

de détails sur l'utilisation d'Android for Work, visitez le site d'assistance technique de Google https://support.google.com/work/android?hl=fr.

> Android for Work est accessible uniquement sur les périphériques gérés par le système d'exploitation Android version 5.0 ou ultérieure à l'aide d'Android for Work.

Vous pouvez créer un profil de travail Android for Work sur le périphérique mobile de l'utilisateur (ci-après, le "profil de travail"). Le *profil de travail Android for Work* est un environnement sécurisé sur le périphérique de l'utilisateur et dans lequel l'administrateur peut gérer des applications et des comptes sans limiter ses possibilités lors de l'utilisation des données personnelles. Lors de la création d'un profil de travail sur le périphérique mobile de l'utilisateur, les applications d'entreprise suivantes sont installées automatiquement dans ce profil : Google Play Store, Google Chrome, Téléchargements, Kaspersky Endpoint Security for Android, etc. Les applications réparties dans le profil de travail et les notifications de ces applications sont signalées par une icône rouge de profil. Pour l'application Google Play Store, un compte d'entreprise Google séparé doit être créé. Les applications réparties dans le profil de travail sont indiquées dans la liste commune d'applications.

► *Pour configurer les paramètres du profil de travail d'Android for Work, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Gestion d'Android for Word**.
3. Cochez la case **Créer un profil de travail** dans le groupe **Paramètres du profil de travail**.
4. Configurez les paramètres du profil de travail :
   - Pour activer le Contrôle des applications dans le profil de travail Android for Word et le désactiver dans le profil personnel, cochez la case **Activer le Contrôle des applications sous le profil de travail uniquement**.

     Vous pouvez créer des listes d'applications autorisées, interdites, recommandées et obligatoires, ainsi que des catégories d'application autorisées et interdites dans la section **Contrôle des applications** (cf. section "**Configuration des paramètres de lancement des applications**" à la page 60).

- Pour activer la Protection Internet dans le profil de travail Android for Work et la désactiver dans le profil personnel, cochez la case **Activer la Protection Internet sous le profil de travail uniquement**.

  La Protection Internet limite l'accès des utilisateurs aux sites Internet uniquement quand le navigateur Google Chrome est utilisé. Vous pouvez configurer les paramètres d'accès aux sites Internet (créer une liste de catégories interdites de sites Internet ou une liste de sites Internet autorisés) dans la section **Protection Internet** (cf. section "**Configuration des paramètres de la Protection Internet**" à la page 50).

- Pour empêcher qu'un utilisateur puisse copier des données via le presse-papiers de l'application entre le profil de travail et des applications privées, cochez la case **Interdire le transfert de données du profil de travail vers un profil privé**.

- Pour empêcher que l'utilisateur puisse installer des applications dans le profil de travail Android for Work, cochez la case **Interdire l'installation de l'application sur un profil de travail à partir de toutes les sources**.

- Pour empêcher que l'utilisateur puisse installer des applications dans le profil de travail Android for Work à partir de toutes les sources, sauf Google Play, cochez la case **Interdire l'installation de l'application sur un profil de travail à partir de sources inconnues**.

- Pour empêcher que l'utilisateur puisse supprimer des applications depuis le profil de travail Android for Work, cochez la case **Interdire la suppression d'applications à partir d'un profil de travail**.

5. Pour configurer les paramètres du profil de travail sur le périphérique mobile de l'utilisateur, bloquez la modification des paramètres.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration. L'espace du périphérique mobile de l'utilisateur sera scindé entre le profil de travail et le profil personnel.

Activation de Kaspersky Endpoint Security for Android

► *Pour activer l'application Kaspersky Endpoint Security for Android, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Gestion de la 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 pour laquelle une licence a été achetée, la durée de validité de la licence et son type.

4. Cochez la case **Activer à l'aide d'une clé provenant du stockage de Kaspersky Security Center**.

   Si l'application Kaspersky Endpoint Security a été activée sans l'aide d'une clé du stockage de Kaspersky Security Center, Kaspersky Enpoint Security remplace cette clé par la clé sélectionnée dans la liste **Clé**.

5. Afin d'activer l'application sur le périphérique mobile de l'utilisateur, verrouillez la modification des paramètres.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Administration de Samsung KNOX

Cette section contient des informations sur la configuration de Samsung KNOX.

Samsung KNOX est une solution mobile pour la configuration et la protection des périphériques mobiles Samsung tournant sous Android. La liste des modèles de périphériques pris en charge figure sur le site Internet de Samsung KNOX https://www.samsungknox.com/knoxportal/files/GalaxyDevicesSupportingKNOX.pdf.

Dans cette section

Configuration du point d'accès (APN)

Pour pouvoir utiliser le point d'accès sur le périphérique mobile de l'utilisateur, le périphérique 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 périphériques Android prenant en charge l'utilisation de Samsung KNOX toutes versions confondues.

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

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).

2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Administration de Samsung KNOX → Point d'accès (APN)**.

3. Dans le groupe **Point d'accès (APN)**, cliquez sur le bouton **Paramètres**.

   La fenêtre **Paramètres du point d'accès (APN)** s'ouvre.

4. Sous l'onglet **Général**, indiquez les paramètres suivants pour le point d'accès :

   a. Dans la liste déroulante **Type d'APN**, 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 **MCC**, indiquez le code mobile du pays (MCC).

   d. Dans le champ **MNC**, indiquez le code mobile du réseau (MNC).

   e. 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 du périphérique mobile sur le serveur de l'opérateur mobile fournissant l'accès au réseau.

   b. 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.

c. 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.

d. Dans le champ **Nom d'utilisateur**, indiquez le nom de l'utilisateur pour l'autorisation sur le réseau mobile.

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

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Configuration du pare-feu

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

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

► *Pour configurer le mode de fonctionnement du Pare-feu, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).

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

   - Sélectionnez la section **Paramètres pour KNOX 1**, si le périphérique mobile est compatible avec Samsung KNOX version 1.

   - Sélectionnez la section **Paramètres pour KNOX 2**, si le périphérique mobile est compatible avec Samsung KNOX version 2.

3. Dans le groupe **Pare-feu**, appuyez sur **Paramètres**.

   La fenêtre **Paramètres du Pare-feu** s'ouvre.

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

   - Pour autoriser toutes les connexions entrantes et sortantes sur le périphérique mobile, déplacez le curseur jusqu'à la position **Tout autoriser**.
   - Pour que l'application bloque toute activité réseau, exceptée celle des applications de la liste des exclusions, déplacez le curseur jusqu'à la position **Tout bloquer, sauf les exclusions**.

5. Si vous avez sélectionné le mode de fonctionnement du Pare-feu **Tout bloquer, sauf les exclusions**, composez la liste des exclusions :

   a. Cliquez sur le bouton **Ajouter**.

      La fenêtre **Exclusion** s'ouvre.

   b. Dans le champ **Nom de l'application**, saisissez le nom de l'application mobile.

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

   d. Cliquez sur le bouton **OK**.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Configuration de la connexion VPN

Il est possible de configurer la connexion VPN uniquement pour des périphériques Android compatibles avec Samsung KNOX version 1.

► *Pour configurer la connexion VPN sur le périphérique mobile de l'utilisateur, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).
2. Dans la fenêtre **Propriétés de <Nom de la stratégie>**, choisissez la section **Administration de Samsung KNOX** → **Paramètres pour KNOX 1**.
3. Dans le groupe **Réseau privé virtuel (VPN)**, appuyez sur le bouton **Paramètres**.

   La fenêtre **Paramètres du réseau privé virtuel (VPN)** s'ouvre.
4. Dans la liste déroulante **Type de réseau**, sélectionnez le type de connexion VPN.
5. Saisissez le nom du tunnel VPN dans le champ **Nom du réseau**.
6. Dans le champ **Adresse du serveur**, saisissez le nom réseau ou l'adresse IP du serveur VPN.
7. 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.
8. Dans le champ **DNS-serveur(s)**, 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.
9. Dans le champ **Redirection**, saisissez la plage d'adresses IP du réseau avec lesquelles s'effectue l'échange de données via la connexion VPN.

   > Si le champ **Redirection** ne contient pas la plage des adresses IP, l'ensemble du trafic Internet passera par la connexion VPN.
10. Configurez les paramètres complémentaires suivants pour les types de réseau **IPSec Xauth PSK** et **L2TP IPSec PSK** :

    a. Dans le champ **Clé partagée IPSec**, saisissez le mot de passe de la clé de sécurité IPSec préalablement installée.

    b. Dans le champ **ID IPSec**, saisissez le nom de l'utilisateur du périphérique mobile.

11. Pour le type de réseau **L2TP IPSec PSK**, indiquez également le mot de passe pour la clé L2TP dans le champ **Clé L2TP**.

12. Pour le type de réseau PPTP, cochez la case **Utiliser le chiffrement** pour que l'application utilise la méthode de chiffrement MPPE (Microsoft® Point-to-Point Encription) afin d'assurer la sécurité du transfert de données lors de la connexion du périphérique mobile au serveur VPN.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Il convient de prendre en compte les exigences suivantes lors de l'utilisation d'un réseau privé virtuel :

- L'application qui utilise la connexion VPN doit être autorisée dans les paramètres du Pare-feu (cf. section "Configuration du Pare-feu" à la page 74).
- 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 des paramètres de Microsoft Exchange

Afin d'assurer une utilisation sécurisée de la messagerie professionnelle sur le périphérique 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 périphériques Android prenant en charge l'utilisation de Samsung KNOX toutes versions confondues.

► *Pour configurer Microsoft Exchange sur le périphérique mobile de l'utilisateur, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).

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

   - Sélectionnez la section **Paramètres pour KNOX 1**, si le périphérique mobile est compatible avec Samsung KNOX version 1.

   - Sélectionnez la section **Paramètres pour KNOX 2**, si le périphérique mobile est compatible avec Samsung KNOX version 2.

3. Dans le groupe **Serveur de messagerie Exchange**, appuyez sur le bouton **Paramètres**.

   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 du périphérique mobile sur le réseau de l'entreprise.

6. Dans la liste déroulante **Période de synchronisation**, sélectionnez la période souhaitée pour la synchronisation du périphérique mobile avec le serveur Microsoft Exchange.

7. Pour utiliser le protocole de transfert de données SSL, cochez la case **Utiliser le chiffrement (SSL)**.

8. Pour utiliser des certificats numériques afin de protéger l'échange de messages entre le périphérique mobile et le serveur Microsoft Exchange, cochez la case **Vérifier le certificat serveur**.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Activation de Samsung KNOX 2

L'utilisation de la fonction Samsung KNOX 2 sur un périphérique mobile requiert l'activation préalable de Samsung KNOX 2. Pour activer Samsung KNOX 2, il est nécessaire d'obtenir une clé KNOX License Manager (ci-après clé KLM) auprès de la société Samsung. *Clé KNOX License Manager* : il s'agit d'un code unique utilisé par le système d'administration des licences Samsung KNOX. Il est possible d'acquérir une clé KLM dans la Boutique KNOX (KNOX Marketplace). Vos pouvez également obtenir une clé KLM auprès d'un intermédiaire commercial ou d'un responsable de la clientèle Samsung. Pour en savoir plus à propos de la clé KLM, consultez le site de support technique Samsung KNOX https://www.samsungknox.com.

Sans clé KLM, il est impossible de configurer les paramètres Samsung KNOX 2 sur un périphérique mobile.

► *Pour activer Samsung KNOX 2, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).
2. Dans la fenêtre **Propriétés de <Nom de la stratégie>**, sélectionnez la section **Administration de Samsung KNOX → Paramètres pour KNOX 2**.
3. Dans le champ **Clé KNOX License Manager**, saisissez la clé KLM obtenue auprès de la société Samsung.
4. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration. Une fois la stratégie appliquée, les fonctions Samsung KNOX 2 seront activées sur le périphérique mobile de l'utilisateur. Les paramètres de l'Access Point Name (APN), du Pare-feu et du serveur de messagerie Exchange seront également configurés en fonction des paramètres de la stratégie.

Désactivation de Samsung KNOX 2

► *Pour désactiver Samsung KNOX 2, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques Android (cf. section "Administration des périphériques Android" à la page 40).

2. Dans la fenêtre **Propriétés de <Nom de la stratégie>**, sélectionnez la section **Administration de Samsung KNOX** → **Paramètres pour KNOX 2**.

3. Dans le champ **Clé KNOX License Manager**, supprimez la clé KLM obtenue auprès de la société Samsung.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration. Une fois la stratégie appliquée, les fonctions Samsung KNOX 2 seront désactivées sur le périphérique mobile de l'utilisateur. Il sera impossible de configurer les paramètres de l'Access Point Name (APN), du Pare-feu et du serveur de messagerie Exchange à l'aide de la stratégie.

