kaspersky

Kaspersky Security for Mobile

Contenu

Aide de Kaspersky Security for Mobile

Kaspersky Security for Mobile est destiné à protéger et à gérer les appareils mobiles d'entreprise, ainsi que les appareils mobiles personnels utilisés par les employés de l'entreprise à des fins professionnelles.

Les composants et fonctionnalités de Kaspersky Security for Mobile dépendent de la console Kaspersky Security Center que vous utilisez comme interface de protection et d'administration des périphériques mobiles.

Sélectionnez la section de l'Aide qui vous correspond en fonction de votre console Kaspersky Security Center :

- Console d'administration basée sur la console de gestion Microsoft
- Web Console ou Cloud Console

Cette section de l'Aide décrit les fonctionnalités et les opérations auxquelles ont accès les utilisateurs de l'application Kaspersky Endpoint Security for Android.

Nouveautés

Informations techniques 41

- Améliorations de l'interface utilisateur de l'application Kaspersky Endpoint Security for Android.
- Améliorations de l'interface utilisateur dans les paramètres de la stratégie du plug-in de Kaspersky Endpoint Security for Android pour Kaspersky Security Center Web Console et Cloud Console.
- Corrections de bogues et améliorations générales.

Informations techniques 40

- Corrections de bogues et améliorations générales.

Informations techniques 39

- Android 12L est maintenant pris en charge.
- Les déclarations et les contrats suivants ont été mis à jour :
  - Contrat de licence utilisateur final
  - Déclaration de Kaspersky Security Network
  - Déclaration sur le traitement des données à des fins marketing

  Notez que l'administrateur peut accepter les nouvelles conditions des contrats et des déclarations dans la Console d'administration. Cela permet aux utilisateurs de l'application Kaspersky Endpoint Security for Android de sauter cette étape sur les appareils.
- Corrections de bogues et améliorations générales.

Informations techniques 33

- Dans le cadre de la gestion de l'application Kaspersky Endpoint Security for Android à l'aide de systèmes EMM tiers, vous pouvez désormais accepter plusieurs contrats de licence utilisateur final en utilisant une seule commande.
- Vous n'avez plus besoin de clé pour activer Samsung KNOX.
- La structure des versions des composants de Kaspersky Security for Mobile a été modifiée pour inclure le numéro de version.

Informations techniques 32

- L'application Kaspersky Endpoint Security for Android a été modifiée pour prendre en charge les exigences Android mises à jour.

Informations techniques 31

- Si Kaspersky Security Center n'est pas déployé dans votre organisation ou s'il n'est pas accessible aux appareils mobiles, les utilisateurs peuvent activer manuellement l'application Kaspersky Endpoint Security for Android sur leurs appareils.
- Kaspersky Security for Mobile prend désormais en charge la fonctionnalité d'onglets personnalisés de Google Chrome.

Informations techniques 30

- Kaspersky Security for Mobile vous permet désormais de protéger et de gérer les appareils mobiles dans Kaspersky Security Center Cloud Console.
- Kaspersky Security for Mobile est désormais compatible avec iOS 15 et iPadOS 15.

Informations techniques 29

- L'application Kaspersky Endpoint Security for Android prend désormais en charge Android 12.

Informations techniques 27

- Kaspersky Security for Mobile vous permet désormais de protéger et de gérer les périphériques mobiles dans Kaspersky Security Center Web Console.

Informations techniques 26

- Kaspersky Endpoint Security prend désormais en charge les licences et les abonnements avec renouvellement automatique.

Informations techniques 22

- Kaspersky Endpoint Security prend désormais en charge Kaspersky Private Security Network , une solution qui permet d'accéder aux bases de données de réputation de Kaspersky Security Network sans envoyer de données en dehors du réseau de l'entreprise.
- Kaspersky Endpoint Security for Android ne peut plus être installé sur les appareils exécutant les versions Android 4.2 à 4.4.4.

Informations techniques 20

- Les utilisateurs ne sont pas invités à accepter les déclarations légales si l'administrateur a choisi d'accepter les déclarations globalement.
- Les performances de l'application ont été optimisées.

Informations techniques 19

- L'administrateur peut désormais accepter Kaspersky Security Network et les autres déclarations au nom des autres utilisateurs via Kaspersky Security Center.
- Correction d'une série d'erreurs, amélioration de la stabilité.

Informations techniques 18

- Kaspersky Security for Mobile prend désormais en charge Huawei Mobile Services.
- Kaspersky Endpoint Security for Android est maintenant disponible à l'installation depuis Huawei App Gallery.

Informations techniques 17

- Kaspersky Endpoint Security vise désormais le niveau 29 de l'API et plus, ce qui entraîne quelques changements dans le comportement de l'applications sur les appareils tournant sous Android 10 ou plus.
- Nouveaux paramètres de force des mots de passe permettant à l'utilisateur de définir les mots de passe de la complexité requise.
- La configuration de l'utilisation de l'empreinte digitale comme méthode de déverrouillage de l'écran est désormais disponible uniquement pour le profil de travail Android.
- Correction d'une série d'erreurs, amélioration de la stabilité.

Informations techniques 16

- Kaspersky Endpoint Security for Android prend désormais en charge Android 11.
- Nouvelles exigences en matière de géolocalisation et d'autorisation des caméras introduites par Android 11. Vous pouvez en savoir plus sur les nouvelles règles relatives aux autorisations d'accès aux caméras et aux lieux dans cette section.
- Vous pouvez désormais spécifier les adresses email professionnelles des utilisateurs dans une console EMM tierce. Ces emails s'afficheront dans Kaspersky Security Center à condition que le nouveau KscCorporateEmail soit configuré.

Informations techniques 14

- Chaque fois qu'un utilisateur autorise ou révoque les privilèges d'Administrateur d'appareil de l'application, un événement est envoyé à la Console de gestion.
- Le paramètre "KscGroup" peut désormais être configuré dans les consoles EMM tierces. Lorsqu'un appareil se connecte à Kaspersky Security Center, il est automatiquement ajouté à un sous-dossier du dossier Appareils non définis du même nom que le groupe configuré dans une console EMM.

Informations techniques 13

- Interface utilisateur revue pour Kaspersky Endpoint Security for Android.
- Toutes les rubriques d'aide sont désormais disponibles en ligne.

- Les adresses IP des appareils administrés sont désormais envoyées à Kaspersky Security Center et elles sont visibles dans les sections reprenant les informations sur les appareils.

Informations techniques 12

- Ajout de la possibilité d'accepter à distance le Contrat de licence utilisateur final (CLUF) dans Kaspersky Security Center 12.1. Si l'administrateur accepte les dispositions du Contrat de licence et de la Politique de confidentialité dans la Console d'administration, l'application ignore ces étapes lors du processus d'installation.

- Ajout de la capacité de modifier le nom de l'appareil dans Kaspersky Security Center pour les utilisateurs de VMware AirWatch. Nous avons ajouté un nouveau paramètre au fichier configuration de l'app. Vous pouvez ajouter des informations supplémentaires au nom de l'appareil (par exemple, son numéro de série). Cela facilite la recherche et le tri des appareils dans Kaspersky Security Center.

Informations techniques 11

Correction d'une série d'erreurs, amélioration de la stabilité.

Informations techniques 10

- Kaspersky Security for Mobile prend désormais en charge Kaspersky Security Center 12.

- Kaspersky Safe Browser n'est plus pris en charge dans Kaspersky Security Center 12. Vous pouvez utiliser les fonctions de Kaspersky Safe Browser à l'aide de Kaspersky Security Center 11 ou une version antérieure.

- Correction d'une série d'erreurs, amélioration de la stabilité.

Service Pack 4 Maintenance Release 3

- Vérification de la prise en charge de Kaspersky Endpoint Security for Android dans Microsoft Intune (une solution Enterprise Mobility Management (EMM)). Pour garantir le fonctionnement de l'application avec les solutions EMM tierces, Kaspersky participe à AppConfig Community.

- Ajout de la possibilité de désactiver les notifications et les messages contextuels lorsque l'application est en mode arrière-plan. Rappelez-vous qu'il est dangereux d'effectuer ces actions en mode d'arrière-plan. Si vous désactivez les notifications et les messages contextuels lorsque l'application est en mode arrière-plan, l'application n'avertira pas les utilisateurs des menaces en temps réel. Les utilisateurs d'appareils mobiles ne peuvent connaître l'état de protection de l'appareil que lorsqu'ils ouvrent l'application.

- Ajout de la possibilité d'accepter le Contrat de licence utilisateur final (CLUF) et la Politique de confidentialité dans VMware AirWatch. Si l'administrateur a accepté le Contrat de licence utilisateur final et la politique de confidentialité dans une console AirWatch Console, Kaspersky Endpoint Security for Android ignore l'étape d'acceptation dans l'Assistant de configuration initiale.

- Ajout de la Déclaration relative au traitement des données aux fins d'utilisation de la Protection Internet (Déclaration sur la Protection Internet). Pour utiliser la Protection Internet, vous devez accepter la déclaration. Kaspersky Endpoint Security for Android utilise Kaspersky Security Network (KSN) pour analyser les sites Internet. La Déclaration sur la Protection Internet contient les conditions générales de l'échange de données avec KSN. Vous pouvez accepter la Déclaration sur la protection Internet dans la stratégie ou le formulaire d'acceptation de la demande provenant d'un utilisateur de l'appareil.

- Correction d'une série d'erreurs, amélioration de la stabilité.

Comparaison des fonctionnalités de l'application selon les outils de gestion

Vous pouvez gérer les appareils mobiles dans Kaspersky Security Center à l'aide des outils de gestion suivants :

- Console d'administration basée sur Microsoft Management Console (ci-après dénommée "basée sur MMC") de Kaspersky Security Center
- Kaspersky Security Center Web Console
- Kaspersky Security Center Cloud Console

Le tableau ci-dessous compare les fonctionnalités disponibles dans ces outils.

Disponibilité des fonctionnalités de l'application selon les outils de gestion

	Console basée sur MMC	Web Console	Cloud Console
Général			
Gestion des appareils iOS	Disponible	Pas disponible	Pas disponible
Gestion des appareils Android	Disponible	Disponible	Disponible
Gestion des appareils mobiles			
Ajout d'appareils via un lien de Google Play	Disponible	Disponible	Disponible
Ajout d'appareils via la création d'un paquet d'installation	Disponible	Pas disponible	Pas disponible
Envoi de commandes aux périphériques mobiles	Disponible	Disponible (sauf la commande Photographier)	Disponible (sauf la commande Photographier)
Suppression des appareils mobiles de Kaspersky Security Center	Disponible	Disponible (Suppression au sein de la liste des appareils uniquement. Il faut supprimer l'application manuellement de l'appareil.)	Disponible (Suppression au sein de la liste des appareils uniquement. Il faut supprimer l'application manuellement de l'appareil.)
Gestion des certificats			
Émission de certificats de messagerie	Disponible	Pas disponible	Pas disponible
Émission de certificats de VPN	Disponible	Pas disponible	Pas disponible
Émission de certificats mobiles	Disponible	Disponible	Disponible
Émission de certificats mobiles via les outils du Serveur d'administration	Disponible	Disponible	Disponible
Désignation des fichiers de certificat	Disponible	Pas disponible	Pas disponible
Intégration à	Disponible	Pas disponible	Pas disponible

l'infrastructure à clé publique			
Gestion des stratégies			
Accès en fonction des rôles pour configurer les stratégies de groupe	Disponible	Pas disponible	Pas disponible
Configuration de la synchronisation des appareils mobiles avec Kaspersky Security Center	Disponible	Disponible	Disponible
Configuration de la recherche de virus sur les appareils mobiles	Disponible	Disponible	Disponible
Configuration de la protection de l'appareil mobile	Disponible	Disponible	Disponible
Configuration des mises à jour des bases antivirus	Disponible	Disponible	Disponible
Configuration de la Protection des données en cas de perte ou de vol de l'appareil	Disponible	Disponible	Disponible
Configuration de l'accès des utilisateurs aux sites Internet	Disponible	Disponible	Disponible
Configuration du contrôle des applications	Disponible	Disponible	Disponible
Configuration du contrôle de conformité	Disponible	Disponible	Disponible
Configuration des profils de travail Android	Disponible	Pas disponible	Pas disponible
Configuration de la connexion au réseau Wi-Fi	Disponible	Pas disponible	Pas disponible
Samsung KNOX	Disponible	Pas disponible	Pas disponible
Autres fonctionnalités			
Acceptation globale du CLUF dans Kaspersky Security Center	Disponible	Pas disponible	Pas disponible
Configuration de Kaspersky Private Security Network	Disponible	Pas disponible	Pas disponible

Paquet de distribution

Le kit de distribution de Kaspersky Security for Mobile peut inclure différents composants selon la version de l'application choisie.