Administration des périphériques iOS

Pour pouvoir administrer des périphériques iOS, l'application Kaspersky Safe Browser for iOS doit être installée sur le périphérique mobile. Pour en savoir plus sur l'installation de Kaspersky Safe Browser pour iOS, consultez le *Manuel d'implantation de Kaspersky Security for Mobile*.

L'administration des périphériques iOS s'opère à l'aide de stratégies de groupe. Les stratégies de groupe permettent de configurer les paramètres de l'application Kaspersky Safe Browser for iOS installée sur le périphérique.

► *Pour configurer la stratégie de groupe pour l'administration des périphériques iOS, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration auquel appartiennent les périphériques dont vous souhaitez configurer les paramètres.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Sélectionnez la stratégie pour Kaspersky Endpoint Security 10 for Mobile Service Pack 1 Maintenance Release 3 dan,s la liste des stratégies.

   Si nécessaire, vous pouvez créer une nouvelle 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 35).
4. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.

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

Dans cette section

Configuration des paramètres 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.

Par défaut, les périphériques 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 périphériques mobiles avec le Serveur d'administration, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques iOS.
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Synchronisation**.
   a. Sélectionnez la fréquence de lancement de la synchronisation dans la liste déroulante **Lancer la synchronisation**.
   b. Pour interdire la synchronisation automatique avec le Serveur d'administration quand le périphérique est en itinérance, cochez la case **Désactiver la synchronisation en itinérance**.
3. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Configuration des paramètres de la Protection Internet

Afin de protéger les données personnelles de l'utilisateur du périphérique mobile lors de la navigation sur Internet, il convient de configurer les paramètres d'accès aux sites sur la base des catégories de sites Internet interdites.

Il est impossible de restreindre l'accès pour des sites Internet individuel dans Kaspersky Safe Browser.

La Protection Internet fonctionne uniquement dans le navigateur Kaspersky Safe Browser et ne fonctionne pas dans les autres navigateurs.

La Protection Internet est activée par défaut : l'accès aux sites Internet des catégories **Phishing** et **Applications malveillantes** 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 des périphériques iOS.

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

2. sélectionnez l'option **Sites Internet interdits des catégories sélectionnées** dans le groupe **Protection Internet**.

3. Composez la liste des catégories interdites : cochez les cases des catégories de sites Internet dont l'accès sera bloqué par l'application.

4. Pour supprimer les restrictions sur l'accès de l'utilisateur du périphérique à certains sites en fonction du contenu, décochez la case **Activer la Protection Internet**.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Envoi de la commande de recherche au périphérique mobile

Afin de pouvoir obtenir les coordonnées du périphérique mobile en cas de perte ou de vol de celui-ci, il faut envoyer la commande de recherche au périphérique en question.

Par défaut, l'envoi de la commande au périphérique mobile est désactivé.

► *Pour envoyer la commande de recherche à un périphérique mobile, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques iOS.

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

2. Dans le groupe **Envoi des instructions**, appuyez su le lien **Envoyer des instructions à partir de la stratégie**.

   La fenêtre de sélection de la commande s'ouvre.

3. Dans la fenêtre **Envoi des instructions** qui s'ouvre, cochez la case **Géolocalisation**.

4. Appuyez sur **OK**.

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

Le périphérique mobile de l'utilisateur recevra l'instruction après la prochaine synchronisation du périphérique avec le Serveur d'administration. En réponse, Kaspersky Safe Browser envoi la position du périphérique. Les coordonnées du périphérique sont consultables dans la Console d'administration, dans la fenêtre des résultats de l'exécution des instructions dans les paramètres du périphérique.

Activation de Kaspersky Safe Browser for iOS

► *Pour activer l'application Kaspersky Safe Browser for iOS, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques iOS.
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Gestion de la 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 pour laquelle une licence a été achetée, la durée de validité de la licence et son type.
4. Pour activer l'application sur le périphérique mobile de l'utilisateur, bloquez la modification des paramètres en fermant le "cadenas".
5. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

L'application sera activée après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Administration des périphériques Windows Phone

Pour pouvoir administrer des périphériques Windows Phone, l'application Kaspersky Safe Browser for Windows Phone doit être installée sur le périphérique mobile. Pour en savoir plus sur l'installation de Kaspersky Safe Browser for Windows Phone, consultez le *Manuel d'implantation de Kaspersky Security for Mobile*.

L'administration des périphériques Windows Phone s'opère à l'aide de stratégies de groupe. Les stratégies de groupe permettent de configurer les paramètres de l'application Kaspersky Safe Browser for Windows Phone installée sur le périphérique.

► *Pour configurer la stratégie de groupe pour l'administration des périphériques Windows Phone, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration auquel appartiennent les périphériques dont vous souhaitez configurer les paramètres.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Sélectionnez la stratégie pour Kaspersky Endpoint Security 10 for Mobile Service Pack 1 Maintenance Release 3 dan,s la liste des stratégies.

   Si nécessaire, vous pouvez créer une nouvelle 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 35).
4. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.

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

Dans cette section

Configuration des paramètres 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.

Par défaut, les périphériques 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 périphériques mobiles avec le Serveur d'administration, procédez comme suit :*

1. Ouvrez la fenêtre des paramètres de la stratégie pour les périphériques Windows Phone.
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Synchronisation**.
   a. Sélectionnez la fréquence de lancement de la synchronisation dans la liste déroulante **Lancer la synchronisation**.
   b. Pour interdire la synchronisation automatique avec le Serveur d'administration quand le périphérique est en itinérance, cochez la case **Désactiver la synchronisation en itinérance**.
3. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Configuration des paramètres de la Protection Internet

Afin de protéger les données personnelles de l'utilisateur du périphérique mobile lors de la navigation sur Internet, il convient de configurer les paramètres d'accès aux sites sur la base des catégories de sites Internet interdites.

Il est impossible de restreindre l'accès pour des sites Internet individuel dans Kaspersky Safe Browser.

La Protection Internet fonctionne uniquement dans le navigateur Kaspersky Safe Browser et ne fonctionne pas dans les autres navigateurs.

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

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

1. Ouvrez la fenêtre des paramètres de la stratégie pour les périphériques Windows Phone.

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

2. Sélectionnez l'option **Sites Internet interdits des catégories sélectionnées** dans le groupe **Protection Internet**.

3. Composez la liste des catégories interdites : cochez les cases des catégories de sites Internet dont l'accès sera bloqué par l'application.

4. Pour supprimer les restrictions sur l'accès de l'utilisateur du périphérique à certains sites en fonction du contenu, décochez la case **Activer la Protection Internet**.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Envoi de la commande de recherche au périphérique mobile

Afin de pouvoir obtenir les coordonnées du périphérique mobile en cas de perte ou de vol de celui-ci, il faut envoyer la commande de recherche au périphérique en question.

Par défaut, l'envoi de la commande au périphérique mobile est désactivé.

► *Pour envoyer la commande de recherche à un périphérique mobile, procédez comme suit :*

1. Ouvrez la fenêtre des paramètres de la stratégie pour les périphériques Windows Phone.

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

2. Dans le groupe **Envoi des instructions**, appuyez su le lien **Envoyer des instructions à partir de la stratégie**.

   La fenêtre de sélection de la commande s'ouvre.

3. Dans la fenêtre **Envoi des instructions** qui s'ouvre, cochez la case **Géolocalisation**.

4. Appuyez sur **OK**.

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

Le périphérique mobile de l'utilisateur recevra l'instruction après la prochaine synchronisation du périphérique avec le Serveur d'administration. En réponse, Kaspersky Safe Browser envoi la position du périphérique. Vous pouvez consulter la position du périphérique dans la Console d'administration, dans la fenêtre des résultats de l'exécution des commandes dans les paramètres du périphérique.

Activation de Kaspersky Safe Browser for Windows Phone

► *Pour activer l'application Kaspersky Safe Browser for Windows Phone, procédez comme suit :*

1. Ouvrez la fenêtre des paramètres de la stratégie pour les périphériques Windows Phone.
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Gestion de la 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 pour laquelle une licence a été achetée, la durée de validité de la licence et son type.
4. Pour activer l'application sur le périphérique mobile de l'utilisateur, bloquez la modification des paramètres en fermant le "cadenas".
5. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

L'application sera activée après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Administration des périphériques EAS

Pour pouvoir administrer des périphériques mobiles EAS, les périphériques doivent êtres connectés au Serveur de périphériques mobiles Exchange ActiveSync. Pour en savoir plus sur la connexion des périphériques au Serveur des périphériques mobiles Exchange ActiveSync, consultez le *Manuel d'implantation du Kaspersky Security Center*.

L'administration des périphériques EAS s'opère à l'aide de stratégies de groupe. Les stratégies de groupe permettent de configurer les paramètres du périphérique mobile.

► *Pour configurer la stratégie de groupe pour l'administration des périphériques EAS, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration auquel appartiennent les périphériques EAS dont vous souhaitez configurer les paramètres.
2. Dans l'espace de travail du groupe, choisissez l'onglet Stratégies.
3. Dans la liste des stratégies, sélectionnez la stratégie pour Kaspersky Mobile Device Management 10 for Mobile.

   Si nécessaire, vous pouvez créer une stratégie de groupe à l'aide de l'Assistant de création de stratégie.
4. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.

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

Dans cette section

Configuration de la robustesse du mot de passe pour le déverrouillage

Afin de protéger les données du périphérique 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 du périphérique mobile.

► *Pour configurer les paramètres de robustesse du mot de passe pour le déverrouillage du périphérique EAS, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie de gestion des périphériques EAS.
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Mot de passe**.
3. Dans le groupe **Réglages 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 :
   - Pour forcer l'utilisation de majuscules et de chiffres dans le 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.
   - Pour que l'utilisateur puisse utiliser la fonctionnalité de restauration du mot de passe, cochez la case **Activer la restauration du mot de passe**.
   - Pour chiffrer les fichiers dans la mémoire du périphérique, cochez la case **Demander le chiffrement de l'appareil**.
   - Pour chiffrer les fichiers sur la carte mémoire, cochez la case **Demander le chiffrement sur la carte mémoire**.
   - Pour autoriser l'utilisateur à utiliser un mot de passe simple composé de chiffres uniquement, cochez la case **Autoriser un mot de passe simplifié**.

- Pour limiter le nombre de tentatives de saisie du mot de passe d'accès au périphérique, 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 pour déverrouiller le périphérique. 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.

- Pour imposer 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.

- Pour imposer la saisie du mot de passe après une période d'inactivité de l'utilisateur (celui-ci n'a réalisé aucune opération sur le périphérique), 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. A l'issue de cette période, le programme propose à l'utilisateur de saisir le mot de passe.

- Pour 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, le programme propose à l'utilisateur de changer de mot de passe.

- Le champ **Historique des mots de passe** permet d'indiquer le nombre de mots de passe antérieurs qui ne peuvent pas être utilisés.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration. Kaspersky Mobile Device Management vérifie la présence d'un mot de passe sur le périphérique 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 paramètres de la synchronisation

Pour garantir l'accès de l'utilisateur du périphérique EAS d'accéder aux messages électroniques, aux événements du calendrier, aux contacts et aux tâches sur le serveur Microsoft Exchange, il convient de configurer les paramètres de la synchronisation. Après la synchronisation, l'utilisateur peut utiliser ces données en mode hors ligne.

Par défaut, les événements du calendrier et les messages électroniques sont toujours conservés sur le périphérique 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 le périphérique mobile les pièces jointes accompagnant les messages électroniques.

► *Pour configurer les paramètres de synchronisation du périphérique EAS avec le Serveur Microsoft Exchange, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie de gestion des périphériques EAS.
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 le périphérique EAS dans la liste déroulante **Enregistrer les événements du calendrier**.
4. Dans la liste déroulante **Enregistrer les messages électroniques**, sélectionnez la durée de conservation des messages sur le périphérique EAS.
5. Pour limiter le volume des messages électroniques, cochez la case **Limiter la taille du courrier électronique (Ko)**. Dans le champ ci-dessous, indiquez le volume de messages autorisé en kilooctets.
6. Pour autoriser l'utilisateur à se synchroniser avec le serveur Microsoft Exchange en itinérance, à l'aide de la technologie Direct Push, cochez la case **Autoriser Direct Push lors de l'itinérance**.
7. Pour autoriser l'utilisateur à consulter ses emails au format HTML, cochez la case **Autoriser l'e-mail au format HTML**.

8. Configurer le téléchargement des pièces jointes accompagnant les messages électroniques :

   a. Pour autoriser l'utilisateur à télécharger sur le périphérique EAS les fichiers joints aux messages électroniques, cochez la case **Autoriser le téléchargement des pièces jointes sur l'appareil**.