Administration des appareils mobiles dans Kaspersky Security Center Web Console

- `Archive_name_kes_android_mdm.xx.x.x.x.zip`

  Archive contenant les fichiers nécessaires à l'installation du plug-in Kaspersky Security for Mobile :

  - `mobile_device_management.zip`

    Archive contenant le plug-in Kaspersky Security for Mobile.

  - `signature.txt`

    Fichier contenant la signature du plug-in Kaspersky Security for Mobile.

- `Archive_name_kes_android_policy.xx.x.x.x.zip`

  Archive contenant les fichiers nécessaires à l'installation du plug-in Kaspersky Endpoint Security for Android :

  - `kes_android.zip`

    Archive contenant le plug-in Kaspersky Endpoint Security for Android.

  - `signature.txt`

    Fichier contenant la signature du plug-in Kaspersky Endpoint Security for Android.

Administration des appareils mobiles dans Kaspersky Security Center Cloud Console

Pour administrer l'appareil mobile dans Kaspersky Security Center Cloud Console, vous n'avez pas besoin de télécharger un paquet de distribution. Il vous suffit de créer un compte dans Kaspersky Security Center Cloud Console. Pour plus d'informations sur la création d'un compte, consultez l'*Aide de Kaspersky Security Center Cloud Console*.

Administration des périphériques mobiles dans la console d'administration basée sur MMC

- `Klcfginst_en.exe`

  Fichier d'installation du plug-in d'administration de Kaspersky Endpoint Security for Android à l'aide du système d'administration à distance Kaspersky Security Center.

- `Klmdminst.exe`

  Fichier d'installation du plug-in d'administration de Kaspersky Device Management for iOS à l'aide du système d'administration à distance Kaspersky Security Center.

Fichier de l'application Kaspersky Endpoint Security for Android

`KES10_xx_xx_xxx.apk` : fichier de package Android de l'application Kaspersky Endpoint Security for Android.

Fichiers auxiliaires

- `sc_package_xx.exe`

  Archive auto-extractible contenant les fichiers nécessaires à l'installation de l'application Kaspersky Endpoint Security for Android en créant des paquets d'installation :

  - `adb.exe, AdbWinApi.dll, AdbWinUsbApi.dll`

    Fichiers requis pour la création de paquets d'installation.

  - `installer.ini`

    Fichier de configuration contenant les paramètres de connexion du Serveur d'administration.

  - `KES10_xx_xx_xxx.apk`

    Fichier de package Android de l'application Kaspersky Endpoint Security for Android.

  - `kmlisten.exe`

    Utilitaire de livraison des paquets d'installation via l'ordinateur de l'administrateur.

  - `kmlisten.ini`

    Fichier de configuration contenant les paramètres de l'utilitaire `kmlisten.exe`.

  - `kmlisten.kpd`

    Fichier de description de l'application.

- `SigningUtility.zip`

  Archive contenant l'utilitaire de signature du paquet de distribution de l'application Kaspersky Endpoint Security for Android et des conteneurs pour les appareils iOS.

Documentation

- Aide pourn Kaspersky Security for Mobile.

Utilisation de Kaspersky Security Center Web Console et Kaspersky Security Center Cloud Console

Cette section de l'Aide décrit la protection et la gestion des appareils mobiles à l'aide de Kaspersky Security Center Web Console (ci-après également dénommée Web Console) ou Kaspersky Security Center Cloud Console (ci-après également dénommée Cloud Console).

A propos de l'administration des appareils mobiles dans Kaspersky Security Center Web Console et Cloud Console

Vous pouvez administrer les appareils mobiles dans Kaspersky Security Center Web Console et Cloud Console en utilisant les composants suivants :

- Application Kaspersky Endpoint Security for Android

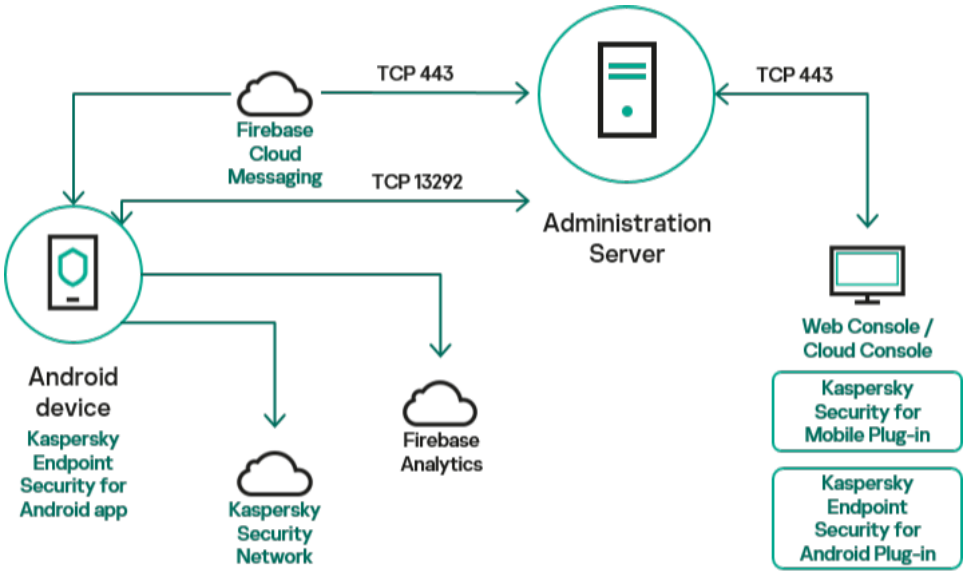
  L'application Kaspersky Endpoint Security for Android assure la protection des appareils mobiles contre les menaces Internet, les virus et autres programmes qui constituent des menaces.

- Plug-in Kaspersky Security for Mobile

  Le plug-in Kaspersky Security for Mobile fournit l'interface d'administration des appareils mobiles et des applications mobiles qui y sont installées via Kaspersky Security Center Web Console et Cloud Console.

- Plug-in d'administration de Kaspersky Endpoint Security for Android

  Le plug-in Kaspersky Endpoint Security for Android vous permet de définir les paramètres de configuration des appareils connectés à Kaspersky Security Center à l'aide de stratégies de groupe.



Administration des appareils mobiles dans Kaspersky Security Center Web Console et Cloud Console

Les plug-ins s'intègrent au *système d'administration à distance Kaspersky Security Center*. Vous pouvez utiliser Kaspersky Security Center Web Console ou Cloud Console pour administrer les appareils mobiles, ainsi que les ordinateurs clients et les systèmes virtuels. Les périphériques mobiles peuvent être administrés dès qu'ils ont été connectés au Serveur d'administration. Vous pouvez commander à distance les appareils administrés.

Principales fonctionnalités de l'administration des appareils mobiles dans Kaspersky Security Center Web Console et Cloud Console

Kaspersky Security for Mobile fournit les fonctionnalités suivantes :

- Diffusion d'emails pour la connexion d'appareils tournant sous Android à Kaspersky Security Center sous la forme de liens vers Google Play ;
- Connexion à distance des appareils mobiles des utilisateurs à Kaspersky Security Center et d'autres systèmes EMM tiers (par exemple, VMWare AirWatch, MobileIron, IBM Maas360, SOTI MobiControl) ;
- Configuration à distance de l'application Kaspersky Endpoint Security for Android, ainsi que des services, des applications et des fonctions des appareils Android ;
- configuration à distance des appareils mobiles conformément aux exigences de sécurité de l'entreprise ;
- Prévention des fuites de données de l'entreprise stockées sur les appareils mobiles en cas de perte ou de vol de ceux-ci (Antivol) ;
- vérification du respect des exigences de sécurité de l'entreprise (Contrôle de conformité) ;
- Contrôle de l'utilisation d'Internet sur les appareils mobiles (Protection Internet) ;
- Configuration des notifications présentées à l'utilisateur dans l'application Kaspersky Endpoint Security for Android ;
- Notification de l'administrateur sur l'état et les événements dans le fonctionnement de l'application Kaspersky Endpoint Security for Android dans Kaspersky Security Center ou par email ;
- Contrôle des modifications des paramètres de la stratégie (Historique des révisions).

Kaspersky Security for Mobile comprend les modules de protection et d'administration suivants :

- Anti-Virus
- Antivol
- Protection Internet
- Contrôle des applications installées
- Contrôle de conformité
- Détection des privilèges root sur les appareils

A propos de l'application Kaspersky Endpoint Security for Android

L'application Kaspersky Endpoint Security for Android assure la protection des appareils mobiles contre les menaces Internet, les virus et autres programmes qui constituent des menaces.

L'application Kaspersky Endpoint Security for Android inclut les composants suivants :

- **Antivirus**. Ce composant détecte et neutralise les menaces sur votre appareil mobile à l'aide des bases antivirus et des services cloud du Kaspersky Security Network. L'Antivirus présente les composants suivants :
  - **Protection**. Elle permet de découvrir les menaces dans les fichiers ouverts, d'analyser les nouvelles applications et de prévenir l'infection des appareils en temps réel.
  - **Analyse**. Lancée à la demande pour l'ensemble du système de fichiers, uniquement pour les apps installées ou le fichier ou le dossier sélectionné.
  - **Mise à jour**. Elle permet de télécharger les nouvelles bases antivirus de l'application.
- **Antivol**. Ce composant protège les informations de l'appareil contre tout accès non autorisé en cas de perte ou de vol de l'appareil. Ce composant vous permet d'envoyer les commandes suivantes à l'appareil :
  - **Localisation**. Elle permet d'obtenir les coordonnées de l'emplacement de l'appareil.
  - **Émettre l'alarme**. Alarme pour faire sonner l'appareil.
  - **Balayer**. Suppression des données d'entreprise pour protéger les informations sensibles de l'entreprise.
- **Protection Internet**. Permet de bloquer les sites Internet malveillants dont le but est de diffuser un code nuisible. La Protection Internet bloque également les faux 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 cloud de 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 cloud de 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, loterie, tirages au sort" ou "Communication via Internet", par exemple).
- **Contrôle des applications.** Ce composant vous permet d'installer les apps recommandées et requises sur votre appareil à l'aide d'un lien direct vers la distribution ou vers Google Play. Grâce au Contrôle des applications, vous pouvez supprimer les applications interdites, non conformes aux exigences à la sécurité corporative.
- **Contrôle de conformité.** Ce composant vous permet de vérifier la conformité des appareils administrés par rapport aux exigences de sécurité de l'entreprise et d'imposer des restrictions sur certaines fonctions des appareils non conformes.

Vous pouvez configurer les composants de l'application Kaspersky Endpoint Security for Android dans Kaspersky Security Center Web Console et Cloud Console en définissant les paramètres des stratégies de groupe.

A propos du plug-in Kaspersky Security for Mobile

Le plug-in Kaspersky Security for Mobile fournit l'interface d'administration des appareils mobiles et des applications mobiles qui y sont installées via Kaspersky Security Center Web Console et Cloud Console. Kaspersky Security for Mobile Plug-in vous permet d'effectuer les opérations suivantes :

- Connecter des appareils mobiles à Kaspersky Security Center.
- Gérer les certificats des appareils mobiles.

- Configurer Firebase Cloud Messaging.
- Envoyer des commandes aux appareils mobiles.

Le plug-in Kaspersky Security for Mobile peut être installé lors de la configuration de Kaspersky Security Center Web Console. Si vous utilisez Kaspersky Security Center Cloud Console, vous n'avez pas besoin d'installer ce plug-in. Pour plus d'informations sur les scénarios de déploiement dans différents types de consoles, consultez la section "Scénarios de déploiement".