      La case **Taille maximale d'une pièce jointe (Ko)** devient alors disponible.

   b. Pour limiter la taille des pièces jointes des messages électroniques entrants, cochez la case **Taille maximale d'une pièce jointe (Ko)**. Dans le champ en dessous, indiquez en kilooctets la taille maximale des pièces jointes pouvant être téléchargées sur le périphérique.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Configuration des restrictions de fonctions

Afin d'assurer la sécurité du périphérique EAS, il convient de configurer les restrictions des fonctions du périphérique.

Par défaut, toutes les fonctions du périphérique EAS peuvent être utilisées sans restriction.

► *Pour configurer les restrictions des fonctions sur le périphérique EAS, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie de gestion des périphériques EAS.
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Restrictions des fonctions**.
3. Dans le groupe **Réglages de restriction des fonctions**, autorisez ou interdisez l'utilisation des fonctions du périphérique EAS :

   - Pour autoriser la connexion d'une carte mémoire ou d'autres disques amovibles au périphérique, cochez la case **Autoriser les supports amovibles**.

- Pour autoriser l'appareil photo, cochez la case **Autoriser la caméra**.
- Pour autoriser les connexions Wi-Fi, cochez la case **Autoriser le Wi-Fi**.
- Pour autoriser l'utilisation du port infrarouge, cochez la case **Autoriser la connexion IR**.
- Pour autoriser l'utilisateur à utiliser le périphérique 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**.
- Pour autoriser une connexion entre le périphérique et un poste de travail distant, cochez la case **Autoriser le Bureau à distance à partir de l'appareil**.
- Pour utiliser le client Desktop ActiveSync sur le périphérique, cochez la case **Autoriser la synchronisation du bureau**.
- Dans la liste déroulante **Utilisation du Bluetooth**, autorisez ou interdisez l'utilisation du Bluetooth sur le périphérique 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 au périphérique mobile.
  - **Refuser**. L'utilisation de Bluetooth est interdite sur le périphérique mobile.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Configuration des restrictions d'applications

Afin d'assurer la sécurité du périphérique EAS, il convient de configurer les restrictions relatives au fonctionnement des applications (navigateur, applications non signées).

Par défaut, les applications du périphérique EAS peuvent être utilisées sans restriction.

► *Pour configurer les restrictions relatives au fonctionnement des applications sur le périphérique EAS, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie de gestion des périphériques EAS.

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

3. Dans le groupe **Réglages de restriction des applications**, configurez les restrictions relatives au fonctionnement des applications :

   - Pour autoriser l'utilisateur à utiliser le navigateur, cochez la case **Autoriser l'utilisation du navigateur**.

   - Pour autoriser l'utilisateur à créer des comptes de messagerie personnels (POP3 ou IMAP4), cochez la case **Autoriser la messagerie utilisateur**.

   - Pour autoriser l'utilisateur à exécuter des applications ne disposant pas d'un certificat d'authenticité signé, cochez la case **Autoriser les applications non signées**.

   - Pour autoriser l'utilisateur à installer des applications ne disposant pas d'un certificat d'authenticité signé, cochez la case **Autoriser les paquets d'installation non signés**.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration.

Administration des périphériques MDM iOS

Pour pouvoir administrer des périphériques mobiles MDM iOS, les périphériques doivent êtres connectés au Serveur de périphériques mobiles MDM iOS. Pour en savoir plus sur la connexion des appareils mobiles au Serveur des périphériques mobiles MDM iOS, consultez le *Manuel d'implantation de Kaspersky Security for Mobile*.

La stratégie d'administration permet de configurer les paramètres de fonctionnement du périphérique 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 périphériques mobiles faisant partie du groupe d'administration.

► *Pour configurer la stratégie de groupe pour l'administration des périphériques EAS, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration auquel appartiennent les périphériques MDM iOS dont vous souhaitez configurer les paramètres.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Dans la liste des stratégies, sélectionnez la stratégie pour Kaspersky Mobile Device Management 10 for Mobile.

   Si nécessaire, vous pouvez créer une stratégie de groupe à l'aide de l'assistant de création d'une stratégie (cf. page 35).
4. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.

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

Dans cette section

Configuration de la robustesse du mot de passe pour le déverrouillage

Afin de protéger les données du périphérique 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 du périphérique iOS MDM, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des périphériques MDM iOS.
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Mot de passe**.
3. Dans le groupe **Réglages 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 :
   - Pour autoriser l'utilisateur à utiliser un mot de passe simple, cochez la case **Autoriser un mot de passe simplifié**.
   - Pour imposer l'utilisation d'un mot de passe contenant des chiffres et des lettres, 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 d'utilisation maximale**, 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 du périphérique 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 **Période de grâce maximale pour le verrouillage sans mot de passe**, sélectionnez la durée pendant laquelle l'utilisateur peut déverrouiller le périphérique 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 le périphérique 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 le périphérique 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 périphériques iOS MDM

Afin de répondre aux exigences en matière de sécurité de l'entreprise, il convient de configurer les restrictions relatives au fonctionnement du périphérique iOS MDM.

► *Pour configurer les restrictions du périphérique iOS MDM, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des périphériques MDM iOS.
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Restrictions des fonctions**.
3. Dans le groupe **Paramètres des restrictions de fonctions**, cochez la case **Appliquer les paramètres à l'appareil**.

4. Configurez les restrictions des fonctions du périphérique iOS MDM.

   Les restrictions sont décrites dans l'Appendice (cf. section "Appendice 2. Restrictions pour les périphériques iOS MDM" à la page 151).

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 le périphérique iOS MDM.

   Les restrictions sont décrites dans l'Appendice (cf. section "Appendice 2. Restrictions pour les périphériques iOS MDM" à la page 151).

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 restriction du contenu multimédia**, cochez la case **Appliquer les paramètres à l'appareil**.

12. Configurez les restrictions pour le contenu multimédia sur le périphérique iOS MDM.

    Les restrictions sont décrites dans l'Appendice (cf. section "Appendice 2. Restrictions pour les périphériques iOS MDM" à la page 151).

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 le périphérique 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 du périphérique iOS MDM à Internet via un serveur proxy.

La connexion automatique à Internet via un serveur proxy n'est disponible que pour les périphériques contrôlés.

► *Pour configurer le proxy HTTP global sur le périphérique iOS MDM, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des périphériques MDM iOS.
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. *Reseaux captifs*: réseaux sans fil exigeant une authentification préalable sur le périphérique 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 réglage**, sélectionnez **Manuel**.

     b. Dans le champ **Adresse et port du serveur proxy**, 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 d'utilisateur**, indiquez le nom du compte utilisateur pour l'autorisation sur le serveur proxy. Vous pouvez utiliser les macros de la liste déroulante **Macros disponibles**.

     d. Dans le champ **Mot de passe**, indiquez le mot de passe du compte utilisateur pour l'autorisation sur le serveur proxy.

     e. Pour autoriser l'utilisateur à accéder aux réseaux via portail captif, cochez la case **Autoriser l'accès aux réseaux via portail captif sans connexion au serveur proxy**.

- Pour 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 réglage**, sélectionnez **Automatique**.

  b. Dans le champ **URL du fichier PAC**, indiquez l'adresse Internet du fichier PAC (par exemple, http://www.example.com/filename.pac).

  c. Pour autoriser l'utilisateur à connecter le périphérique mobile au réseau sans fil sans passer par le serveur proxy lorsque le fichier PAC est inaccessible, cochez la case **Autoriser une connexion directe si le fichier PAC n'est pas accessible**.

  d. Pour autoriser l'utilisateur à 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 du périphérique mobile se connectera ainsi à Internet via le serveur proxy une fois la stratégie appliquée.

Configuration des paramètres 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 le périphérique 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 du périphérique iOS MDM, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des périphériques MDM iOS.

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

3. Dans le groupe **Réglages du compte unique**, cochez la case **Appliquer les réglages à l'appareil**.

4. Dans le champ **Nom du compte**, saisissez le nom du compte utilisateur pour l'autorisation sur le serveur Kerberos. Vous pouvez utiliser les macros de la liste déroulante **Macros disponibles**.

5. Dans le champ **Nom d'utilisateur Kerberos**, saisissez le principal nom du compte de l'utilisateur du périphérique 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 **Macros disponibles**.

6. Dans le champ **Zone de travail de Kerberos**, saisissez le nom du réseau regroupant les serveurs Kerberos et les périphériques iOS MDM. L'espace de travail Kerberos doit être indiqué en majuscules.

7. Pour autoriser l'utilisateur à utiliser le compte unique sur les sites Internet ajoutés à la liste des adresses Internet autorisées uniquement, procédez comme suit :

   a. Cochez la case **Limiter l'utilisation du compte utilisateur pour les URL**.

   b. Cliquez sur le bouton **Paramètres** 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. Pour autoriser l'utilisateur à utiliser 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 pour les applications**.

    b. Cliquez sur le bouton **Paramètres** à droite de la case.

    c. La fenêtre **Identifiants des applications** s'ouvre.

    d. Dans la fenêtre **Identifiants des 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 le périphérique mobile de l'utilisateur une fois la stratégie appliquée.

Configuration de l'accès aux sites Internet

Afin de contrôler l'accès de l'utilisateur du périphérique 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. 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 périphériques contrôlés.

► *Pour configurer l'accès aux sites Internet sur le périphérique iOS MDM, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des périphériques MDM iOS.
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 bloqués**, créez la liste des sites Internet interdits.

      L'adresse du site Internet doit commencer par "http://" ou "**Error! Hyperlink reference not valid.**. 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 les sites Internet uniquement depuis la liste des signets**.

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 le périphérique mobile de l'utilisateur.

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

Le filtrage des sites Internet sera ainsi configuré sur le périphérique mobile de l'utilisateur conformément au mode sélectionné et aux listes crées une fois la stratégie appliquée.

Connexion au réseau sans fil

Afin de connecter automatiquement le périphérique 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 du périphérique iOS MDM à un réseau sans fil, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des périphériques MDM iOS.
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Réseaux sans fil (Wi-Fi)**.
3. Dans le groupe **Réglages des réseaux sans fil**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Réseau sans fil** s'ouvre.
4. Dans le champ **SSID réseau**, saisissez le nom du réseau sans fil contenant le point d'accès (SSID).
5. Pour que le périphérique MDM iOS se connecte automatiquement au réseau sans fil, cochez la case **Connexion automatique**.
6. Pour que le réseau sans fil n'apparaisse pas dans la liste des réseaux disponibles sur le périphérique MDM iOS, cochez la case **Réseau masqué**.

   Dans ce cas, pour se connecter au réseau l'utilisateur devra saisir manuellement sur le périphérique 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 :

   - **Aucun**. 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 **Tout (d'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 du périphérique iOS MDM sur les serveurs de confiance.

8. Configurez le compte pour l'authentification de l'utilisateur lors de la connexion du périphérique 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. Pour imposer à l'utilisateur la saisie manuelle d'un mot de passe à chaque 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 d'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 139).

f. Dans le champ **Identifiant 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 le périphérique 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 **Paramètres**.

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 du périphérique au réseau sans fil via le serveur proxy seront ainsi configurés sur le périphérique 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 le périphérique iOS MDM de l'utilisateur une fois la stratégie appliquée. le périphérique 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 données de l'utilisateur à 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 108), 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 périphériques MDM iOS.
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Réseau sans fil (Wi-Fi)**.
3. Dans le groupe **Réglages 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 **Paramètres**.

   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 :
   - Pour utiliser une clé cryptographique PAC (Protected Access Credential) pour l'identification de l'utilisateur, cochez la case **Utiliser le PAC (Protected Access Credential)**.
   - Pour préparer une clé PAC pour l'identification de l'utilisateur selon le protocole EAP-FAST, cochez la case **Autoriser l'approvisionnement automatique du PAC**.
   - Pour 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 le périphérique 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 108), il est recommandé de créer une liste des certificats de confiance pour l'authentification de l'utilisateur du périphérique 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 périphériques MDM iOS.
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Réseaux sans fil (Wi-Fi)**.
3. Dans le groupe **Réglages 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 **Paramètres**.
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 serveurs 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 le périphérique iOS MDM.

Configuration de la connexion VPN

Afin de connecter le périphérique 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 le périphérique iOS MDM, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des périphériques MDM iOS.
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 périphériques SonicWALL™ Aventail E-Class Secure Remote Access version 10.5.4 et suivantes, les périphériques SonicWALL SRA version 5.5 et suivantes ainsi que les périphériques 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**, saisissez le nom du compte utilisateur pour l'autorisation sur le serveur VPN. Vous pouvez utiliser les macros de la liste déroulante **Macros disponibles**.