A propos du plug-in Kaspersky Endpoint Security for Android

Le plug-in Kaspersky Endpoint Security for Android vous permet de définir les paramètres de configuration des appareils connectés à Kaspersky Security Center à l'aide de stratégies de groupe. Le plug-in Kaspersky Endpoint Security for Android peut être utilisé pour effectuer les opérations suivantes :

- Créer des stratégies de sécurité de groupe pour les appareils mobiles.
- Configurer à distance les paramètres de fonctionnement de l'application Kaspersky Endpoint Security sur les appareils mobiles des utilisateurs.
- Recevoir les rapports et les statistiques sur le fonctionnement de l'application Kaspersky Endpoint Security sur les appareils mobiles des utilisateurs.

Le plug-in Kaspersky Endpoint Security for Android peut être installé lors de la configuration de Kaspersky Security Center Web Console. Si vous utilisez Kaspersky Security Center Cloud Console, vous n'avez pas besoin d'installer ce plug-in. Pour plus d'informations sur les scénarios de déploiement dans différents types de consoles, consultez la section "Scénarios de déploiement".

Configurations logicielles et matérielles

Cette section énumère la configuration matérielle et logicielle requise pour l'ordinateur de l'administrateur utilisé pour installer le plug-in Kaspersky Security for Mobile et le plug-in Kaspersky Endpoint Security for Android dans Kaspersky Security Center Web Console et Cloud Console, déployer Kaspersky Endpoint Security for Android sur les appareils mobiles, ainsi que la configuration matérielle et logicielle de l'application Kaspersky Endpoint Security for Android.

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

Pour installer le plug-in Kaspersky Security for Mobile et le plug-in Kaspersky Endpoint Security for Android, l'ordinateur de l'administrateur doit répondre aux exigences matérielles de Kaspersky Security Center. Pour plus d'informations sur la configuration matérielle et logicielle de Kaspersky Security Center :

- Si vous utilisez Kaspersky Security Center Web Console, veuillez consulter l'*Aide de Kaspersky Security Center*.
- Si vous utilisez Kaspersky Security Center Cloud Console, veuillez vous reporter à l'*Aide de Kaspersky Security Center Cloud Console*.

Pour utiliser le plug-in Kaspersky Security for Mobile et le plug-in Kaspersky Endpoint Security for Android dans Kaspersky Security Center Web Console, Kaspersky Security Center Web Console doit être installé sur l'ordinateur de l'administrateur.

Pour utiliser le plug-in Kaspersky Security for Mobile et le plug-in Kaspersky Endpoint Security for Android dans Kaspersky Security Center Cloud Console, vous devez créer un compte dans Kaspersky Security Center Cloud Console. Pour plus d'informations sur la création d'un compte, consultez l'*Aide de Kaspersky Security Center Cloud Console*.

L'application Kaspersky Endpoint Security for Android peut aussi fonctionner avec les systèmes EMM tiers suivants :

- VMWare AirWatch 9.3 et suivant ;
- MobileIron 10.0 et version supérieure ;
- IBM MaaS360 10.68 et version supérieure ;
- Microsoft Intune 1908 et version supérieure ;
- SOTI MobiControl 14.1.4 (1693) et version supérieure.

Configurations matérielle et logicielle requises sur l'appareil mobile de l'utilisateur pour prendre en charge l'installation de l'application Kaspersky Endpoint Security for Android

L'application 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 ;
- Android 5.0 à 12 (y compris Android 12L, sauf Go Edition) ;
- processeur d'architecture x86, x86-64, ARM5, ARM6, ARM7, ARM8.

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

Questions et éléments particuliers à prendre en considération connues

Kaspersky Endpoint Security comporte une série de problèmes connus non critiques pour le fonctionnement de l'application.

Problèmes connus lors du démarrage de l'administration des appareils mobiles dans Kaspersky Security Center Web Console

- Vous pouvez démarrer l'administration des appareils mobiles lors de la configuration initiale de la Console d'administration basée sur MMC de Kaspersky Security Center (lors de l'exécution de l'Assistant de démarrage rapide) ou ultérieurement en affichant le dossier Administration des appareils mobiles dans la Console d'administration.

Problèmes connus lors de l'installation des applications

- Kaspersky Endpoint Security for Android s'installe seulement dans la mémoire principale de l'appareil.

- Sur les appareils tournant sous Android 7.0, lors de la tentative de désactivation des privilèges d'administrateur pour Kaspersky Endpoint Security for Android dans les paramètres de l'appareil, un échec peut survenir si la superposition de fenêtres est interdite pour Kaspersky Endpoint Security for Android. Le problème est lié à un défaut connu dans Android 7.

- L'app Kaspersky Endpoint Security for Android sur les appareils tournant sous Android 7.0 et suivant ne prend pas en charge le mode d'affichage de plusieurs fenêtres.

- Kaspersky Endpoint Security for Android ne fonctionne pas sur les appareils Chromebook tournant sous Chrome.

- Kaspersky Endpoint Security for Android ne fonctionne pas sur les appareils tournant sous Android (Go edition).

- Lors de l'utilisation de l'application Kaspersky Endpoint Security for Android avec des systèmes EMM tiers (par exemple, VMWare AirWatch), seuls les composants Antivirus et Protection Internet sont accessibles. L'administrateur peut configurer les paramètres de l'Antivirus et de Protection Internet dans la console du système EMM. Dans ce cas, les notifications du fonctionnement de l'application sont accessibles seulement dans l'interface de l'application Kaspersky Endpoint Security for Android (Rapports).

Problèmes connus lors de la mise à jour de la version de l'application

- Vous pouvez mettre à jour Kaspersky Endpoint Security for Android uniquement jusqu'à la version la plus récente de l'application. Il est impossible de mettre à jour Kaspersky Endpoint Security for Android vers une version plus ancienne.

Problèmes connus dans le fonctionnement de l'Antivirus

- En raison de restrictions techniques, Kaspersky Endpoint Security for Android n'est pas capable d'analyser les fichiers de 2 Go ou plus. Dans le cadre de l'analyse, l'app ignore ces fichiers et ne les signale pas.

- Pour une analyse supplémentaire de l'appareil afin d'y détecter des nouvelles menaces dont les informations ne sont pas encore entrées dans les bases antivirus, vous devez activer l'utilisation de Kaspersky Security Network. *Kaspersky Security Network (KSN)* est une infrastructure de services cloud offrant un accès à la base opérationnelle de connaissances de Kaspersky sur la réputation des fichiers, des ressources Internet et du logiciel. L'utilisation de KSN nécessite la connexion de l'appareil mobile à Internet.

- Dans certains cas, la mise à jour des bases antivirus à partir du Serveur d'administration sur un appareil mobile peut échouer. Dans ce cas, exécutez la tâche de mise à jour de la base antivirus sur le Serveur d'administration.

- Sur certains appareils, Kaspersky Endpoint Security for Android ne détecte pas les appareils connectés via USB OTG. Il est impossible d'exécuter la recherche de virus sur ces appareils.

- Sur les appareils exécutant Android 11.0 ou une version ultérieure, l'utilisateur doit accorder l'autorisation " Autoriser l'accès pour gérer tous les fichiers ".

- Sur les appareils tournant sous Android 7.0 et suivant, la fenêtre de programmation de la recherche de virus peut ne pas s'afficher correctement (les éléments d'administration ne sont pas affichés). Le problème est lié à un défaut connu dans Android 7.

- Sur les appareils exécutant Android 7.0, la protection en temps réel en mode étendu ne détecte pas les menaces dans les fichiers stockés sur une carte SD externe.

- Sur les appareils tournant sous Android 6.0, Kaspersky Endpoint Security for Android ne détecte pas le téléchargement d'un fichier malveillant dans la mémoire de l'appareil. Un fichier malveillant peut être détecté par

l'Antivirus lors du lancement du fichier ou lors de la recherche de virus sur l'appareil. Le problème est lié à un défaut connu dans Android 6.0. Pour assurer la sécurité de l'appareil, il est recommandé de configurer le lancement de la recherche de virus d'après l'horaire planifié.

Problèmes connus dans le fonctionnement de la Protection Internet

- La Protection Internet sur les appareils Android fonctionne seulement dans les navigateurs Google Chrome (y compris la fonction Onglets personnalisés), Huawei Browser et Samsung Internet Browser.
- Pour le fonctionnement de la Protection Internet, vous devez activer l'utilisation de Kaspersky Security Network. La Protection Internet bloque les sites Internet à la base des données sur la réputation et les catégories des sites Internet, qui se trouvent dans KSN.
- Sur les appareils tournant sous Android 6.0 avec le navigateur installé Google Chrome version 51 ou les versions précédentes, les sites internet interdits peuvent ne pas être bloqués par la Protection Internet s'ils sont ouverts par les moyens suivants (le problème est liée à un défaut connu dans Google Chrome) :
  - suite à une requête de recherche ;
  - à partir de la liste des signets ;
  - à partir de l'historique des requêtes de recherche ;
  - lors de l'utilisation de la fonction de remplissage automatique de l'adresse Internet ;
  - lors de l'ouverture du site Internet dans un nouvel onglet dans Google Chrome.
- Les Sites internet interdits peuvent ne pas être bloqués dans le navigateur Google Chrome de la version 50 ou antérieures si le site Internet est ouvert depuis les résultats de recherche Google et que l'option "**Fusionner les onglets et les applications**" a été cochée dans les paramètres du navigateur. Le problème est lié à un défaut connu dans Google Chrome.
- Il se peut que les sites Internet des catégories interdites ne soient pas bloqués dans Google Chrome si l'utilisateur les ouvre depuis des applications tierces (par exemple, depuis un client IM). Le problème est lié aux particularités du fonctionnement du service des fonctions d'accessibilité avec la fonction Chrome Custom Tabs.
- Les sites internet interdits ne peuvent être bloqués dans Samsung Internet Browser si l'utilisateur les ouvre en mode d'arrière-plan via un menu contextuel ou depuis des applications tierces (par exemple, depuis un client IM).
- Pour que Protection Internet fonctionne, Kaspersky Endpoint Security for Android doit être installé en tant que service des Fonctionnalités d'accessibilité.
- Les sites Internet autorisés peuvent être bloqués dans Samsung Internet Browser en mode de Protection Internet **Seuls les sites Internet répertoriés sont autorisés** lors de la mise à jour de la page. Les sites Internet sont bloqués si l'expression régulière contient des paramètres supplémentaires (par exemple, `^https?:\/\/example\.com\/pictures\/`). Il est recommandé d'utiliser des expressions régulières sans paramètres supplémentaires (par exemple, `^https?:\/\/example\.com`).

Problèmes connus dans le fonctionnement de l'Antivol

- Pour un envoi opportun des commandes aux appareils Android, l'application utilise le service Firebase Cloud Messaging (FCM). Si FCM n'est pas configuré, les commandes seront envoyées à l'appareil seulement lors de la

synchronisation avec Kaspersky Security Center d'après l'horaire spécifié dans la stratégie par exemple, toutes les 24 heures.

- Pour le verrouillage de l'appareil, Kaspersky Endpoint Security for Android doit être installé en tant qu'administrateur de l'appareil.
- Sur les appareils tournant sous le système d'exploitation Android version 7.0 et suivantes pour le verrouillage de l'appareil, Kaspersky Endpoint Security for Android doit être installé en tant que service des Fonctionnalités d'accessibilité.
- Sur certains appareils, les commande d'Antivol ne peuvent pas être exécutées si le mode d'économie d'énergie est activé. Ce défaut est confirmé sur Alcatel 5080X.
- Pour localiser des appareils tournant sous Android 10.0 ou une version ultérieure, l'utilisateur doit accorder l'autorisation "Tout le temps" à la localisation de l'appareil.

Problèmes connus dans le fonctionnement du Contrôle des applications

- Pour que le contrôle des applications fonctionne, Kaspersky Endpoint Security for Android doit être installé en tant que service des Fonctionnalités d'accessibilité.
- Pour le fonctionnement du contrôle des applications (catégorie des applications), l'utilisation de Kaspersky Security Network doit être activée. Le contrôle des applications définit des catégories d'applications en fonction des données contenues dans KSN. L'utilisation de KSN nécessite la connexion de l'appareil mobile à Internet. Pour le fonctionnement du contrôle des applications, vous pouvez ajouter des applications séparées dans les listes des applications bloquées et des applications autorisées. Dans ce cas, KSN n'est pas obligatoire.
- Lors de la configuration du contrôle des applications, il est recommandé de décocher la case **Bloquer les apps système**. Le blocage des apps système peut donner lieu à des défaillances dans le fonctionnement de l'appareil.