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 du périphérique au réseau VPN via le serveur proxy seront ainsi configurés sur le périphérique 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 le périphérique 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 périphériques MDM iOS.
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 du périphérique 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 SecurID et d'une clé commune. L'authentification de l'utilisateur requiert la définition de la clé dans le champ **Clé partagée**.
   - **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. Pour 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 périphériques MDM iOS.
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 du périphérique 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 SecurID 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. Pour 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 périphériques MDM iOS.
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 du périphérique 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 **Général**, cochez/décochez la case **Demander le code PIN**.
   - Sous l'onglet **Paramètres avancés** :
     - **Certificats** ;
     - **Activer le VPN lors de la connexion des domaines** ;
     - **Délai d'inactivité jusqu'à la 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 périphériques MDM iOS.
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 **Auth. des utilisateurs**, sélectionnez le type d'authentification de l'utilisateur du périphérique 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** ;
     - **Délai d'inactivité jusqu'à la 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 périphériques MDM iOS.
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 **Portée**, saisissez le nom du réseau où se trouvent les serveurs VPN et les périphériques 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 **Auth. des utilisateurs**, sélectionnez le type d'authentification de l'utilisateur du périphérique 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** ;
     - **Délai d'inactivité jusqu'à la 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 périphériques MDM iOS.
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 **Auth. des utilisateurs**, sélectionnez le type d'authentification de l'utilisateur du périphérique 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** ;
     - **Délai d'inactivité jusqu'à la 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 périphériques MDM iOS.
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 **Auth. des utilisateurs**, sélectionnez le type d'authentification de l'utilisateur du périphérique 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** ;
     - **Délai d'inactivité jusqu'à la 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 périphériques MDM iOS.
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 **Auth. des utilisateurs**, sélectionnez le type d'authentification de l'utilisateur du périphérique 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** ;
     - **Délai d'inactivité jusqu'à la 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 périphériques MDM iOS.
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 du périphérique 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 **Auth. des utilisateurs**, sélectionnez le type d'authentification de l'utilisateur du périphérique 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** ;
     - **Délai d'inactivité jusqu'à la 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 périphériques iOS MDM vers un périphérique AirPlay, il convient de configurer la connexion automatique aux appareils AirPlay. Pour pouvoir utiliser la technologie AirPlay, le périphérique mobile et le périphérique 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 périphériques contrôlés.

► *Pour configurer la connexion du périphérique iOS MDM aux appareils AirPlay, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des périphériques MDM iOS.
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 du périphérique AirPlay sur le réseau sans fil.
6. Dans la colonne **Mot de passe**, saisissez le mot de passe du périphérique AirPlay.
7. Pour restreindre la connexion du périphérique MDM iOS aux appareils AirPlay, créez la liste des périphériques autorisés dans le groupe **Appareils autorisés**. Pour ce faire, ajoutez les adresses MAC des périphériques AirPlay à la liste des périphériques autorisés.

   L'accès aux appareils AirPlay ne figurant pas dans la liste des périphériques autorisés est interdit. Si la liste des périphériques autorisés est laissée vide, Kaspersky Mobile Device Management autorise l'accès à tous les périphériques AirPlay.
8. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées.

le périphérique 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 à une imprimante AirPrint

Afin d'imprimer des documents depuis le périphérique iOS MDM à l'aide de la technologie sans fil AirPrint, il convient de configurer la connexion automatique aux imprimantes AirPrint. Le périphérique 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 du périphérique iOS MDM à une imprimante AirPrint, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des périphériques MDM iOS.
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 de 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 du périphérique mobile pourra ainsi imprimer des documents sur une imprimante AirPrint via une connexion sans fil une fois la stratégie appliquée.

Ajout d'un compte email

Afin de permettre à l'utilisateur du périphérique 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 sortants du périphérique 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 du périphérique iOS MDM, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des périphériques MDM iOS.
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **E-mail**.
3. Dans le groupe **Comptes de messagerie électronique**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Compte de messagerie électronique** s'ouvre.
4. Dans le champ **Description du compte**, 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 d'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 email**, saisissez l'adresse électronique de l'utilisateur du périphérique iOS MDM.

9. Configurez les paramètres avancés du compte de messagerie électronique :

   - Pour autoriser l'utilisateur à transférer les messages électroniques d'un de ses comptes utilisateur à un autre, cochez la case **Autoriser le déplacement des messages entre les comptes**.
   - Pour autoriser la synchronisation des adresses email utilisées entre les comptes, cochez la case **Autoriser la synchronisation des dernières adresses utilisées**.
   - Pour autoriser l'utilisateur à employer uniquement le client de messagerie iOS standard, cochez la case **Autoriser l'utilisation de Mail uniquement**.
   - Pour 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 **Paramètres** 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** : 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 le périphérique mobile de l'utilisateur à partir de la liste créée une fois la stratégie appliquée.

Ajout d'un compte Exchange ActiveSync

Afin de permettre à l'utilisateur du périphérique 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 du périphérique 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 du périphérique iOS MDM, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des périphériques MDM iOS.
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 **Général**.
4. Dans le champ **Nom du compte**, saisissez le nom du compte utilisateur pour l'autorisation sur le serveur Microsoft Exchange. Vous pouvez utiliser les macros de la liste déroulante **Macros disponibles**.
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 du périphérique iOS MDM. Vous pouvez utiliser les macros de la liste déroulante **Macros disponibles**.
8. Dans le champ **Utilisateur du compte**, saisissez le nom de l'utilisateur du périphérique 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 le périphérique iOS MDM. Vous pouvez utiliser les macros de la liste déroulante **Macros disponibles**.
9. Dans le champ **Adresse email**, saisissez l'adresse électronique de l'utilisateur du périphérique iOS MDM. Vous pouvez utiliser les macros de la liste déroulante **Macros disponibles**.
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 Exchange ActiveSync :

    - **Synchroniser l'e-mail 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 le périphérique 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 du périphérique 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 du périphérique iOS MDM, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des périphériques MDM iOS.
2. Dans la fenêtre **Propriétés de <nom de la stratégie>** qui s'ouvre, sélectionnez la section **LDAP**.

3. Dans le groupe **Comptes LDAP**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Compte LDAP et paramètres de la recherche** s'ouvre.

4. Dans le champ **Description du compte**, saisissez la description du compte LDAP de l'utilisateur. Vous pouvez utiliser les macros de la liste déroulante **Macros disponibles**.

5. Dans le champ **Nom du compte**, saisissez le nom du compte utilisateur pour l'autorisation sur le serveur LDAP. Vous pouvez utiliser les macros de la liste déroulante **Macros disponibles**.

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 **Macros disponibles**.

8. Pour 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 du périphérique 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 **Niveau de 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-arborescence**: recherche dans les dossiers de tous les niveaux d'imbrication à partir du dossier de base.

d. Dans la colonne **Base de 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 au périphérique 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 le périphérique 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 du périphérique 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 du périphérique iOS MDM, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des périphériques MDM iOS.

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

3. Dans le groupe **Comptes CalDAV**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Compte CalDAV** s'ouvre.

4. Dans le champ **Description du compte**, saisissez la description du compte CalDAV de l'utilisateur. Vous pouvez utiliser les macros de la liste déroulante **Macros disponibles**.

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'adresse Internet du compte CalDAV de l'utilisateur du périphérique 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**, indiquez le nom du compte utilisateur pour l'autorisation sur le serveur CalDAV. Vous pouvez utiliser les macros de la liste déroulante **Macros disponibles**.

8. Dans le champ **Mot de passe du compte**, indiquez le mot de passe du compte utilisateur CalDAV pour l'autorisation sur le serveur CalDAV.

9. Pour utiliser le protocole de transfert de données SSL afin de protéger le transfert de données sur les événements entre le serveur CalDAV et le périphérique 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 le périphérique 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 du périphérique 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 du périphérique iOS MDM, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des périphériques MDM iOS.
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Contacts**.
3. Dans le groupe **Comptes CardDAV**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Compte CardDAV** s'ouvre.
4. Dans le champ **Description du compte**, saisissez la description du compte CardDAV de l'utilisateur. Vous pouvez utiliser les macros de la liste déroulante **Macros disponibles**.
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'adresse Internet du compte CardDAV de l'utilisateur du périphérique 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**, indiquez le nom du compte utilisateur pour l'autorisation sur le serveur CardDAV. Vous pouvez utiliser les macros de la liste déroulante **Macros disponibles**.
8. Dans le champ **Mot de passe du compte**, indiquez le mot de passe du compte utilisateur CardDAV pour l'autorisation sur le serveur CardDAV.
9. Pour utiliser le protocole de transfert de données SSL afin de protéger le transfert de contacts entre le serveur CardDAV et le périphérique 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 le périphérique mobile de l'utilisateur à partir de la liste créée une fois la stratégie appliquée.

Configuration de l'abonnement à un calendrier

Afin que l'utilisateur du périphérique 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 de 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 périphériques MDM iOS.
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 **Macros disponibles**.
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 **Macros disponibles**.
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. Pour utiliser le protocole de transfert de données SSL afin de protéger le transfert de données sur les événements entre le serveur CalDAV et le périphérique 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 du périphérique mobile de l'utilisateur à partir de la liste créée une fois la stratégie appliquée.

Ajout de clips Internet

Un *clip Internet* est une application qui ouvre un site Internet depuis l'écran principal du périphérique mobile. En cliquant sur l'icône des clips Internet sur l'écran principal du périphérique, l'utilisateur peut rapidement ouvrir des sites Internet (tels que le site de l'entreprise). Vous pouvez ajouter des clips Internet sur les périphériques 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 clips Internet :

- L'utilisateur ne peut pas supprimer lui-même les clips Internet du périphérique mobile.
- Les sites Internet qui s'ouvrent en cliquant sur l'icône du clip 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 clip Internet sur l'écran.

► *Pour ajouter un clip Internet au périphérique iOS MDM de l'utilisateur, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des périphériques MDM iOS.
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Clips Internet**.
3. Dans le groupe **Paramètres des clips Internet**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Clips Internet** s'ouvre.

4. Dans le champ **Nom**, saisissez le nom du clip Internet qui s'affichera sur l'écran principal du périphérique iOS MDM.

5. Dans le champ **URL**, saisissez l'adresse du site Internet qui s'ouvrira si vous cliquez sur l'icône du clip Internet. L'adresse du site Internet doit commencer par "http://" ou "https://".

6. Pour autoriser à l'utilisateur à supprimer un clip Internet du périphérique MDM iOS, cochez la case **Autoriser la suppression**.

7. Cliquez sur le bouton **Sélectionner** et indiquez le fichier contenant l'image pour l'icône du clip Internet.

   L'icône s'affichera sur l'écran principal du périphérique 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 clip 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 clip Internet s'affiche sans effet graphique particulier (arrondissement des coins de l'icône et effet de brillance), cochez la case **Clip Internet sans effet visuels**.

9. Si vous souhaitez qu'en cas de pression sur l'icône le site Internet s'ouvre sur toute la surface de l'écran du périphérique iOS MDM, cochez la case **Clip Internet en plein écran**.

10. Cliquez sur le bouton **OK**.

    Le nouveau clip Internet s'affichera dans la liste.

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

Les icônes des clips Internet seront ainsi ajoutés à l'écran principal du périphérique mobile de l'utilisateur à partir de la liste créée une fois la stratégie appliquée.

Ajout de polices d'écriture

► *Pour ajouter une police d'écriture au périphérique iOS MDM de l'utilisateur, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des périphériques MDM iOS.
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 le périphérique mobile à partir de la liste créée une fois la stratégie appliquée.

Ajout de certificats de sécurité

Afin de faciliter l'authentification de l'utilisateur et d'assurer la sécurité des données, il convient d'ajouter des certificats au périphérique 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 au périphérique iOS MDM de l'utilisateur, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des périphériques MDM iOS.
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Certificats**.
3. Dans le groupe **Réglages 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 le périphérique mobile à partir de la liste créée une fois la stratégie appliquée.

Configuration du profil SCEP

Afin de permettre à l'utilisateur du périphérique 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 périphériques MDM iOS.
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'adresse Internet 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 du périphérique 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 :

   - **Non** : l'identification par un nom alternatif n'est pas utilisée.
   - **Nom RFC 822** : identification en fonction de l'adresse de messagerie électronique. L'adresse email 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 du périphérique 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 email de l'utilisateur, domaine ou URL.

9. Dans le champ **Nom du sujet NT**, saisissez le nom DNS de l'utilisateur du périphérique 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 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'inscription**, 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 **Dimension de 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 comme signature numérique**.

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 digitale 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 le périphérique mobile de l'utilisateur une fois la stratégie appliquée.

Configuration du point d'accès (APN)

Afin de permettre à l'utilisateur du périphérique 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 le périphérique iOS MDM de l'utilisateur, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés de la stratégie d'administration des périphériques MDM iOS.
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 (APN)**, 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 d'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 et port du serveur proxy**, 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 le périphérique mobile de l'utilisateur une fois la stratégie appliquée.

Participation au Kaspersky Security Network

Cette section contient des informations relatives à la participation au Kaspersky Security Network et explique comment activer ou désactiver l'utilisation de Kaspersky Security Network.

Dans cette section

Présentation de la participation au Kaspersky Security Network

Pour renforcer l'efficacité de la protection des périphériques mobiles, Kaspersky Endpoint Security for Android et Kaspersky Safe Browser utilisent des données fournies par des utilisateurs du monde entier. Le réseau *Kaspersky Security Network* permet de traiter ces données.

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

Votre participation au Kaspersky Security Network permet à Kaspersky Lab d'obtenir efficacement des informations sur les types et les sources des nouvelles menaces, de développer des outils de neutralisation et de réduire le nombre de faux positifs de Kaspersky Endpoint Security for Android et Kaspersky Safe Browser. De plus, la participation au Kaspersky Security Network donne accès aux données sur la réputation des applications et des sites Internet.

Si vous participez au Kaspersky Security Network, certaines statistiques obtenues lors du fonctionnement de Kaspersky Endpoint Security for Android et Kaspersky Safe Browser sur l'ordinateur de l'utilisateur sont envoyées automatiquement à Kaspersky Lab" (cf. section "Echange des informations avec Kaspersky Security Network" à la page 146). Ces informations permet de suivre les menaces en temps réel. De même, des fichiers (ou des parties de ceux-ci) qui pourraient être utilisés par des individus malintentionnés pour nuire l'ordinateur ou aux données de l'utilisateur, peuvent être envoyés à Kaspersky Lab pour une analyse complémentaire.

La participation au Kaspersky Security Network est volontaire. Afin de pouvoir utiliser le Kaspersky Security Network, vous devez accepter les dispositions reprises dans la Déclaration de Kaspersky Security Network. Vous pouvez vous retirer à tout moment du Kaspersky Security Network (cf. section "Activation et désactivation de l'utilisation de Kaspersky Security Network" à la page 148). Kaspersky Security Network ne collecte, ne traite et ne conserve aucune donnée personnelle de l'utilisateur. La Déclaration de Kaspersky Security Network présente les types de données que Kaspersky Endpoint Security for Android et Kaspersky Safe Browser transmettent au Kaspersky Security Network. Vous pouvez utiliser les services de Kaspersky Security Network si la durée de validité de la licence de la suite logicielle n'a pas expiré et si la clé ne figure pas dans la liste noire.

Echange des informations avec Kaspersky Security Network

Kaspersky Security Network (KSN) 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 utilise Kaspersky Security Network pendant le fonctionnement des composants suivants :

- Analyse : les applications mobiles Kaspersky Endpoint Security effectuent une analyse supplémentaire des applications installées avant leur premier lancement. De nouvelles menaces dont les informations n'ont pas encore été ajoutées aux bases antivirus peuvent être détectée pendant l'analyse d'une application.

- Protection Internet : les applications mobiles Kaspersky Endpoint Security exécutent une analyse supplémentaire des sites Internet avant leur ouverture.

Le Contrat de Licence Utilisateur Final détaille la nature des données transmises à Kaspersky Lab lorsque le KSN est utilisé parallèlement aux applications mobiles Kaspersky Endpoint Security sur les périphériques 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 périphériques 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 du périphérique mobile ;
- Les données statistiques sur les menaces détectées.

Les informations transmises au KSN ne contiendront pas de données personnelles ni d'autres informations confidentielles de l'utilisateur.

Les informations obtenues par 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 Kaspersky Security Network, reportez-vous au site Internet http://support.kaspersky.com/fr/.

Activation et désactivation de l'utilisation de Kaspersky Security Network

Kaspersky Security Network est utilisé par les composants suivants de Kaspersky Endpoint Security for Android :

- Anti-Virus (protection cloud) ;
- Protection Internet ;
- Contrôle des applications (catégories d'applications).

Kaspersky Security Network est utilisé par le composant Protection Internet de Kaspersky Safe Browser.

Si l'utilisation de Kaspersky Security Network est désactivée sur le périphérique, les composants Protection cloud, Protection Internet et Contrôle des applications sont automatiquement désactivés.

► *Pour activer ou désactiver l'utilisation de Kaspersky Security Network, procédez comme suit :*

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des périphériques mobiles sur lesquels Kaspersky Endpoint Security for Android ou Kaspersky Safe Browser sont installés.
2. Dans la fenêtre **Propriétés de <nom de la stratégie>**, sélectionnez la section **Paramètres avancés**.

3. Réalisez une des opérations suivantes dans le groupe **Paramètres d'utilisation de Kaspersky Security Network** :

   - Cochez la case**Autoriser l'utilisation de Kaspersky Security Network** pour activer l'utilisation de Kaspersky Security Network.

   - Décochez la case **Autoriser l'utilisation de Kaspersky Security Network** pour désactiver l'utilisation de Kaspersky Security Network.

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

Les paramètres sur le périphérique mobile seront configurés après la prochaine synchronisation du périphérique avec le Serveur d'administration. Une fois que la stratégie aura été appliquée, les modules qui utilisent Kaspersky Security Network seront désactivés et la configuration des modules sera impossible.

Appendice 1. Autorisations de configuration des stratégies de groupe

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.

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.

Tableau 2. Autorisations d'accès aux sections du plug-in d'administration de Kaspersky Endpoint Security

Zone opérationnelle	Section Stratégies
Antivol	Antivol
Contrôle des applications	Contrôle des applications, Applications tierces
Protection	Protection, Analyse, Mise à jour
Contrôle de la conformité	Contrôle de la conformité
Conteneurs	Conteneurs
Paramètres du périphérique	Gestion de l'appareil, Synchronisation

Zone opérationnelle	Section Stratégies
Administration des périphériques Samsung	Paramètres généraux, Paramètres de KNOX 1, Paramètres de KNOX 2
Administration du système	Paramètres avancés, Section Réseaux sans fil (Wi-Fi)
Protection Internet	Protection Internet

Tableau 3. Autorisations d'accès aux plug-in d'administration de Kaspersky Mobile Device Management

Zone opérationnelle	Section Stratégies
Avancé	Clips Internet, Polices, AirPlay, AirPrint
Exchange ActiveSync	Généraux, Mot de passe, Synchronisation, Restrictions des fonctions, Restrictions des applications
Général	Généraux, Compte utilisateur unique, Protection Internet, Réseaux sans fil (Wi-Fi), Point d'accès (APN), Exchange ActiveSync, Courrier électronique, Paramètres de configuration
LDAP (calendriers/contacts)	LDAP, Calendrier, Contacts, Abonnements à un calendrier
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

Appendice 2. Restrictions pour les périphériques iOS MDM

Kaspersky Mobile Device Management prend en charge l'administration des paramètres des périphériques iOS MDM qui peuvent être configurés selon la stratégie de sécurité de l'entreprise.

Restrictions des fonctions :

- **Autoriser l'utilisation de la caméra**

  Utilisation du périphérique photo sur le périphérique mobile de l'utilisateur.

  Quand la case est cochée, l'utilisateur peut utiliser le périphérique photo du périphérique mobile.

  Si la case est décochée, le périphérique photo du périphérique mobile de l'utilisateur est désactivé. L'utilisateur ne peut prendre aucune photo ou vidéo. Il ne peut pas non plus utiliser l'application FaceTime. L'icône du périphérique photo disparaît de l'écran principal du périphérique.

  Cette case est cochée par défaut.

- **Autoriser FaceTime**

  Utilisation de l'application FaceTime sur le périphérique mobile de l'utilisateur. La case est accessible si l'utilisation de l'appareil photo est autorisée sur l'appareil mobile. Ce paramètre est accessible si la case **Autoriser l'utilisation de la caméra** est cochée.

  Si la case est cochée, l'utilisateur peut émettre et recevoir des appels vidéo avec FaceTime.

  Si la case est décochée, l'application FaceTime est désactivée sur le périphérique mobile de l'utilisateur. L'utilisateur ne peut pas émettre ou recevoir d'appels vidéo.

  Cette case est cochée par défaut.

- **Autoriser les aperçus**

  Possibilité de réaliser des aperçus sur le périphérique mobile iOS MDM.

  Si la case est cochée, l'utilisateur peut réaliser et enregistrer des aperçus sur le périphérique mobile.

  Si la case est décochée, l'utilisateur ne peut pas réaliser et enregistrer des aperçus sur le périphérique mobile.

  Cette case est cochée par défaut.

- **Autoriser AirDrop** (uniquement pour les périphériques contrôlés)

  Utilisation de la fonction AirDrop pour la transmission des données de l'utilisateur depuis un périphérique mobile iOS MDM vers un autre périphérique Apple.

  Si la case est cochée, l'utilisateur peut utiliser AirDrop pour la transmission de données vers un autre périphérique Apple.

  Si la case est décochée, l'utilisateur n'est pas autorisé à transmettre des données à d'autres périphériques Apple à l'aide d'AirDrop.

  Cette case est cochée par défaut.

- **Autoriser iMessage** (uniquement pour les périphériques contrôlés)

  Utilisation du service iMessage sur le périphérique mobile de l'utilisateur.

  Si la case est cochée, l'utilisateur peut envoyer et recevoir des messages avec le service iMessage.

  Si la case est décochée, le service iMessage n'est pas accessible sur le périphérique mobile. L'utilisateur ne peut pas envoyer ou recevoir de messages iMessage.

  Cette case est cochée par défaut.

- **Autoriser la composition vocale**

  Utilisation de la fonction de composition vocale sur le périphérique mobile de l'utilisateur.

  Si la case est cochée, l'utilisateur peut utiliser la commande vocale pour composer des numéros de téléphone.

Si la case est décochée, l'utilisateur ne peut pas utiliser la commande vocale pour composer des numéros de téléphone.

Cette case est cochée par défaut.

- **Autoriser l'utilisation de Siri**

  Utilisation de l'application Siri sur le périphérique mobile de l'utilisateur.

  Si la case est cochée, l'utilisateur peut utiliser la commande vocale de l'application Siri sur le périphérique.

  Si la case est décochée, l'utilisateur ne peut pas utiliser la commande vocale Siri sur le périphérique.

  Cette case est cochée par défaut.

- **Autoriser le filtre de vulgarité** (uniquement pour les périphériques contrôlés)

  Filtrage du langage vulgaire lors de l'utilisation de l'application Siri sur le périphérique mobile de l'utilisateur.

  Si la case est cochée, la vulgarité n'est pas filtrée lors de l'utilisation de Siri.

  Si la case est décochée, la vulgarité n'est pas filtrée lors de l'utilisation de Siri.

  Cette case est cochée par défaut.

- **Autoriser quand l'appareil est verrouillé**

  Utilisation de la commande vocale Siri lorsque le périphérique mobile de l'utilisateur est verrouillé. Un mot de passe doit être installé sur le périphérique mobile de l'utilisateur. Ce paramètre est accessible si la case **Autoriser l'utilisation de Siri** est cochée.

  Si la case est cochée, l'utilisateur peut utiliser la commande vocale Siri sur le périphérique mobile verrouillé.

  Si la case est décochée, l'utilisateur n'est pas autorisé à utiliser la commande vocale Siri sur le périphérique verrouillé.

  Cette case est cochée par défaut.

- **Afficher les données de l'utilisateur** (uniquement pour les périphériques contrôlés)

  Ajout de données personnelles à Siri pour pouvoir les utiliser avec la commande vocale Siri (par exemple, "Rappelle-moi d'appeler ma femme lorsque j'arrive à la maison") sur le périphérique mobile iOS MDM. Ce paramètre est accessible si la case **Autoriser l'utilisation de Siri** est cochée.

  Si la case est cochée, l'utilisateur peut remplir sa carte personnelle dans les paramètres de Siri et utiliser ces données pour la commande vocale Siri.

  Si la case est décochée, l'utilisateur n'est pas autorisé à ajouter ses données personnelles dans Siri.

  Cette case est cochée par défaut.

- **Autoriser iBooks Store** (uniquement pour les périphériques contrôlés)

  Accès à la boutique en ligne iBooks Store à partir de l'application iBooks sur le périphérique mobile de l'utilisateur.

  Si la case est cochée, l'utilisateur peut se rendre sur la boutique en ligne iBookStore à partir de l'application iBooks installée sur le périphérique.

  Si la case est décochée, l'utilisateur ne peut pas se rendre sur iBookStore à partir de l'application iBooks.