Problèmes connus lors de la configuration de la sécurité du mot de passe de déverrouillage de l'appareil

- Sur les appareils tournant sous Android 10.0 ou une version ultérieure, Kaspersky Endpoint Security résout les exigences de force du mot de passe en une des valeurs du système : moyenne ou élevée.

  Si la longueur du mot de passe requise est de 1 à 4 symboles, l'application invite l'utilisateur à définir un mot de passe de force moyenne. Elle doit être soit numérique (PIN) sans séquence répétée ou ordonnée (par exemple 1234), soit alphanumérique. Le code PIN ou le mot de passe doit comporter au moins 4 caractères.

  Si la longueur du mot de passe requise est d'au moins 5 symboles, l'application invite l'utilisateur à définir un mot de passe de force élevée. Elle doit être soit numérique (PIN) sans séquence répétée ou ordonnée, soit alphanumérique (mot de passe). Le code PIN doit comporter au moins 8 chiffres ; le mot de passe doit comporter au moins 6 caractères.
- Sur appareils tournant sous Android 7.1.1, si le mot de passe de déverrouillage ne respecte pas les exigences de sécurité de l'entreprise (Contrôle de conformité), l'app système Paramètres peut ne pas fonctionner correctement lors d'une tentative de modification du mot de passe de déverrouillage via Kaspersky Endpoint Security for Android. Le problème est lié à un défaut connu dans Android 7.1.1. Pour modifier le mot de passe de déverrouillage dans ce cas, utilisez uniquement l'app système Paramètres.
- Sur certains appareils sous Android 6.0 ou suivant, une erreur peut se produire lors de la saisie du mot de passe de déverrouillage de l'écran si les données de l'appareil sont chiffrées. Le problème est lié aux particularités du fonctionnement du service des fonctionnalités d'accessibilité avec le firmware MIUI.

Problèmes connus avec la protection contre la suppression de l'application

- Kaspersky Endpoint Security for Android doit être installé avec les droits de l'administrateur de l'appareil.
- Sur les appareils tournant sous le système d'exploitation Android version 7.0 et suivantes, Kaspersky Endpoint Security for Android doit être installé en tant que service des Fonctionnalités d'accessibilités pour protéger l'app contre la suppression.
- Sur certains appareils Xiaomi et Huawei, la protection de Kaspersky Endpoint Security for Android contre la suppression ne fonctionne pas. Le problème est lié aux particularités du firmware MIUI 7 et 8 sur Xiaomi et du firmware EMUI sur Huawei.

Problèmes connus lors de la configuration des restrictions de l'appareil

- Sur les appareils tournant sous Android 10.0 ou version ultérieure, l'interdiction d'utiliser les réseaux Wi-Fi n'est pas prise en charge.
- Sur les appareils tournant sous Android 10.0 ou version ultérieure, l'utilisation de la caméra ne peut pas être totalement interdite.
- Sur les appareils tournant sous Android 11 et suivantes, Kaspersky Endpoint Security for Android doit être installé en tant que service des fonctionnalités d'accessibilité. Kaspersky Endpoint Security for Android propose à l'utilisateur d'installer l'app comme service des Fonctionnalités d'accessibilité pendant l'exécution de l'Assistant de configuration initiale. L'utilisateur peut ignorer cette étape ou désactiver ultérieurement le service dans les paramètres de l'appareil. Si tel est le cas, vous ne pourrez pas restreindre l'utilisation de l'appareil photo.

Problèmes connus lors de l'envoi de commandes vers des appareils mobiles

- Sur les appareils tournant sous Android 12 ou version ultérieure, si l'utilisateur a accordé l'autorisation "Utiliser l'emplacement approximatif", l'application Kaspersky Endpoint Security for Android essaie d'abord d'obtenir l'emplacement précis de l'appareil. En cas d'échec, l'emplacement approximatif de l'appareil n'est renvoyé que s'il n'a pas été reçu plus de 30 minutes plus tôt. Sinon, la commande **Géolocaliser l'appareil** échoue.

Problèmes connus avec des appareils spécifiques

- Sur certains appareils (par exemple, Huawei, Meizu et Xiaomi), vous devez accorder à Kaspersky Endpoint Security for Android une autorisation de démarrage automatique ou l'ajouter manuellement à la liste des applications qui sont lancées au démarrage du système d'exploitation. Si l'application n'est pas ajoutée à la liste, Kaspersky Endpoint Security for Android cesse d'exécuter toutes les fonctions après le redémarrage de l'appareil mobile. Aussi, si l'appareil a été bloqué, il est impossible de le déverrouiller à l'aide d'une commande. Vous pouvez déverrouiller l'appareil seulement à l'aide du code à usage unique de déblocage.
- Sur certains appareils (par exemple, Meizu, Asus) tournant sous Android 6.0 et suivant, il faut saisir un mot de passe numérique pour déverrouiller l'appareil après le chiffrement des données et le redémarrage de l'appareil. Si l'utilisateur utilise un mot de passe graphique pour le déverrouillage, ce mot de passe graphique doit être converti au format chiffré. Pour savoir comment convertir le schéma en chiffres, consultez le site Internet d'assistance technique du fabricant de l'appareil mobile. Le problème est lié aux particularités du fonctionnement du service des Fonctionnalités d'accessibilité.
- Sur certains appareils Huawei sous Android 5.X, après l'installation de Kaspersky Endpoint Security for Android en tant que services des fonctions d'accessibilité, un message incorrect qui indique l'absence de ces droits s'affiche. Pour masquer ce message, ajoutez l'application aux applications protégées dans les paramètres de l'appareil.

- Sur certains appareils Huawei tournant sous Android 5.X et 6.x, l'utilisateur peut quitter lui-même l'application quand le mode d'économie d'énergie pour Kaspersky Endpoint Security for Android est activé. L'appareil de l'utilisateur n'est pas protégé dans ce cas. Le problème est lié aux particularités du logiciel Huawei. Pour rétablir la protection de l'appareil, lancez Kaspersky Endpoint Security for Android manuellement. Il est recommandé de désactiver le mode Économie d'énergie pour Kaspersky Endpoint Security for Android dans les paramètres de l'appareil.

- Sur les appareils Huawei avec surcouche EMUI sous Android 7.0, l'utilisateur peut masquer la notification sur l'état de la protection de Kaspersky Endpoint Security for Android. Le problème est lié aux particularités du logiciel Huawei.

- Sur certains appareils Xiaomi, lors de la mise en place dans la stratégie d'une longueur de mot de passe dépassant 5 caractères, il sera proposé à l'utilisateur de modifier le mot de passe de déverrouillage de l'écran, et non le code PIN. Il est impossible de définir un code PIN d'une longueur de plus de 5 caractères. Le problème est lié aux particularités du logiciel Xiaomi.

- Sur les appareils Xiaomi, avec surcouche MIUI sous Android 6.0, l'icône de Kaspersky Endpoint Security for Android peut être masquée dans la barre d'état. Le problème est lié aux particularités du logiciel Xiaomi. Il est recommandé d'autoriser l'affichage des icônes de notification dans les paramètres des notifications.

- Sur certains appareils Nexus tournant sous Android 6.0.1, il est impossible d'octroyer les autorisations nécessaires au bon fonctionnement pendant l'utilisation de l'Assistant de configuration initiale de Kaspersky Endpoint Security for Android. Le problème est lié à un défaut connu dans Security Patch pour Android de Google. Pour le fonctionnement correct de l'application, les droits nécessaires doivent être attribués normalement dans les paramètres de l'appareil.

- Sur certains appareils Samsung tournant sous le système d'exploitation Android 7.0 et version ultérieure, si l'utilisateur tente de configurer des modes de déverrouillage de l'appareil non pris en charge (par exemple, mot de passe graphique), l'appareil peut être verrouillé si les conditions suivantes sont réunies : la protection contre la suppression de Kaspersky Endpoint Security for Android est activée et les exigences de la sécurité du mot de passe de déverrouillage de l'écran sont définies. Pour déverrouiller l'appareil, il faut lui envoyer une commande spéciale.

- Sur certains appareils Samsung, il est impossible d'interdire l'utilisation des empreintes digitales pour le déverrouillage de l'écran.

- Sur certains appareils Samsung, Protection Internet ne fonctionne pas si l'appareil est connecté à un réseau 3G/4G, si le mode d'économie d'énergie est activé sur l'appareil et si les données d'arrière-plan sont limitées. Il est recommandé de désactiver la fonction de restriction des processus d'arrière-plan dans l'Économie d'énergie.

- Aussi, sur certains appareils Samsung, si le mot de passe de déverrouillage n'est pas conforme aux exigences de sécurité de l'entreprise, Kaspersky Endpoint Security for Android n'interdit pas l'utilisation des empreintes digitales pour le déverrouillage de l'écran.

- Sur certains appareils Honor et Huawei, vous ne pouvez pas restreindre l'utilisation du Bluetooth. Lorsque Kaspersky Endpoint Security for Android tente de restreindre l'utilisation du Bluetooth, le système d'exploitation affiche une notification avec les options suivantes : rejeter ou autoriser. Ainsi, l'utilisateur peut refuser la restriction et continuer à utiliser le Bluetooth.

- Sur les appareils Blackview, l'utilisateur peut effacer la mémoire de l'application Kaspersky Endpoint Security for Android. Par conséquent, la protection et l'administation des appareils sont désactivées, tous les paramètres définis deviennent inefficaces et l'application Kaspersky Endpoint Security for Android est supprimée des fonctionnalités d'accessibilité. En effet, les appareils de ce fournisseur fournissent à l'application Écrans récents personnalisée des privilèges élevés. Cette application peut remplacer les paramètres de Kaspersky Endpoint Security for Android et ne peut pas être remplacée, car elle fait partie du système d'exploitation Android.

- Sur certains appareils fonctionnant sous Android 11, l'application Kaspersky Endpoint Security for Android se bloque immédiatement après le démarrage. Le problème est lié à un défaut bien connu dans Android 11.

Déploiement d'une solution d'administration des appareils mobiles dans Kaspersky Security Center Web Console ou Cloud Console

Pour gérer les appareils mobiles à l'aide de Kaspersky Security Center Web Console ou Cloud Console, vous devez déployer une solution d'administration des appareils mobiles.

Scénarios de déploiement

Déploiement dans Kaspersky Security Center Web Console

Le déploiement de la solution d'administration des appareils mobiles dans Kaspersky Security Center Web Console comprend les étapes suivantes :

1. Préparation de Kaspersky Security Center Web Console au déploiement
2. Déploiement des plug-ins d'administration
3. Déploiement de l'application Kaspersky Endpoint Security for Android
4. (Facultatif) Configuration de l'échange d'informations avec Firebase Cloud Messaging

   Il est recommandé d'effectuer cette étape pour garantir la remise rapide des commandes aux appareils mobiles et la synchronisation forcée lorsque les paramètres de stratégie sont modifiés.

Déploiement dans Kaspersky Security Center Cloud Console

Le déploiement de la solution d'administration des appareils mobiles dans Kaspersky Security Center Cloud Console comprend les étapes suivantes :

1. Préparation de Kaspersky Security Center Cloud Console au déploiement
2. Déploiement de l'application Kaspersky Endpoint Security for Android
3. (Facultatif) Configuration de l'échange d'informations avec Firebase Cloud Messaging

   Il est recommandé d'effectuer cette étape pour garantir la remise rapide des commandes aux appareils mobiles et la synchronisation forcée lorsque les paramètres de stratégie sont modifiés.

Préparation de Kaspersky Security Center Web Console et Cloud Console pour le déploiement

Cette section fournit des instructions sur la préparation de Kaspersky Security Center Web Console et de Cloud Console au déploiement.

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

Pour que les appareils mobiles puissent se connecter au Serveur d'administration, vous devez définir les paramètres de connexion des appareils mobiles dans les propriétés du Serveur d'administration avant d'installer l'application Kaspersky Endpoint Security for Android sur les appareils mobiles.