  Cette case est cochée par défaut.

- **Autoriser l'installation des applications**

  Possibilité d'installer soi-même des applications sur le périphérique mobile iOS MDM.

  Si la case est cochée, l'utilisateur peut installer ou mettre à jour lui-même des applications de l'App Store ou d'iTunes.

  Si la case est décochée, l'utilisateur ne peut pas installer ou mettre à jour lui-même des applications de l'App Store ou d'iTunes sur le périphérique mobile. Le raccourci App Store disparaît de l'écran principal du périphérique mobile iOS MDM.

  Cette case est cochée par défaut.

- **Autoriser la suppression d'applications** (uniquement pour les périphériques contrôlés)

  Possibilité de supprimer des applications du périphérique mobile.

  Si la case est cochée, l'utilisateur peut supprimer les applications qui ont été installées à partir de l'App Store ou d'iTunes du périphérique.

  Si la case est décochée, l'utilisateur ne peut pas supprimer les applications qui ont été installées à partir de l'App Store ou d'iTunes du périphérique mobile.

  Cette case est cochée par défaut.

- **Autoriser les Achats intégrés**

  Utilisation du système in-App Purchase sur le périphérique mobile.

  Si la case est cochée, l'utilisateur peut effectuer des achats dans les applications installées sur le périphérique mobile.

  Si la case est décochée, l'utilisateur ne peut pas effectuer d'achats dans les applications installées sur le périphérique mobile.

  Cette case est cochée par défaut.

- **Demander le mot de passe lors de chaque achat sur iTunes Store**

  Utilisation du mot de passe des restrictions lors de l'achat de contenu multimédia dans l'iTunes Store.

  Si la case est cochée, l'utilisateur doit définir un mot de passe des restrictions dans les paramètres de restriction des achats avant le premier achat dans l'iTunes Store. Il devra ensuite l'utiliser pour éviter les achats non souhaités ou non autorisés. Suite à la vérification de l'authenticité du compte utilisateur, chaque achat est suivi d'une période de 15 minutes pendant laquelle il n'est plus nécessaire de saisir le mot de passe de restriction.

  Si la case est décochée, l'utilisateur n'est pas obligé de saisir un mot de passe de restriction avant d'effectuer un achat sur l'iTunes Store.

  Cette case est décochée par défaut.

- **Autoriser la sauvegarde iCloud**

  Copie de sauvegarde automatique des données depuis le périphérique mobile iOS MDM dans iCloud. Le processus de copie de sauvegarde ne copie pas les données déjà enregistrées dans iCloud. De même, le contenu multimédia obtenu suite à la synchronisation du périphérique avec un ordinateur plutôt que sur l'iTunes Store n'est pas copié non plus.

  Si la case est cochée, l'utilisateur peut enregistrer une copie de sauvegarde des données du périphérique mobile dans iCloud. Les copies de sauvegarde sont enregistrées quotidiennement dans iCloud lorsque le périphérique est allumé, verrouillé ou branché à une source d'alimentation.

  Si la case est décochée, l'utilisateur n'est pas autorisé à enregistrer une copie de sauvegarde des données du périphérique mobile dans iCloud.

  Cette case est cochée par défaut.

- **Autoriser la conservation des documents et des données dans iCloud**

  Copie de sauvegarde automatique des documents dans iCloud. Les documents iCloud peuvent être ouverts et modifiés sur d'autres périphériques dotés du service iCloud.

  Si la case est cochée, l'utilisateur peut enregistrer ses documents dans iCloud, puis les ouvrir et les modifier sur d'autres périphériques dans les applications prenant en charge l'utilisation d'iCloud (par exemple, dans TextEdit).

  Si la case est décochée, l'utilisateur n'est pas autorisé à enregistrer des documents dans iCloud.

  Cette case est cochée par défaut.

- **Autoriser le Trousseau iCloud**

  Synchronisation automatique des données des comptes de l'utilisateur du périphérique mobile iOS MDM avec les autres périphériques Apple du périphérique. Les données de synchronisation sont stockées dans le Trousseau iCloud. Les données du Trousseau iCloud sont chiffrées. Le Trousseau iCloud permet d'enregistrer les données suivantes dans iCloud :

  - comptes utilisateur des sites Internet ;
  - numéros de cartes bancaires et leur date d'expiration ;
  - mots de passe des réseaux sans fil.

Si la case est cochée, l'utilisateur peut synchroniser les données de ses comptes utilisateur avec ses autres périphériques Apple.

Si la case est décochée, l'utilisateur n'est pas autorisé à utiliser le Trousseau iCloud sur le périphérique mobile.

Cette case est cochée par défaut.

- **Autoriser l'Accès au partage aux photos dans iCloud**

  Utilisation de la fonction Partage des photos iCloud sur le périphérique mobile iOS MDM pour permettre à d'autres utilisateurs d'accéder aux photos et vidéos sur le serveur iCloud. Les autres utilisateurs doivent être dotés de la fonction Partage des photos iCloud.

  Si la case est cochée, l'utilisateur du périphérique mobile peut accéder à la fonction Partage des photos iCloud. Les utilisateurs d'autres périphériques peuvent consulter les photos et vidéo de l'utilisateur, laisser des commentaires et ajouter leurs photos et vidéo. De même, l'utilisateur peut obtenir un accès aux données d'autres utilisateurs sur le serveur iCloud.

  Si la case est décochée, l'utilisateur du périphérique ne peut pas accéder à la fonction Partage des photos iCloud. L'utilisateur ne peut pas partager l'accès à ses photos et vidéos sur le serveur iCloud avec d'autres utilisateurs. Il ne peut pas non plus accéder aux données d'autres utilisateurs sur le serveur iCloud.

  Cette case est cochée par défaut.

- **Autoriser Mon flux de photos**

  Utilisation de la fonction Mon flux de photos pour l'envoi automatique des photos et vidéos prises depuis le périphérique mobile iOS MDM sur d'autres périphériques Apple. Les photos et vidéos sont stockées dans le dossier "Mon flux de photos" sur le serveur iCloud pendant 30 jours.

  Si la case est cochée, l'utilisateur peut accéder à la fonction Mon flux de photos lors de l'utilisation des applications iPhoto ou Aperture.

  Si la case n'est pas cochée, l'utilisateur ne peut pas accéder à la fonction Mon flux de photos. Les photos et vidéos de l'utilisateur enregistrées dans le dossier "Mon flux de photos" sont supprimées du serveur iCloud.

  Cette case est cochée par défaut.

- **Autoriser la synchronisation automatique en itinérance**

  Synchronisation automatique des données lorsque le périphérique mobile iOS MDM se trouve en itinérance.

  Si la case est cochée, l'utilisateur peut activer la synchronisation automatique des données en itinérance. L'activation de la synchronisation automatique en itinérance peut entraîner des dépenses non provisionnées en communications mobiles.

  Si la case est décochée, l'utilisateur n'est pas autorisé à utiliser la synchronisation automatique des données en itinérance.

  Cette case est décochée par défaut.

- **Activer le chiffrement des copies de sauvegarde**

  Chiffrement de la copie de sauvegarde des données du périphérique mobile iOS MDM dans l'application iTunes sur l'ordinateur de l'utilisateur. Le chiffrement des données de la stratégie de configuration de Kaspersky Mobile Device Management ne s'exécute pas, que le chiffrement de la copie de sauvegarde soit activé ou non.

  Si la case est cochée, les données sont chiffrées et protégées par un mot de passe dès la création d'une copie de sauvegarde des données du périphérique mobile dans l'application iTunes.

  Si la case est décochée, l'utilisateur peut choisir comment utiliser le chiffrement de la copie de sauvegarde des données dans l'application iTunes.

  Cette case est décochée par défaut.

- **Limiter le suivi de la publicité**

  Utilisation de la technologie IFA (Identifier for advertisers) pour le suivi des sites Internet ouverts et des applications lancées sur le périphérique mobile iOS MDM. IFA permet de configurer le cheminement de la publicité sur le périphérique mobile en fonction des centres d'intérêt de l'utilisateur.

  Si la case est cochée, la technologie IFA est désactivée sur le périphérique mobile de l'utilisateur.

Si la case est décochée, la technologie IFA est activée sur le périphérique mobile et suit les sites Internet ouverts et les applications lancées pour l'affichage de publicités ciblées.

Cette case est décochée par défaut.

- **Autoriser l'utilisation des certificats TLS non approuvés**

  Utilisation de certificats TLS douteux pour l'établissement d'un canal de communication chiffré entre les applications du périphérique mobile iOS MDM (Mail, Contacts, Calendrier, Safari) et les ressources de l'entreprise.

  Si la case est cochée, l'utilisation d'un certificat TLS douteux peut être acceptée après l'affichage d'un avertissement.

  Si la case est décochée, Kaspersky Mobile Device Management interdit automatiquement l'utilisation de certificats TLS douteux.

  Cette case est cochée par défaut.

- **Autoriser la mise à jour automatique des certificats de confiance**

  Mise à jour automatique des certificats de confiance sur le périphérique mobile iOS MDM.

  Si la case est cochée, Kaspersky Mobile Device Management applique automatiquement les modifications dans les paramètres de confiance du certificat.

  Si la case est décochée, les modifications des paramètres de confiance du certificat ne sont pas appliquées automatiquement. Après avertissement, l'utilisateur peut appliquer lui-même les modifications dans les paramètres de confiance du certificat.

  Cette case est cochée par défaut.

- **Autoriser l'installation des profils de configuration** (uniquement pour les périphériques contrôlés)

  Application de profils de configuration supplémentaires, excepté les stratégies Kaspersky Security Center, sur le périphérique mobile iOS MDM.

  Si la case est cochée, l'utilisateur peut installer des profils de configuration supplémentaires sur le périphérique mobile.

Si la case est décochée, l'utilisateur ne peut pas installer de profils de configuration supplémentaires (sauf la stratégie Kaspersky Security Center) sur le périphérique mobile.

Cette case est cochée par défaut.

- **Autoriser la modification des paramètres du compte utilisateur** (uniquement pour les périphériques contrôlés)

  Possibilité d'ajouter de nouveaux comptes utilisateur sur le périphérique mobile iOS MDM (par exemple, des comptes de messagerie électronique) et d'en modifier les paramètres.

  Si la case est cochée, l'utilisateur du périphérique mobile peut ajouter de nouveaux comptes utilisateur et modifier les paramètres de ceux existants.

  Si la case est décochée, l'utilisateur du périphérique mobile n'est pas autorisé à ajouter de nouveaux comptes utilisateur et à modifier les paramètres de ceux existants.

  Cette case est cochée par défaut.

- **Autoriser la modification des paramètres de la fonction Localiser mes amis** (uniquement pour les périphériques contrôlés)

  Possibilité de modifier les paramètres de l'application Localiser mes amis sur le périphérique mobile iOS MDM.

  Si la case est cochée, l'utilisateur peut modifier les paramètres de l'application Localiser mes amis sur le périphérique mobile.

  Si la case est décochée, l'utilisateur ne peut pas modifier les paramètres définis de l'application Localiser mes amis sur le périphérique mobile.

  Cette case est cochée par défaut.

- **Autoriser les connexions tierces**

  Protection du périphérique mobile iOS MDM contre les connexions tierces. Une *Connexion tierce* est une connexion avec d'autres périphériques ou une synchronisation avec les services Apple, par exemple iTunes.

  Si la case est cochée, l'utilisateur peut synchroniser le périphérique mobile iOS MDM avec d'autres périphériques et avec les services Apple.

Si la case est décochée, Kaspersky Mobile Device Management bloque les connexions tierces sur le périphérique mobile de l'utilisateur.

Cette case est cochée par défaut.

- **Autoriser le transfert des documents depuis les applications contrôlées dans les non contrôlées**

  Possibilité d'ouvrir des documents créés avec des applications et comptes utilisateur administrés (de l'entreprise) dans les applications non-administrées (personnelles) du périphérique mobile iOS MDM. Les *applications administrées* sont des applications installées, configurées et administrées à l'aide de Kaspersky Mobile Device Management.

  Si la case est cochée, l'utilisateur peut ouvrir des documents créés avec des applications administrées dans des applications non-administrées.

  Si la case est décochée, l'utilisateur n'est pas autorisé à ouvrir des documents créés avec des applications administrées dans des applications non-administrées. Par exemple, ce paramètre permet d'éviter l'ouverture d'une pièce jointe confidentielle provenant du compte de messagerie administré dans les applications personnelles de l'utilisateur.

  Cette case est cochée par défaut.

- **Autoriser le transfert des documents depuis les applications non contrôlées dans les contrôlées**

  Possibilité d'ouvrir des documents créés avec des applications et comptes utilisateur non-administrés (personnels) dans les applications administrées (d'entreprise) du périphérique mobile iOS MDM. Les *applications non-administrées* sont des applications installées, configurées et administrées par l'utilisateur du périphérique mobile.

  Si la case est cochée, l'utilisateur peut ouvrir des documents créés avec des applications non-administrées dans les applications administrées.

  Si la case est décochée, l'utilisateur n'est pas autorisé à ouvrir des documents créés avec des applications non-administrées dans des applications administrées. Par exemple, ce paramètre permet d'éviter l'ouverture d'un document à partir d'un compte utilisateur iCloud privé dans les applications d'entreprise.

  Cette case est cochée par défaut.

- **Autoriser l'envoi des données utilisateur et diagnostiques dans Apple**

  Réception automatique d'informations relatives au diagnostic et à l'utilisation du périphérique mobile MDM iOS, et envoi d'un rapport consignant ces informations à l'entreprise Apple pour analyse.

  Si la case est cochée, l'utilisateur peut, après réception d'un avertissement, autoriser l'envoi de rapports reprenant les informations concernant le diagnostic et l'utilisation du périphérique mobile à l'entreprise Apple.

  Si la case est décochée, Kaspersky Mobile Device Management bloque l'envoi de rapports reprenant les informations concernant le diagnostic et l'utilisation du périphérique mobile à l'entreprise Apple.

  Cette case est cochée par défaut.

- **Autoriser Touch ID pour déverrouiller l'appareil**

  Utilisation de la technologie Touch ID permettant d'utiliser les empreintes digitales à la place du mot de passe pour déverrouiller le périphérique mobile iOS MDM.

  Si la case est cochée, l'utilisateur peut utiliser les empreintes digitales au lieu d'un mot de passe pour déverrouiller le périphérique mobile.

  Si la case est décochée, l'utilisateur ne peut pas utiliser la technologie Touch ID pour déverrouiller le périphérique mobile.

  Cette case est cochée par défaut.

- **Exiger un mot de passe pour la première connexion AirPlay**

  Utilisation d'un mot de passe lors de la connexion du périphérique mobile iOS MDM aux périphériques compatibles avec AirPlay. Le mot de passe est appliqué pour assurer la sécurité du transfert du contenu multimédia.

  Si la case est cochée, l'utilisateur doit définir un mot de passe dans les paramètres de sécurité AirPlay avant la première connexion du périphérique aux périphériques compatibles avec cette application. Il devra ensuite utiliser ce mot de passe.

  Si la case est décochée, l'utilisateur décide lui-même s'il souhaite utiliser un mot de passe pour la connexion du périphérique mobile aux périphériques compatibles avec AirPlay.

Cette case est décochée par défaut.

Ce paramètre s'applique uniquement aux appareils mobiles iOS 7.1 ou version suivante.

- **Autoriser Passbook à afficher les notifications sur l'écran verrouillé**

  Utilisation des notifications de l'application Passbook sur l'écran de verrouillage du périphérique mobile iOS MDM.

  Si la case est cochée, les notifications Passbook s'affichent sur l'écran de verrouillage du périphérique mobile.

  Si la case est décochée, les notifications Passbook ne s'affichent pas sur l'écran de verrouillage du périphérique mobile.

  Cette case est cochée par défaut.

- **Afficher le Centre de contrôle quand l'écran est verrouillé**

  Possibilité d'accéder au Centre de contrôle avec le périphérique mobile iOS MDM lorsque ce dernier est verrouillé.

  Si la case est cochée, l'utilisateur peut accéder au Centre de contrôle en faisant glisser l'écran de verrouillage vers le haut.

  Si la case est décochée, l'utilisateur ne peut pas accéder au Centre de contrôle lorsque le périphérique mobile est verrouillé.

  Cette case est cochée par défaut.

- **Afficher le Centre de notifications quand l'écran est verrouillé**

  Possibilité d'accéder au Centre de notifications avec le périphérique mobile iOS MDM lorsque ce dernier est verrouillé.

  Si la case est cochée, l'utilisateur peut accéder au Centre de notifications en faisant glisser l'écran de verrouillage vers le bas.

  Si la case est décochée, l'utilisateur ne peut pas accéder au Centre de notifications lorsque le périphérique mobile est verrouillé.

  Cette case est cochée par défaut.

- **Afficher "Aujourd'hui" sur l'écran verrouillé**

  Affichage des informations de la section "Aujourd'hui" du centre de notifications sur le périphérique mobile iOS MDM verrouillé. La section "Aujourd'hui" du Centre de notifications affiche les informations suivantes :

  - Evénements planifiés dans le calendrier ;
  - rappels ;
  - actions ;
  - météo.

  Si la case est cochée, l'utilisateur peut consulter les notifications de la section "Aujourd'hui" du Centre de notifications sur le périphérique mobile verrouillé.

  Si la case est décochée, la section "Aujourd'hui" ne s'affiche pas sur le périphérique mobile verrouillé.

  Cette case est cochée par défaut.

Restrictions des applications :

- **Autoriser l'utilisation de iTunes Store**

  Accès au service multimédia iTunes Store de l'application iTunes installée sur le périphérique mobile iOS MDM.

  Si la case est cochée, l'utilisateur peut consulter, acheter et télécharger du contenu multimédia à partir du service iTunes Store à l'aide de l'application iTunes sur le périphérique mobile.

  Si la case est décochée, l'utilisateur ne peut pas consulter, acheter et télécharger du contenu multimédia à partir du service iTunes Store à l'aide de l'application iTunes sur le périphérique mobile. Le raccourci iTunes disparaît de l'écran principal du périphérique mobile iOS MDM.

  Cette case est cochée par défaut.

- **Autoriser l'utilisation de Game Center**

  Accès au service de jeu Game Center de l'application Game Center installée sur le périphérique mobile iOS MDM.

Si la case est cochée, l'utilisateur peut utiliser le service de jeu Game Center de l'application Game Center sur le périphérique mobile.

Si la case est décochée, l'utilisateur ne peut pas utiliser le service de jeu Game Center de l'application Game Center sur le périphérique mobile. Le raccourci Game Center disparaît de l'écran principal du périphérique mobile iOS MDM.

Cette case est cochée par défaut.

- **Autoriser l'ajout des amis**

  Ajout d'utilisateurs au service Game Center sur le périphérique mobile iOS MDM.

  Si la case est cochée, l'utilisateur peut ajouter d'autres utilisateurs au service de jeu Game Center sur le périphérique mobile.

  Si la case est décochée, l'utilisateur n'est pas autorisé à ajouter d'autres utilisateurs au service de jeu Game Center sur l'appareil mobile.

  Cette case est accessible si la case **Autoriser l'utilisation de Game Center** est cochée.

  Cette case est cochée par défaut.

- **Autoriser le jeu à plusieurs**

  Utilisation du service de jeu Game Center en mode partagé sur le périphérique mobile iOS MDM.

  Si la case est cochée, l'utilisateur peut participer à des jeux à plusieurs dans l'application Game Center sur le périphérique mobile.

  Si la case est décochée, l'utilisateur ne peut pas participer à des jeux à plusieurs dans l'application Game Center sur le périphérique mobile.

  Cette case est accessible si la case **Autoriser l'utilisation de Game Center** est cochée.

  Cette case est cochée par défaut.

- **Autoriser l'utilisation de Safari**

  Utilisation du navigateur Safari sur le périphérique mobile iOS MDM.

  Si la case est cochée, l'utilisateur peut utiliser le navigateur Safari.

Si la case est décochée, l'utilisateur n'est pas autorisé à utiliser le navigateur Safari. Le raccourci Safari disparaît de l'écran principal du périphérique mobile iOS MDM.

Cette case est cochée par défaut.

- **Activer le remplissage automatique des champs**

  Enregistrement et renseignement automatique des données que l'utilisateur saisit dans les formulaires Internet sur le navigateur Safari.

  Si la case est cochée, Kaspersky Mobile Device Management enregistre les données de l'utilisateur lors du remplissage d'un formulaire Internet. Par la suite, Kaspersky Mobile Device Management renseigne automatiquement les données enregistrées dans les autres formulaires Internet.

  Si la case est décochée, Kaspersky Mobile Device Management ne renseigne pas les données de l'utilisateur lors du remplissage de formulaires Internet.

  Ce paramètre est accessible si la case **Autoriser l'utilisation de Safari** est cochée.

  Cette case est cochée par défaut.

- **Activer la notification sur les site Internet dangereux**

  Avertissement de l'utilisateur avant toute consultation de sites Internet considérés comme dangereux par Kaspersky Mobile Device Management.

  Si la case est cochée, Kaspersky Mobile Device Management avertit l'utilisateur avant l'ouverture d'un site Internet dangereux.

  Si la case est décochée, Kaspersky Mobile Device Management n'avertit pas l'utilisateur avant l'ouverture d'un site Internet dangereux.

  Ce paramètre est accessible si la case **Autoriser l'utilisation de Safari** est cochée.

  Cette case est décochée par défaut.

- **Activer JavaScript**

  Utilisation de JavaScript par le navigateur Safari.

  Si la case est cochée, le navigateur Safari utilise JavaScript lors de l'ouverture de sites Internet.

Si la case est décochée, le navigateur Safari n'utilise pas JavaScript lors de l'ouverture de sites Internet.

Cette case est accessible si la case **Autoriser l'utilisation de Safari** est cochée.

Cette case est cochée par défaut.

- **Bloquer les fenêtres pop-up**

  Blocage des fenêtres pop-up dans le navigateur Safari.

  Si la case est cochée, Kaspersky Mobile Device Management bloque les fenêtres pop-up dans le navigateur Safari.

  Si la case est décochée, Kaspersky Mobile Device Management autorise les fenêtres pop-up dans le navigateur Safari.

  Cette case est accessible si la case **Autoriser l'utilisation de Safari** est cochée.

  Cette case est décochée par défaut.

- **Accepter les cookies**

  Sélection des conditions d'acceptation des fichiers cookie:

  - **Toujours** : le navigateur Safari accepte tous les fichiers cookie.
  - **Uniquement des sites Internet visités** : le navigateur Safari accepte uniquement les fichiers cookie des sites Internet consultés par l'utilisateur.
  - **Jamais** : le navigateur Safari bloque tous les fichiers cookie.

  La valeur par défaut est **Toujours**.

Restrictions du contenu multimédia :

- **Région**

  Sélection du pays du système de classification qui s'applique automatiquement au contenu multimédia sur le périphérique mobile iOS MDM.

  La valeur par défaut est **Etats-Unis**.

- **Films**

  Sélection de la restriction par catégorie pour l'accès aux films sur le périphérique mobile iOS MDM.

  La liste des catégories dépend de la région sélectionnée.

  Si la valeur **Tout autoriser** est sélectionnée, l'utilisateur peut regarder tous les films sur le périphérique mobile.

  La valeur sélectionnée par défaut est **Tout autoriser**.

- **Emissions TV**

  Sélection de la restriction par catégorie pour l'accès aux émissions télévisées sur le périphérique mobile iOS MDM.

  La liste des catégories dépend de la région sélectionnée.

  Si la valeur **Tout autoriser** est sélectionnée, l'utilisateur peut regarder toutes les émissions télévisées sur le périphérique mobile.

  La valeur sélectionnée par défaut est **Tout autoriser**.

- **Applications**

  Sélection de la restriction par catégorie pour l'accès aux applications tierces sur le périphérique mobile iOS MDM.

  La liste des catégories dépend du système de classification sélectionné.

  Si la valeur **Tout autoriser** est sélectionnée, l'utilisateur peut utiliser toutes les applications tierces sur le périphérique mobile.

  La valeur sélectionnée par défaut est **Tout autoriser**.

- **Autoriser la lecture de clips vidéo, de podcasts et de contenu iTunes U comportant du contenu explicite**

  Accès à du contenu multimédia présentant des expressions vulgaires à partir des applications iTunes Store et iTunes U sur le périphérique mobile iOS MDM. Les restrictions sont définies par les fournisseurs iTunes Store et iTunes U.

Si la case est cochée, le contenu comportant du langage vulgaire acheté sur iTunes Store ou iTunes U est accessible à l'utilisateur du périphérique mobile.

Si la case est décochée, le contenu comportant du langage vulgaire acheté sur iTunes Store ou iTunes U est masqué pour l'utilisateur du périphérique mobile.

Cette case est cochée par défaut.

- **Autoriser le contenu réservé aux adultes sur iBooks Store**

  Accès au contenu réservé aux adultes sur la boutique en ligne iBooks Store depuis le périphérique mobile de l'utilisateur.

  Si la case est cochée, l'utilisateur peut télécharger du contenu réservé aux adultes à partir de l'application iBooks sur le périphérique mobile iOS MDM.