Pour définir les paramètres du Serveur d'administration pour la connexion des appareils mobiles :

1. Démarrez l'administration des appareils mobiles dans le Serveur d'administration.

   Vous pouvez démarrer l'administration des appareils mobiles lors de la configuration initiale de la Console d'administration basée sur MMC de Kaspersky Security Center (lors de l'exécution de l'Assistant de démarrage rapide) ou ultérieurement en affichant le dossier Administration des appareils mobiles dans la Console d'administration.

2. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, cliquez sur **Paramètres** ( ).

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

3. Configurez les ports du Serveur d'administration qui seront utilisés par les appareils mobiles :

   a. Choisissez la section **Ports supplémentaires**.

   b. Activez le bouton bascule **Ouvrir le port pour les appareils mobiles**.

   c. Dans le champ **Port pour la synchronisation des appareils mobiles**, spécifiez le port que les appareils mobiles utiliseront pour se connecter au Serveur d'administration.

      Le port 13292 est le port choisi par défaut.

      Si le bouton bascule **Ouvrir le port pour les appareils mobiles** est désactivé ou qu'un port invalide a été indiqué pour la connexion, les appareils mobiles ne pourront pas se connecter au Serveur d'administration.

   d. Dans le champ **Port d'activation des appareils mobiles**, indiquez le port par lequel les appareils mobiles se connecteront au Serveur d'administration pour l'activation de l'application Kaspersky Endpoint Security for Android.

      Le port 17100 est le port choisi par défaut.

      Si vous spécifiez un port de connexion incorrect, les utilisateurs des appareils mobiles ne pourront pas activer l'application Kaspersky Endpoint Security for Android à l'aide du Serveur d'administration.

4. Si nécessaire, modifiez le certificat qui sera utilisé par les appareils mobiles pour se connecter au Serveur d'administration.

   Par défaut, le Serveur d'administration utilise le certificat créé lors de l'installation du Serveur d'administration. Si vous le souhaitez, remplacez le certificat émis via le Serveur d'administration par un autre certificat ou réémettez le certificat émis via le Serveur d'administration.

   Pour modifier le certificat *:*

   a. Choisissez la section **Certificats**.

   b. Définissez les paramètres requis.

Pour plus d'informations sur les certificats, reportez-vous à l' *Aide de Kaspersky Security Center*.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées aux paramètres et quitter la fenêtre des propriétés du Serveur d'administration.

Après avoir configuré les paramètres de connexion des appareils mobiles, vous pouvez installer l'application Kaspersky Endpoint Security for Android sur les appareils mobiles et les connecter au Serveur d'administration en utilisant les paramètres spécifiés.

Création d'un groupe d'administration

Les stratégies de groupe servent à effectuer la configuration centralisée des applications Kaspersky Endpoint Security for Android installées sur les appareils mobiles des utilisateurs.

Pour appliquer une stratégie à un groupe d'appareils, il est conseillé de créer un groupe séparé pour ces appareils dans le dossier **Appareils administrés** avant l'installation des applications mobiles sur les appareils des utilisateurs.

Après la création du groupe d'administration, il est recommandé de configurer l'option de placement automatique dans ce groupe des appareils sur lesquels vous voulez installer les applications. Il faut ensuite définir les paramètres communs à l'ensemble des périphériques en utilisant une stratégie de groupe.

Pour créer un groupe d'administration :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **HIÉRARCHIE DES GROUPES** .

2. Dans la structure des groupes d'administration, sélectionnez le groupe d'administration qui doit inclure le nouveau groupe d'administration.

3. Cliquez sur le bouton **Ajouter**.

4. Dans la fenêtre **Nom du nouveau groupe d'administration** qui s'ouvre, saisissez un nom pour le groupe, puis cliquez sur le bouton **Ajouter.**

Un nouveau groupe d'administration portant le nom spécifié apparaît dans la hiérarchie des groupes d'administration.

Création d'une règle d'attribution automatique d'un périphérique aux groupes d'administration

Lorsque l'application Kaspersky Endpoint Security for Android est installée sur les appareils mobiles, ils s'affichent sur la page **DÉCOUVERTE ET DÉPLOIEMENT** > **APPAREILS NON DÉFINIS** de Kaspersky Security Center Web Console ou Cloud Console. Afin d'administrer les appareils nouvellement connectés, vous pouvez les déplacer manuellement vers un groupe d'administration ou créer une règle pour les attribuer automatiquement aux groupes d'administration.

Pour créer une règle d'attribution automatique des appareils mobiles aux groupes d'administration :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **DÉCOUVERTE ET DÉPLOIEMENT** > **DÉPLOIEMENT ET AFFECTATION** > **RÈGLES DE DÉPLACEMENT**.

2. Dans la fenêtre **Nouvelle règle** qui s'ouvre, cliquez sur le bouton **Ajouter**.

3. Dans le champ **Nom de la règle**, spécifiez le nom de la règle.

4. Dans le champ **Groupe d'administration**, choisissez le groupe d'administration dans lequel les appareils mobiles seront affectés une fois l'application Kaspersky Endpoint Security for Android installée sur ces derniers.

5. Dans le groupe **Appliquer la règle**, sélectionnez l'option **Appliquer une fois pour chacun des appareils**.

6. Cochez la case **Déplacer uniquement les appareils non ajoutés à un groupe d'administration** pour que les appareils mobiles déjà affectés à d'autres groupes d'administration ne soient pas déplacés suite à l'application de cette règle.

7. Cochez la case **Activer la règle** pour appliquer la règle immédiatement après l'avoir créée.

   Vous pouvez activer la règle à tout moment ultérieurement en utilisant le bouton bascule sur la page **RÈGLES DE DÉPLACEMENT**.

8. Sélectionnez **CONDITIONS DE LA RÈGLE** > **Applications** et procédez comme suit :

   a. Activez le bouton bascule de la **Version du système d'exploitation.**

   b. Dans la liste des systèmes d'exploitation qui s'ouvre, sélectionnez **Android**.

   La règle sera appliquée aux appareils Android. Vous devez spécifier au moins une condition pour créer une règle.

9. Cliquez sur **Enregistrer** pour créer la règle.

La règle nouvellement créée s'affiche sur la page **RÈGLES DE DÉPLACEMENT**. Conformément à la règle, Kaspersky Security Center attribuera tous les appareils Android nouvellement connectés au groupe d'administration sélectionné.

Pour des informations détaillées sur l'administration des groupes d'administration et les actions avec les appareils non définis :

- Si vous utilisez Kaspersky Security Center Web Console, veuillez consulter l'*Aide de Kaspersky Security Center*.
- Si vous utilisez Kaspersky Security Center Cloud Console, veuillez vous reporter à l'*Aide de Kaspersky Security Center Cloud Console*.

Déploiement des plug-ins d'administration

Pour administrer les appareils mobiles dans Kaspersky Security Center Web Console, les plug-ins d'administration suivants doivent être installés :

- Plug-in Kaspersky Security for Mobile
- Plug-in d'administration de Kaspersky Endpoint Security for Android

Si vous utilisez Kaspersky Security Center Cloud Console, vous n'avez pas besoin d'installer les plug-ins d'administration. Il vous suffit de créer un compte dans Kaspersky Security Center Cloud Console. Pour plus d'informations sur la création d'un compte, consultez l'*Aide de Kaspersky Security Center Cloud Console*.

Vous pouvez utiliser les méthodes suivantes pour installer les plug-ins d'administration :

- En utilisant l'Assistant de démarrage rapide de Kaspersky Security Center Web Console.

  Kaspersky Security Center Web Console vous invite automatiquement à exécuter l'Assistant de démarrage rapide une fois le Serveur d'administration installé et lorsque vous vous connectez à celui-ci pour la première fois. Vous pouvez également lancer l'Assistant de démarrage rapide manuellement à tout moment.

  Pour plus d'informations sur l'Assistant de démarrage rapide pour Kaspersky Security Center, veuillez consulter *l'Aide de Kaspersky Security Center*.

- En utilisant la liste des paquets de distribution disponibles dans Kaspersky Security Center Web Console.

  La liste des paquets de distribution disponibles est mise à jour automatiquement après la sortie des nouvelles versions des applications Kaspersky.

- Téléchargez les paquets de distribution à partir d'une source externe et ajoutez des plug-ins d'administration à Kaspersky Security Center Web Console.

  Les paquets de distribution du plug-in d'administration peuvent par exemple être téléchargés sur le site de Kaspersky.

Installation des plug-ins d'administration à partir de la liste des paquets de distribution disponibles

Pour installer les plug-ins d'administration, procédez comme suit :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console, sélectionnez **PARAMÈTRES DE LA CONSOLE** > **PLUG-INS WEB**.
2. Cliquez sur le bouton **Ajouter**.

   Cette opération ouvre la liste des versions mises à jour des applications Kaspersky.
3. Pour installer les plug-ins d'administration, procédez comme suit :

   a. Dans la liste des applications disponibles, cliquez sur la section **Android** pour la développer.

   b. Sélectionnez **Plug-in Kaspersky Security for Mobile**, puis cliquez sur **Installer le plug-in**.

   c. Sélectionnez **Plug-in Kaspersky Endpoint Security for Android**, puis cliquez sur **Installer le plug-in**.

Les paquets de distribution sont téléchargés et les plug-ins sont installés. Lorsque chaque plug-in est installé et ajouté à Kaspersky Security Center Web Console, une fenêtre de confirmation s'affiche.

Installation des plug-ins d'administration à partir du paquet de distribution

Vous pouvez télécharger le paquet de distribution sur le site Web de Kaspersky.

Pour installer Kaspersky Security for Mobile Plug-in à partir du paquet de distribution :

1. Copiez les fichiers `mobile_device_management.zip` et `signature.txt` du paquet de distribution sur le poste de travail de l'administrateur.
2. Dans la fenêtre principale de Kaspersky Security Center Web Console, sélectionnez **PARAMÈTRES DE LA CONSOLE** > **PLUG-INS WEB**.

3. Cliquez sur **Ajouter à partir du fichier**.
4. Dans la fenêtre **Ajouter à partir du fichier** qui s'ouvre, cliquez sur **Télécharger le fichier ZIP**, puis recherchez `mobile_device_management.zip`.
5. Cliquez sur **Télécharger la signature**, puis recherchez `signature.txt`.
6. Cliquez sur le bouton **Ajouter**.

Le plug-in Kaspersky Security for Mobile est installé et ajouté à Kaspersky Security Center Web Console.

Pour installer le plug-in Kaspersky Endpoint Security for Android à partir du paquet de distribution :

1. Copiez les fichiers `kes_android.zip` et `signature.txt` du paquet de distribution sur le poste de travail de l'administrateur.
2. Dans la fenêtre principale de Kaspersky Security Center Web Console, sélectionnez **PARAMÈTRES DE LA CONSOLE** > **PLUG-INS WEB**.
3. Cliquez sur **Ajouter à partir du fichier**.
4. Dans la fenêtre **Ajouter à partir du fichier** qui s'ouvre, cliquez sur **Télécharger le fichier ZIP**, puis recherchez `kes_android.zip`.
5. Cliquez sur **Télécharger la signature**, puis recherchez `signature.txt`.
6. Cliquez sur le bouton **Ajouter**.

Le plug-in Kaspersky Endpoint Security for Android est installé et ajouté à Kaspersky Security Center Web Console.

Vous pouvez vous assurer que les plug-ins d'administration ont été installés en consultant la liste des plug-ins installés sur la page **PARAMÈTRES DE LA CONSOLE** > **PLUG-INS WEB**.

Déploiement de l'application Kaspersky Endpoint Security for Android

Pour gérer les appareils mobiles dans Kaspersky Security Center Web Console ou Cloud Console, vous devez déployer l'application Kaspersky Endpoint Security for Android sur les appareils mobiles. Vous pouvez déployer l'application Kaspersky Endpoint Security for Android sur les appareils mobiles à l'aide de Kaspersky Security Center Web Console ou Cloud Console.

Déploiement de l'application Kaspersky Endpoint Security for Android à l'aide de Kaspersky Security Center Web Console ou Cloud Console

L'application Kaspersky Endpoint Security for Android est déployée sur les appareils mobiles des utilisateurs dont le compte a été ajouté à Kaspersky Security Center. Pour plus d'informations sur les comptes d'utilisateurs dans Kaspersky Security Center :

- Si vous utilisez Kaspersky Security Center Web Console, veuillez consulter l'*Aide de Kaspersky Security Center*.