  Si la case est décochée, l'utilisateur ne peut pas télécharger du contenu réservé aux adultes à partir de l'application iBooks sur le périphérique mobile iOS MDM.

  Cette case est cochée par défaut.

Appendice 3. Catégories d'applications

Le Contrôle des applications prend en charge le classement des applications par catégorie. Le mode de fonctionnement défini pour une catégorie d'applications sera appliqué à toutes les applications de cette catégorie. La catégorie de chaque application est définie par le service cloud Kaspersky Security Network.

Tableau 4. Catégories d'applications

Catégorie	Description
Divertissements	Applications pour divertissements interactifs.
Clients IM, applications téléphoniques	Applications de messagerie instantanée, de communication audio et vidéo via la téléphonie sur IP.
Réseaux sociaux	Applications destinées à l'utilisation des réseaux sociaux et des blogs.
Applications d'entreprise	Applications pour l'évaluation des taxes, la gestion des opérations bancaires, les tableurs, la comptabilité, et autres applications d'entreprise. Traitements de texte.
Maison, Famille, Hobbies, Santé	Applications proposant des recettes, des conseils de mode. Applications pour le fitness, la création de programmes d'entraînement, les conseils en matière de régime, la santé, l'alimentation, la prévention des accidents, la sécurité au travail.
Médecine	Applications proposant des guides des symptômes et des médicaments, applications destinées aux employés de la santé publique, magazines et actualités de la médecine.
Multimédia	Services d'abonnement à des films, contenus multimédias et lecteurs vidéo. Services d'écoute de musique, lecteurs, radiodiffusion.
Applications pour la photo	Applications de retouche de photos, applications de traitement d'image, applications de gestion et de publication de photos.

Catégorie	Description
Plug-in pour lire les actualités et les flux RSS	Applications destinées à la lecture de journaux, de magazines, de blogs, d'agrégateurs d'actualités.
Météo	Applications destinées à obtenir les prévisions météorologiques.
Applications éducatives	Applications destinées à la lecture de livres, d'ouvrages de référence, de manuels, de dictionnaires, de thésaurus, d'encyclopédies. Applications destinées à la préparation d'examens, documents pédagogiques, dictionnaires, jeux éducatifs, outils d'apprentissage de langues étrangères.
Achats en ligne	Applications destinées à réaliser des achats sur Internet et à participer à des enchères, cartes cadeaux, outils de comparaison de prix et de création de listes de souhaits, consultation de commentaires sur les produits.
Utilitaires de lancement	Applications destinées à modifier l'apparence du bureau, à gérer les widgets et les étiquettes.
Systèmes d'exploitation et utilitaires	Applications système assurant l'administration du système d'exploitation, les interactions avec l'utilisateur et la gestion de la mémoire vive.
Applications de cartographie	Guides de villes, informations sur les entreprises locales, outils de création d'itinéraires.
Autres applications	Bibliothèques logicielles, versions démos d'applications. Applications n'entrant dans aucune des catégories.
Transport	Applications pour l'utilisation des transports en commun, outils de navigation et de conduite.
Jeux	Arcades, Quiz, Courses, Autres, Casino, Cartes, Musique, Jeux de société, Didacticiels, Puzzles, Aventures, Jeux de rôles, Simulateurs, Jeux de lettres, Jeux sportifs, Stratégie, Action.
Navigateurs	Applications pour la consultation de sites Internet, de documents Web, de fichiers. Applications de gestion des applications Web.

Catégorie	Description
Outils de développement	Applications destinées à la création d'applications. Outils de réglages, éditeurs de lien, éditeurs de code source, éditeurs d'interface graphique.
Applications de système d'exploitation	Applications installées en même temps que le système d'exploitation et nécessaires à son fonctionnement.
Applications Internet	Gestionnaires de téléchargement, clients de messagerie, applications de recherche sur Internet et autres applications pour utiliser Internet.
Applications pour l'infrastructure réseau	Applications pour la gestion des serveurs, des périphériques d'enregistrement des données pour les équipements réseau, des logiciels de réseaux d'entreprise, applications pour l'automatisation et l'intégration des infrastructures.
Applications réseau	Applications destinées à organiser la collaboration entre les utilisateurs de plusieurs appareils et à la communication entre les périphériques.
Utilitaires système	Applications installées en même temps que le système d'exploitation : gestionnaires de fichiers, logiciels de compression de données, utilitaires de diagnostic matériel et logiciel, outils d'optimisation de la mémoire, outils de désinstallation, utilitaires de gestion des processeurs.
Applications de sécurité	Applications de protection des données de l'appareil. Applications de détection et de suppression des menaces sur l'appareil. Pare-feu. Applications de chiffrement de données.
Gestionnaires de téléchargement	Applications pour le téléchargement de fichiers à partir de sources externes.
Applications de sauvegarde des fichiers sur Internet	Applications pour l'enregistrement sur le cloud de fichiers, de notes et de fichiers multimédias.
Applications d'aide	Applications destinées à la lecture de livres, d'ouvrages de référence, de manuels, de dictionnaires, de thésaurus, de pages wiki.

Glossaire

A

Administrateur d'appareil

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

Appareil EAS

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

Appareil contrôlé

Le périphérique iOS dont la configuration est contrôlée dans l'application pour la configuration de groupe des périphériques iOS Apple Configurator. le périphérique contrôlé possède l'état supervised dans Apple Configurator. A chaque connexion du périphérique contrôlé à l'ordinateur, Apple Configurator vérifie la conformité de la configuration du périphérique aux paramètres définis et les configure, le cas échéant. le périphérique contrôlé ne peut être synchronisé avec une version d'Apple Configurator installée sur un autre ordinateur.

un périphérique contrôlé offre plus de paramètres pour la configuration à l'aide d'une stratégie Kaspersky Mobile Device Management qu'un périphérique non contrôlé. Il est, par exemple, possible de configurer sur le périphérique contrôlé un proxy HTTP pour le contrôle du trafic Internet sur le périphérique dans les limites du réseau de l'entreprise. Par défaut, aucun périphérique mobile n'est contrôlé.

Appareil iOS MDM

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

Application tierce

Application élaborée par une entreprise tierce (par exemple, client de messagerie pour le périphérique 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 des périphériques mobiles iOS MDM peut administrer les périphériques iOS.

Conteneur

Enveloppe spéciale pour les applications mobiles qui permet de contrôler les activités des applications qu'elle contient. Le conteneur protège les données personnelles et les données d'entreprise figurant sur l'appareil.

Contrôle de la conformité

Vérification de la conformité des périphériques mobiles des utilisateurs à la stratégie de groupe. Ce contrôle permet également de s'assurer de la conformité des paramètres des périphériques 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 périphériques iOS pour chercher, télécharger et installer des applications depuis un serveur Internet.

G

Groupe d'administration

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

K

Kaspersky Security Network (KSN)

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

P

Paquet autonome d'installation

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

Paquet d'applications mobiles

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

Paquet d'installation

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

Plug-in d'administration de l'application

Un composant spécialisé qui fournit une interface pour administrer l'application de Kaspersky Lab via la Console d'administration. Chaque application a son propre plug-in d'administration. Ce plug-in d'administration fait partie de toutes les applications de Kaspersky Lab administrées à l'aide du Kaspersky Security Center.

Poste de travail de l'administrateur

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

Profil de travail Android for Work

Environnement sécurisé sur le périphérique de l'utilisateur et dans lequel l'administrateur peut gérer des applications et des comptes sans limiter ses possibilités lors de l'utilisation des données personnelles. Lors de la création d'un profil de travail sur le périphérique mobile de l'utilisateur, les applications d'entreprise suivantes sont installées automatiquement dans ce profil : Google Play Store, Google Chrome, Téléchargements, Kaspersky Endpoint Security for Android, etc. Les applications réparties dans le profil de travail et les notifications de ces applications sont signalées par une icône rouge de profil. Pour l'application Google Play Store, un compte d'entreprise Google séparé doit être créé. Les applications réparties dans le profil de travail sont indiquées dans la liste commune d'applications.

Profil iOS MDM

Profil comportant tout un ensemble de paramètres pour la connexion des périphériques mobiles iOS au Serveur d'administration. Ce profil permet de diffuser les profils de configuration iOS en

arrière-plan à l'aide du Serveur de gestion des périphériques mobiles iOS MDM et d'obtenir un diagnostic étendu sur les périphériques mobiles. Vous devez envoyer le lien vers le profil iOS MDM à l'utilisateur pour permettre au serveur des périphériques mobiles iOS de détecter et de connecter son appareil mobile fonctionnant avec iOS.

Profil provisioning

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

R

Requête Certificate Signing Request

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

S

Serveur Web de Kaspersky Security Center

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

Serveur d'administration

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

Serveur de gestion des périphériques mobiles Exchange ActiveSync

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

Serveur des périphériques mobiles iOS MDM

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

Stratégie

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

Synchronisation

Processus au cours duquel la connexion entre le périphérique mobile et le système d'administration à distance s'établit et pendant lequel des données sont échangées. Lors de la synchronisation, le périphérique reçoit les paramètres de Kaspersky Endpoint Security définis par l'administrateur. le périphérique envoie au système d'administration à distance les rapports sur le fonctionnement des modules de l'application mobile.

T

Tâche de groupe

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

U

Utilitaire Kaspersky SMS Broadcasting

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

Kaspersky Lab AO

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

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement "IDC Worldwide Endpoint Security Revenue by Vendor"). En Russie, selon les données d'IDC, Kaspersky Lab est le fournisseur de système de protection informatique favori des particuliers ("IDC Endpoint Tracker 2014").

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, c'est un groupe international qui dispose de 34 succursales dans 31 pays. La société emploie plus de 3000 experts qualifiés.

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

La gamme de logiciels pour particuliers comprend des applications de sécurité informatique pour ordinateurs de bureau et ordinateurs portables ainsi que des applications pour la protection des tablettes, des smartphones et d'autres appareils mobiles.

La société propose des solutions et des technologies de protection et de contrôle des stations de travail et des appareils mobiles, des machines virtuelles, des serveurs de fichiers et des serveurs Web, des passerelles de messagerie et des pare-feu. L'entreprise propose également des produits spécialisés pour la protection contre les attaques DDoS, pour la protection des systèmes d'automatisation industrielle ainsi que pour la prévention des escroqueries financières. Ces solutions, associées à une administration centralisée, permettent de créer et d'exploiter une protection automatisée efficace des entreprises de toutes tailles contre les menaces informatiques. Les logiciels de Kaspersky Lab ont obtenu les certificats des plus grands laboratoires d'essai. Ils sont compatibles avec les applications de nombreux éditeurs et sont optimisés pour de nombreuses plate-formes matérielles.

Les experts de la lutte antivirus de Kaspersky Lab travaillent 24h/24. Chaque jour, ils trouvent des centaines de milliers de nouvelles menaces informatiques, développent les outils d'identification et de neutralisation de ces menaces et ajoutent les signatures de ces menaces aux bases utilisées par les applications de Kaspersky Lab.

TECHNOLOGIES. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est donc pas un hasard si le moteur logiciel de Kaspersky Anti-Virus est intégré aux logiciels de plusieurs autres éditeurs, notamment : Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, General Dynamics, Facebook, Juniper Networks, Lenovo, H3C, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. De nombreuses technologies novatrices développées par la société sont brevetées.

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

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

Information sur le code tiers

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

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

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

Avis de marques déposées

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

Postscript est une marque d'Adobe Systems Incorporated enregistrée aux Etats-Unis et/ou dans d'autres pays.

Apple, Apple TV, AirDrop, AirPlay, AirPrint, AiCal, AirPort Express, Aperture, Bonjour, FaceTime, iBook, iBooks, iCal, iPhone, iPhoto, iTunes, Mac OS et Safari sont des marques d'Apple Inc., déposées aux Etats-Unis et dans d'autres pays.

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

Android, Google Chrome, Google, Google Mail, Google Play, Google Analytics sont des marques commerciales de Google, Inc.

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

Aruba Networks est une marque déposée d'Aruba Networks, Inc. aux Etats-Unis et dans d'autres pays.

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

Cisco, Aironet et AnyConnect sont des marques de Cisco Systems, Inc. déposées aux Etats-Unis et dans d'autres pays, et/ou de ses compagnies affiliées.

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

Samsung et KNOX sont des marques commerciales de SAMSUNG aux Etats-Unis et dans d'autres pays.

SonicWALL, SonicWALL Mobile Connect sont des marques de Dell, Inc.

Juniper Networks et JUNOS sont des marques de Juniper Networks, Inc. déposées aux Etats-Unis et dans d'autres pays.

Index

A

C

F

G

K

M

P

R

S