- Si vous utilisez Kaspersky Security Center Cloud Console, veuillez vous reporter à l'*Aide de Kaspersky Security Center Cloud Console*.

Vous pouvez utiliser le plug-in Kaspersky Security for Mobile pour installer l'application à partir de Kaspersky Security Center Web Console et Cloud Console en envoyant un lien Google Play vers un appareil mobile.

L'utilisateur reçoit un lien vers Google Play. L'installation s'effectue selon la méthode classique sur la plateforme Android. Après l'installation de l'application Kaspersky Endpoint Security for Android, l'utilisateur doit fournir les autorisations requises.

Certains appareils Huawei et Honor qui ne disposent pas des services Google et donc d'un accès aux applications de Google Play. Si certains utilisateurs d'appareils Huawei et Honor ne peuvent pas installer l'application à partir de Google Play, il faut leur demander d'installer l'application à partir de Huawei App Gallery.

Le lien contient les données suivantes :

- Paramètres de synchronisation de Kaspersky Security Center
- Certificat commun

Pour déployer l'application Kaspersky Endpoint Security for Android sur un appareil mobile :

1. Lancez l'Assistant de connexion d'un nouvel appareil mobile.

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS** , puis cliquez sur **Ajouter**.
   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **UTILISATEURS ET RÔLES** > **UTILISATEURS**. Cliquez sur le nom de l'utilisateur ou du groupe d'utilisateurs auquel vous souhaitez envoyer le lien pour connecter un appareil mobile, puis sélectionnez **APPAREILS.** Cliquez sur **Ajouter un appareil mobile**, puis passez à l'étape 3.

   Continuez dans l'Assistant en utilisant le bouton **Suivant**.

2. Sélectionnez l'utilisateur ou le groupe d'utilisateurs auquel vous souhaitez envoyer le lien pour connecter un appareil mobile.

3. Sélectionnez l'adresse email à laquelle le lien sera envoyé :

   - **Toutes les adresses email**
   - **Adresse email principale**
   - **Adresse email alternative**
   - **Une autre adresse email**

     Si vous sélectionnez cette option, indiquez l'adresse email ci-dessous.

4. Le résumé du lien s'affiche.

   Assurez-vous que tous les paramètres du lien sont corrects, puis cliquez sur **OK**.

5. Une fenêtre s'ouvre avec une confirmation que le lien pour ajouter un appareil mobile a été envoyé.

   Fermez la fenêtre.

Lorsque l'utilisateur installe l'application Kaspersky Endpoint Security for Android, l'appareil de l'utilisateur s'affiche dans l'onglet **APPAREILS** > **MOBILE** > **APPAREILS** de Web Console ou Cloud Console.

Après que Kaspersky Endpoint Security for Android a été installé sur les appareils mobiles des utilisateurs, vous pouvez configurer les paramètres des appareils et des applications à l'aide de stratégies de groupe. Vous pouvez également envoyer des commandes aux appareils mobiles pour protéger les données en cas de perte ou de vol des appareils.

Activation de l'application Kaspersky Endpoint Security for Android

Dans Kaspersky Security Center, la licence peut couvrir différents groupes fonctionnels. Pour être sûr que l'application Kaspersky Endpoint Security for Android est entièrement fonctionnelle, la licence Kaspersky Security Center achetée par l'organisation doit couvrir la fonction **Administration des appareils mobiles**. La fonction **Gestion des appareils mobiles** permet de connecter des appareils mobiles à Kaspersky Security Center et de les gérer.

Pour plus d'informations sur les licences de Kaspersky Security Center et les options de licence :

- Si vous utilisez Kaspersky Security Center Web Console, veuillez consulter l'*Aide de Kaspersky Security Center*.
- Si vous utilisez Kaspersky Security Center Cloud Console, veuillez vous reporter à l'*Aide de Kaspersky Security Center Cloud Console*.

L'activation de l'application Kaspersky Endpoint Security for Android sur un appareil mobile s'effectue en fournissant des informations de licence valides à l'application. Les informations sur la licence sont transmises à l'appareil mobile avec la stratégie lors de la synchronisation de l'appareil avec Kaspersky Security Center.

Si Kaspersky Endpoint Security for Android n'est pas activé dans les 30 jours qui suivent l'installation sur l'appareil mobile, l'application passe automatiquement en mode limité. Dans ce mode de fonctionnement, la majorité des composants de l'app est inopérationnelle. Lorsque l'application passe en mode limité, elle ne réalise plus la synchronisation automatique avec Kaspersky Security Center. Dès lors, si l'application n'est pas activée pour une raison quelconque dans les 30 jours qui suivent l'installation, l'utilisateur doit synchroniser l'appareil avec Kaspersky Security Center manuellement.

Si Kaspersky Security Center n'est pas déployé dans votre organisation ou s'il n'est pas accessible aux appareils mobiles, les utilisateurs peuvent activer manuellement l'application Kaspersky Endpoint Security for Android sur leurs appareils.

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

1. Ouvrez la fenêtre des propriétés de la stratégie :
   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.
   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**
2. Dans la page des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **Licences**.

3. Utilisez la liste déroulante pour sélectionner la clé de licence requise dans le stockage des clés du Serveur d'administration.

   Les détails de la clé de licence s'affichent dans les champs ci-dessous.

   Vous pouvez remplacer la clé d'activation existante sur l'appareil mobile si elle est différente de celle sélectionnée dans la liste déroulante ci-dessus. Pour cela, cochez la case **Si la clé sur l'appareil diffère, replacez-la par cette clé**.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Fournir les autorisations requises pour l'application Kaspersky Endpoint Security for Android

Certaines fonctionnalités de l'application Kaspersky Endpoint Security for Android nécessitent des autorisations. Kaspersky Endpoint Security for Android demande des autorisations obligatoires pendant l'installation, ainsi qu'après l'installation et avant d'utiliser les fonctionnalités individuelles de l'application. Sans octroi des autorisations obligatoires, il est impossible d'installer Kaspersky Endpoint Security for Android.

Sur certains appareils (par exemple, Huawei, Meizu, Xiaomi) il faut ajouter manuellement Kaspersky Endpoint Security for Android à la liste des applications lancées au chargement du système d'exploitation dans les paramètres de l'appareil. Si l'application n'est pas ajoutée à la liste, Kaspersky Endpoint Security for Android cesse d'exécuter toutes les fonctions après le redémarrage de l'appareil mobile.

Sur les appareils exécutant Android 11 ou version ultérieure, vous devez désactiver le paramètre système **Supprimer les autorisations si l'application n'est pas utilisée**. Sinon, après quelques mois d'inutilisation de l'application, le système réinitialise automatiquement les autorisations que l'utilisateur a accordées à l'application.

Autorisations demandées par l'application Kaspersky Endpoint Security for Android

Autorisation	Fonction de l'application
Téléphone (obligatoire uniquement pour Android 5.0 à 9.X)	Connexion à Kaspersky Security Center (identifiant de l'appareil)
Stockage (obligatoire)	Anti-Virus
Accès pour gérer tous les fichiers	Antivirus (seulement pour Android 11 et version ultérieure)
Administrateur de l'appareil (obligatoire)	Antivol : verrouillage de l'appareil (seulement pour Android 5.0 à 6.X)
	Antivol : prendre une photo avec la caméra avant

	Bien que la prise de photos ne soit pas prise en charge dans Kaspersky Security Center Web Console et Cloud Console, l'application Kaspersky Endpoint Security for Android requiert cette autorisation afin qu'elle puisse être gérée par toutes les consoles Kaspersky Security Center.
	Antivol : reproduction de l'alarme
	Antivol : rétablissement des paramètres par défaut
	Protection par mot de passe
	Protection contre la suppression de l'application
	Installation des certificats de sécurité
	Contrôle des applications installées
	Restriction de l'utilisation de la caméra, Bluetooth, Wi-Fi
Appareil photo	Antivol : prendre une photo avec la caméra avant Bien que la prise de photos ne soit pas prise en charge dans Kaspersky Security Center Web Console et Cloud Console, l'application Kaspersky Endpoint Security for Android requiert cette autorisation afin qu'elle puisse être gérée par toutes les consoles Kaspersky Security Center. Sur les appareils tournant sous Android 11.0 ou une version ultérieure, l'utilisateur doit accorder la permission "Pendant l'utilisation de l'application" lorsqu'il y est invité.
Localisation	Antivol : définition de l'emplacement de l'appareil Sur les appareils tournant sous Android 10.0 ou une version ultérieure, l'utilisateur doit accorder l'autorisation "Tout le temps" lorsqu'il y est invité
Fonctionnalités d'accessibilité	Antivol : verrouillage de l'appareil (seulement pour Android 7.0 et version ultérieure)
	Protection Internet
	Contrôle des applications installées
	Protection de la suppression de l'application (seulement pour Android 7.0 et version ultérieure)
	Affichage des avertissements de Kaspersky Endpoint Security for Android (seulement Android 10.0 et version ultérieure)
	Restreindre l'utilisation de l'appareil photo (uniquement pour Android 11 ou version ultérieure)

Administration des certificats

Les certificats mobiles sont utilisés dans le but d'identifier les utilisateurs d'appareils mobiles sur le Serveur d'administration.

Kaspersky Security Center Web Console et Cloud Console vous permettent d'effectuer les actions suivantes avec les certificats mobiles des utilisateurs :

- Consultez les certificats et leurs statuts.
- Créez de nouveaux certificats.
- Renouvelez les certificats expirés.
- Supprimez les certificats.

Pour plus d'informations sur les certificats Kaspersky Security Center :

- Si vous utilisez Kaspersky Security Center Web Console, veuillez consulter l'*Aide de Kaspersky Security Center*.
- Si vous utilisez Kaspersky Security Center Cloud Console, veuillez vous reporter à l'*Aide de Kaspersky Security Center Cloud Console*.

Affichage de la liste des certificats

Kaspersky Security Center Web Console et Cloud Console vous permettent d'afficher les certificats mobiles des utilisateurs appliqués, leurs statuts et leurs propriétés.

Pour afficher la liste des certificats mobiles utilisateur appliqués :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**.
2. Sélectionnez **Administrer les certificats**.

   La page **Certificats mobiles** s'ouvre avec des informations sur les certificats mobiles utilisateur appliqués. Vous pouvez afficher les détails d'un certificat en cliquant dessus dans la colonne **Nom d'utilisateur**

Définition des paramètres de certificat

Vous pouvez utiliser Kaspersky Security Center Web Console ou Cloud Console pour configurer la durée de vie, les mises à jour automatiques et la protection par mot de passe des certificats mobiles.

Pour définir les paramètres de certificat mobile :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**.
2. Sélectionnez **Administrer les certificats**.
3. Sélectionnez **Réglages des certificats**.
4. Dans la fenêtre **Générer des certificats mobiles** qui s'ouvre, vous pouvez configurer les éléments suivants :

- **Validité du mot du certificat (jours)**

  Durée de vie du certificat en jours. La durée de vie par défaut d'un certificat est de 365 jours. A l'expiration de ce délai, l'appareil mobile ne pourra plus se connecter au Serveur d'administration.

- **Réémettre quand le certificat expire dans (jours)**

  Le nombre de jours restants jusqu'à l'expiration du certificat actuel pendant lesquels le Serveur d'administration doit émettre un nouveau certificat. Par exemple, si la valeur du champ est 4, le Serveur d'administration émet un nouveau certificat quatre jours avant l'expiration du certificat actuel. La valeur par défaut est 1.

- **Émettre à nouveau le certificat automatiquement le cas échéant**

  Si possible, les certificats seront réémis automatiquement. Si cette option est désactivée, les certificats doivent être réémis manuellement lorsqu'ils expirent. Par défaut, cette option est désactivée.

- **Demander la saisie du mot de passe lors de l'installation du certificat**

  L'utilisateur sera invité à saisir un mot de passe lors de l'installation du certificat sur un appareil mobile. Le mot de passe n'est utilisé qu'une seule fois, lors de l'installation du certificat sur l'appareil mobile. Le mot de passe sera généré automatiquement par le Serveur d'administration et envoyé à l'utilisateur par message électronique. Vous pouvez spécifier la longueur du mot de passe dans le champ **Longueur du mot de passe**.

5. Cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

Les paramètres spécifiés seront utilisés par Kaspersky Security Center pour créer, mettre à jour et protéger les certificats mobiles.

Création d'un certificat

Vous pouvez créer des certificats mobiles dans Kaspersky Security Center Web Console et Cloud Console dans le but d'identifier les utilisateurs des appareils mobiles.

Pour créer un certificat mobile :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**.

2. Sélectionnez **Administrer les certificats**.

3. Dans la fenêtre **Certificats mobiles** qui s'ouvre, cliquez sur **Ajouter** pour démarrer l'**Assistant de création de certificat mobile**. Continuez dans l'Assistant en utilisant le bouton **Suivant**.

4. Sélectionnez les utilisateurs ou les groupes d'utilisateurs dont vous souhaitez gérer les appareils mobiles avec un nouveau certificat.

5. Spécifiez les **Paramètres de publication** :

   - Si vous souhaitez informer les utilisateurs du nouveau certificat, cochez la case **Prévenir l'utilisateur au sujet du nouveau certificat**.

   - Si vous souhaitez autoriser l'utilisation d'un même certificat plusieurs fois sur le même appareil, cochez la case **Autoriser l'utilisation d'un certificat à plusieurs reprises sur le même appareil (uniquement pour les appareils dotés de Kaspersky Endpoint Security for Android)**.

6. Sélectionnez le **Type d'authentification** :

- Sélectionnez **Identifiants (connexion au domaine ou nom d'utilisateur)** si vous souhaitez que les utilisateurs accèdent au certificat à l'aide de leurs identifiants.

- Sélectionnez **Mot de passe à usage unique** si vous souhaitez que les utilisateurs accèdent au certificat à l'aide d'un mot de passe à usage unique.

  Cette option est disponible si vous n'avez pas coché la case **Autoriser l'utilisation d'un certificat à plusieurs reprises sur le même appareil (uniquement pour les appareils dotés de Kaspersky Endpoint Security for Android)** à l'étape précédente.

- Sélectionnez **Mot de passe** si vous souhaitez que les utilisateurs accèdent au certificat à l'aide d'un mot de passe.

  Cette option est disponible si vous avez coché la case **Autoriser l'utilisation d'un certificat à plusieurs reprises sur le même appareil (uniquement pour les appareils dotés de Kaspersky Endpoint Security for Android)** à l'étape précédente.

7. Spécifiez la méthode de livraison du certificat dans le champ **Remise du certificat** :

   - Si vous avez sélectionné **Mot de passe à usage unique** à l'étape précédente, sélectionnez l'une des options suivantes :

     - Si vous souhaitez envoyer le mot de passe par email, sélectionnez **Prévenir l'utilisateur par email**.

       Sélectionnez ensuite l'adresse email à utiliser ou sélectionnez **Une autre adresse email** pour spécifier une autre adresse email.

     - Si vous souhaitez informer les utilisateurs du mot de passe par d'autres moyens, sélectionnez **Afficher le mot de passe à la fin de l'assistant**.

   - Si vous avez sélectionné **Identifiants (connexion au domaine ou nom d'utilisateur)** à l'étape précédente, sélectionnez l'adresse email à utiliser ou sélectionnez **Une autre adresse email** pour spécifier une autre adresse e-mail.

8. Le résumé du certificat s'affiche.

   Assurez-vous que tous les paramètres sont corrects, puis cliquez sur **Créer**.

Au terme de l'exécution de **Assistant de création de certificat mobile**, un certificat commun sera créé et pourra être installé par les utilisateurs sur leurs appareils mobiles. Le certificat devient disponible après la prochaine synchronisation des appareils mobiles avec Kaspersky Security Center.

Pour plus d'informations sur la création de certificats et la configuration de leurs règles d'émission :

- Si vous utilisez Kaspersky Security Center Web Console, veuillez consulter l'*Aide de Kaspersky Security Center*.

- Si vous utilisez Kaspersky Security Center Cloud Console, veuillez vous reporter à l'*Aide de Kaspersky Security Center Cloud Console*.

Renouvellement d'un certificat

Si l'un des certificats mobiles appliqués est sur le point d'expirer, vous pouvez le renouveler en utilisant Kaspersky Security Center Web Console ou Cloud Console.

Pour renouveler un certificat mobile :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**.

2. Sélectionnez **Administrer les certificats**.

3. Sélectionnez le certificat que vous souhaitez renouveler, puis cliquez sur **Réémission**.

   Le statut du certificat passe à **Le certificat a été réémis**.

Suppression d'un certificat

Vous pouvez supprimer les certificats mobiles en utilisant Kaspersky Security Center Web Console ou Cloud Console.

Si vous supprimez un certificat mobile, l'appareil ne peut plus se synchroniser avec le Serveur d'administration et ne peut pas être administré via Kaspersky Security Center. Pour recommencer à administrer l'appareil mobile, vous devez réinstaller l'application Kaspersky Endpoint Security for Android dessus.

Pour supprimer un certificat mobile :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**.

2. Sélectionnez **Administrer les certificats**.

3. Sélectionnez le certificat que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

   Le certificat est supprimé et retiré de la liste des certificats.

Échange d'informations avec Firebase Cloud Messaging

Kaspersky Endpoint Security for Android utilise le service Firebase Cloud Messaging (FCM) pour un envoi opportun des commandes aux appareils mobiles et une synchronisation forcée en cas de modification des paramètres de la stratégie.

Pour utiliser le service Firebase Cloud Messaging, vous devez configurer les paramètres du service dans Kaspersky Security Center Web Console ou Cloud Console.

Pour activer Firebase Cloud Messaging dans Kaspersky Security Center Web Console ou Cloud Console :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **SYNCHRONISATION DES APPAREILS ANDROID**.

   La fenêtre de **Synchronisation des appareils Android** s'ouvre.

2. Dans les champs **Identifiant de l'expéditeur** et **Clé du serveur**, spécifiez les paramètres de Firebase Cloud Messaging : SENDER_ID et Clé API.

   Firebase Cloud Messaging est activé.

Pour obtenir un Identifiant d'expéditeur et la Clé de serveur :

1. Inscrivez-vous sur le portail Google.
2. Accédez à Google Cloud Platform.
3. Créez un projet.

   Attendez que le projet soit créé.
4. Recherchez le SENDER_ID pertinent du projet.
5. Activez Google Firebase Cloud Messaging pour Android.
6. Suivez les instructions à l'écran pour créer des identifiants.
7. Récupérez la clé API à partir des propriétés des nouveaux identifiants.

Pour des informations détaillées sur les opérations dans Google Cloud Platform, veuillez consulter la documentation correspondante .

Vous disposez maintenant d'un **Identifiant de l'expéditeur** et d'une **Clé du serveur** pour configurer les paramètres de Firebase Cloud Messaging.

Si les paramètres de Firebase Cloud Messaging ne sont pas définis, les commandes sur l'appareil seront exécutées et les paramètres de la stratégie seront envoyés pendant la synchronisation de l'appareil avec Kaspersky Security Center d'après la programmation définie dans la stratégie (par exemple, toutes les 24 h.). Ainsi, les commandes et les paramètres de la stratégie seront envoyés avec du retard.

Pour garantir le fonctionnement général du produit, vous acceptez automatiquement d'accorder au service Firebase Cloud Messaging l'identifiant unique d'instance de l'application (Instance ID) ainsi que les données suivantes :

- les informations sur le logiciel installé : la version de l'application, l'identifiant de l'application, la version de l'application, le nom du paquet de l'application ;
- les informations sur l'ordinateur sur lequel est installé le logiciel : la version du système d'exploitation, l'identifiant de l'appareil, la version des services Google ;
- les informations sur FCM : l'identifiant de l'application dans FCM, l'identifiant de l'utilisateur FCM, la version du protocole.

Les données sont transmises aux services Firebase via un canal sécurisé. L'accès et la protection des informations sont régis par les conditions d'utilisation pertinentes des services Firebase : Conditions relatives au traitement des données et à la sécurité de Firebase, Confidentialité et sécurité dans Firebase.

Pour interdire l'échange d'informations avec le service Firebase Cloud Messaging, procédez comme suit :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **SYNCHRONISATION DES APPAREILS ANDROID**.

   La fenêtre de **Synchronisation des appareils Android** s'ouvre.
2. Cliquez sur **Effacer**.
3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **OK** pour confirmer la réinitialisation.

Les paramètres de Firebase Cloud Messaging sont effacés.

Administration des appareils mobiles dans Kaspersky Security Center Web Console et Cloud Console

Vous pouvez administrer les appareils mobiles dans Kaspersky Security Center Web Console et Cloud Console en utilisant des stratégies de groupe et en envoyant des commandes aux appareils mobiles.

Pour administrer les appareils mobiles dans Kaspersky Security Center Web Console, vous devez installer les plug-ins d'administration.

Connexion des appareils mobiles à Kaspersky Security Center

Pour administrer un appareil mobile à l'aide de Kaspersky Security Center Web Console ou Cloud Console, l'appareil doit être connecté à Kaspersky Security Center. Vous pouvez consulter la liste des appareils mobiles connectés à Kaspersky Security Center dans l'onglet **APPAREILS** > **MOBILE** > **APPAREILS** de Web Console ou Cloud Console.

Pour connecter un appareil mobile à Kaspersky Security Center :

1. Lancez l'Assistant de connexion d'un nouvel appareil mobile.

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS** , puis cliquez sur **Ajouter**.
   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **UTILISATEURS ET RÔLES** > **UTILISATEURS**. Cliquez sur le nom de l'utilisateur ou du groupe d'utilisateurs auquel vous souhaitez envoyer le lien pour connecter un appareil mobile, puis sélectionnez **APPAREILS.** Cliquez sur **Ajouter un appareil mobile**, puis passez à l'étape 3.

   Continuez dans l'Assistant en utilisant le bouton **Suivant**.

2. Sélectionnez l'utilisateur ou le groupe d'utilisateurs auquel vous souhaitez envoyer le lien pour connecter un appareil mobile.

3. Sélectionnez l'adresse email à laquelle le lien sera envoyé :

   - **Toutes les adresses email**
   - **Adresse email principale**
   - **Adresse email alternative**
   - **Une autre adresse email**

     Si vous sélectionnez cette option, indiquez l'adresse email ci-dessous.

4. Le résumé du lien s'affiche.

   Assurez-vous que tous les paramètres du lien sont corrects, puis cliquez sur **OK**.

5. Une fenêtre s'ouvre avec une confirmation que le lien pour ajouter un appareil mobile a été envoyé.

Fermez la fenêtre.

Lorsque l'utilisateur installe l'application Kaspersky Endpoint Security for Android, l'appareil de l'utilisateur s'affiche dans l'onglet **APPAREILS** > **MOBILE** > **APPAREILS** de Web Console ou Cloud Console.

Déplacement des appareils mobiles non définis vers des groupes d'administration

Lorsque l'application Kaspersky Endpoint Security est installée sur les appareils mobiles, ils s'affichent sur la page **DÉCOUVERTE ET DÉPLOIEMENT** > **APPAREILS NON DÉFINIS** de Kaspersky Security Center Web Console ou Cloud Console. Afin d'administrer les appareils nouvellement connectés, vous pouvez créer une règle pour leur attribution automatique aux groupes d'administration ou les déplacer manuellement vers un groupe d'administration.

Pour déplacer un appareil mobile non défini vers un groupe d'administration :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **DÉCOUVERTE ET DÉPLOIEMENT** > **APPAREILS NON DÉFINIS**.
2. Sélectionnez l'appareil que vous souhaitez déplacer vers un groupe d'administration, puis cliquez sur **Déplacer vers le groupe**.
3. Dans l'arborescence des groupes d'administration qui s'ouvre, sélectionnez le groupe cible vers lequel vous souhaitez déplacer l'appareil.

   Vous pouvez créer un nouveau groupe d'administration en sélectionnant un groupe existant, puis en cliquant sur **Ajouter un groupe enfant**.
4. Cliquez sur **Déplacer**.

L'appareil est déplacé vers le groupe d'administration spécifié et la stratégie de groupe lui est appliquée.

Envoi de commandes aux périphériques mobiles

Vous pouvez envoyer des commandes aux appareils mobiles pour protéger les données d'un appareil mobile perdu ou volé, ou pour effectuer une synchronisation forcée d'un appareil mobile avec Kaspersky Security Center.

Vous pouvez utiliser Kaspersky Security Center Web Console ou Cloud Console pour envoyer les commandes suivantes :

- **Verrouiller l'appareil**

  L'appareil mobile est verrouillé.
- **Déverrouiller l'appareil**

  L'appareil mobile est déverrouillé. Sur les appareils tournant sous le système d'exploitation Android version 5.0 à 6.X, le mot de passe de déverrouillage de l'écran (code PIN) de l'appareil sera remplacé par "1234" après le déverrouillage de l'appareil mobile. Sur les appareils tournant sous le système d'exploitation Android 7.0 et suivant, le mot de passe de déverrouillage de l'écran reste inchangé après le déverrouillage de l'appareil mobile.
- **Rétablir les paramètres par défaut**

Toutes les données sont supprimées de l'appareil mobile et les paramètres de configuration sont réinitialisés à leurs valeurs par défaut.

- **Supprimer les données d'entreprise**

  Les données conteneurisées et le compte email de l'entreprise sont effacés de l'appareil mobile.

- **Géolocaliser l'appareil**

  La géolocalisation est déterminée et apparaît sur Google Maps. Le fournisseur de services mobiles peut facturer des frais d'accès à Internet.

  Sur les appareils tournant sous Android 12 ou version ultérieure, si l'utilisateur a accordé l'autorisation "Utiliser l'emplacement approximatif", l'application Kaspersky Endpoint Security for Android essaie d'abord d'obtenir l'emplacement précis de l'appareil. En cas d'échec, l'emplacement approximatif de l'appareil n'est renvoyé que s'il n'a pas été reçu plus de 30 minutes plus tôt. Sinon, la commande **Géolocaliser l'appareil** échoue.

- **Activer l'alarme**

  L'appareil mobile émet l'alarme. L'alarme est émise pendant 5 minutes (ou 1 minute si le niveau de la batterie est faible).

- **Synchroniser l'appareil**

  L'appareil mobile est synchronisé avec Kaspersky Security Center.

L'application Kaspersky Endpoint Security for Android nécessite des autorisations spécifiques pour l'exécution des commandes. Pendant le fonctionnement de l'Assistant de configuration initiale, Kaspersky Endpoint Security for Android propose à l'utilisateur d'accorder les autorisations requises à l'app. L'utilisateur peut ignorer ces étapes ou désactiver les droits ultérieurement dans les paramètres de l'appareil. Dans ce cas, l'exécution des commandes est impossible.

Sur les appareils tournant sous Android 10.0 ou une version ultérieure, l'utilisateur doit accorder l'autorisation "Tout le temps" pour accéder à la localisation. Sur les appareils tournant sous Android 11.0 ou une version ultérieure, l'utilisateur doit également accorder l'autorisation "Pendant l'utilisation de l'application" pour accéder à la caméra. Sinon, les commandes Antivol ne fonctionnent pas. L'utilisateur sera informé de cette limitation, et sera à nouveau invité à accorder le niveau requis d'autorisations. Si l'utilisateur sélectionne l'option "Seulement cette fois" pour l'autorisation de la caméra, l'accès est considéré comme accordé par l'application. Il est recommandé de contacter directement l'utilisateur si l'autorisation de la caméra est à nouveau demandée.

Pour envoyer une commande à un appareil mobile :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**.
2. Sélectionnez l'appareil auquel vous souhaitez envoyer la commande, puis cliquez sur **Contrôle** ou **Administrer**.
3. Sélectionnez la commande requise dans la liste **Commandes disponibles**, puis cliquez sur **OK**.
4. Cliquez sur **OK** si vous êtes invité à confirmer l'opération.

La commande spécifiée est envoyée à l'appareil mobile et la fenêtre de confirmation s'affiche.

Suppression des appareils mobiles de Kaspersky Security Center

Si vous n'avez plus besoin d'administrer un appareil mobile, vous pouvez le supprimer de Kaspersky Security Center à l'aide de Web Console ou Cloud Console.

Pour supprimer un appareil mobile de Kaspersky Security Center :

1. Supprimez l'application Kaspersky Endpoint Security de l'appareil mobile.
2. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**.
3. Sélectionnez l'appareil mobile que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
4. Cliquez sur **OK** pour confirmer l'opération.

L'appareil est supprimé de Kaspersky Security Center.

Administration des stratégies de groupe

Cette section décrit comment administrer les stratégies de groupe dans Kaspersky Security Center Web Console et Cloud Console.

Stratégies de groupe pour l'administration des appareils mobiles

Une *stratégie de groupe* est un ensemble unique de paramètres pour l'administration des appareils mobiles appartenant à un groupe d'administration, et des applications mobiles qui y sont installées.

Une stratégie permet de configurer les paramètres de appareils 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.

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

Les valeurs de paramètres définies dans la stratégie et dans les paramètres locaux de l'application sont enregistrées sur le Serveur d'administration. Elles sont diffusées sur les appareils mobiles lors de la synchronisation et sont considérées comme des paramètres actifs. 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 préserver l'actualité de la sécurité d'entreprise sur les appareils mobiles, vous pouvez contrôler la conformité des appareils des utilisateurs aux exigences de sécurité de l'entreprise.

Pour plus d'informations sur l'administration des stratégies et des groupes d'administration dans Kaspersky Security Center Web Console et Cloud Console :

- Si vous utilisez Kaspersky Security Center Web Console, veuillez consulter l'*Aide de Kaspersky Security Center*.
- Si vous utilisez Kaspersky Security Center Cloud Console, veuillez vous reporter à l'*Aide de Kaspersky Security Center Cloud Console*.

Affichage de la liste des stratégies de groupe

Kaspersky Security Center Web Console et Cloud Console vous permettent d'afficher les stratégies de groupes, leurs statuts et leurs propriétés.

Pour consulter la liste des stratégies de groupe, procédez comme suit :

Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**.

La liste des stratégies de groupe s'ouvre avec de brèves informations sur les stratégies de groupe. Sur cette page, vous pouvez créer, modifier, copier, déplacer et supprimer des stratégies de groupe.

Affichage des résultats de la distribution des stratégies

Kaspersky Security Center Web Console et Cloud Console vous permettent d'afficher le tableau de distribution d'une stratégie de groupe et des informations sur tous les appareils qui relèvent de cette stratégie.

Pour afficher les résultats de distribution d'une stratégie de groupe :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**.
2. Dans la liste des stratégies de groupe qui s'ouvre, cochez la case en regard du nom de la stratégie pour laquelle vous souhaitez afficher les résultats de la distribution, puis cliquez sur **Distribution**.

La page des résultats de la distribution des stratégies s'ouvre. Cette page contient le résumé de la stratégie, le tableau de distribution des stratégies et le tableau contenant des informations sur tous les appareils qui relèvent de cette stratégie. Vous pouvez ouvrir la fenêtre des propriétés de la stratégie en cliquant sur le bouton **Configurer la stratégie**.

Création d'une stratégie de groupe

Kaspersky Security Center Web Console et Cloud Console vous permettent de créer des stratégies de groupe dans le but d'administrer les appareils mobiles.

Pour supprimer une stratégie de groupe, procédez comme suit :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**.
2. Dans la liste des stratégies de groupe de Kaspersky Security Center qui s'ouvre, cliquez sur **Chemin actuel** pour sélectionner le groupe d'administration pour lequel vous souhaitez créer une stratégie.

   Par défaut, la nouvelle stratégie de groupe est appliquée au groupe **Appareils administrés**.

3. Cliquez sur **Ajouter** pour démarrer l'Assistant de création de stratégie. Continuez dans l'Assistant en utilisant le bouton **Suivant**.

4. Sélectionnez **Kaspersky Endpoint Security for Android**.

5. Saisissez 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.

6. Sélectionnez l'état de la stratégie :

   - **Actif**

     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.

   - **Inactif**

     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.

7. Vous pouvez activer ou désactiver deux options d'héritage, **Hériter des paramètres de la stratégie parent** et **Forcer l'héritage des paramètres dans les stratégies enfants** :

   - Si vous activez **Hériter des paramètres de la stratégie parent** pour un groupe d'administration enfant et que vous verrouillez certains paramètres dans la stratégie parent, vous ne pouvez pas modifier ces paramètres dans la stratégie du groupe enfant. Vous pouvez toutefois modifier les paramètres qui ne sont pas verrouillés dans la stratégie parent.

   - Si vous désactivez **Hériter des paramètres de la stratégie parent** pour un groupe d'administration enfant , vous pouvez modifier tous les paramètres du groupe enfant, même si certains paramètres sont verrouillés dans la stratégie parent.

   - Si vous activez **Forcer l'héritage des paramètres dans les stratégies enfants** dans le groupe d'administration parent , cela active l'option **Hériter des paramètres de la stratégie parent** pour chaque stratégie enfant. Dans ce cas, vous ne pouvez pas désactiver cette option pour une stratégie enfant. Tous les paramètres verrouillés dans la stratégie parent sont hérités de force dans les groupes enfants et vous ne pouvez pas modifier ces paramètres dans les groupes enfants.

   - Dans les stratégies du groupe **Appareils administrés**, l'option **Hériter des paramètres de la stratégie parent** n'affecte aucun paramètre, car le **groupe Appareils administrés** n'a aucun groupe en amont et n'hérite donc d'aucune stratégie.

   Par défaut, l'option **Hériter des paramètres de la stratégie parent** est activée et l'option **Forcer l'héritage des paramètres dans les stratégies enfants** est désactivée.

8. Si vous le souhaitez, vous pouvez définir les paramètres de la stratégie nouvellement créée. Pour ce faire, sélectionnez l'onglet **PARAMÈTRES DE L'APPLICATION**, puis procédez comme décrit dans la section "Définition des paramètres de la stratégie".

   Vous pouvez également le faire plus tard.

9. Cliquez sur **Enregistrer** pour créer la stratégie.

Une nouvelle stratégie de groupe pour l'administration des appareils mobiles est créée.

Modification d'une stratégie de groupe

Kaspersky Security Center Web Console et Cloud Console vous permettent de modifier les paramètres des stratégies de groupe.

Pour supprimer une stratégie de groupe, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie :

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**

2. Dans la fenêtre des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION**, puis définissez les paramètres de la stratégie comme décrit dans la section "Définition des paramètres de la stratégie".

   Vous pouvez également configurer les paramètres généraux, l'héritage des paramètres, la journalisation des événements et les notifications, les profils de stratégie et afficher l'historique des révisions. Pour en savoir plus, consultez *l'Aide de Kaspersky Security Center*.

3. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Copie d'une stratégie de groupe

Kaspersky Security Center Web Console et Cloud Console vous permettent de créer une copie d'une stratégie de groupe.

Pour créer une copie d'une stratégie de groupe :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**.

2. Dans la liste des stratégies de groupe qui s'ouvre, cochez la case en regard du nom de la stratégie pour laquelle vous souhaitez créer une copie, puis cliquez sur **Copier** .

3. Dans l'arborescence des groupes d'administration qui s'ouvre, sélectionnez le groupe cible dans lequel vous souhaitez créer une copie de la stratégie.

   Vous pouvez créer un nouveau groupe d'administration en sélectionnant un groupe existant, puis en cliquant sur **Ajouter un groupe enfant**.

4. Cliquez sur **Copier**.

5. Cliquez sur **OK** pour confirmer l'opération.

Une copie de la stratégie sera créée dans le groupe cible sous le même nom. L'état de chaque stratégie copiée ou déplacée dans le groupe cible sera **Inactif**. Vous pouvez remplacer l'état en **Actif** à tout moment.

Si une stratégie avec un nom identique à celui de la stratégie nouvellement créée ou déplacée existe déjà dans le groupe cible, l'index (<numéro de séquence suivant>) est ajouté au nom de la stratégie nouvellement créée ou déplacée, par exemple : (1).

Déplacement d'une stratégie vers un autre groupe d'administration

Kaspersky Security Center Web Console et Cloud Console vous permettent de déplacer une stratégie vers un autre groupe d'administration.

Pour déplacer une stratégie vers un autre groupe d'administration :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**.

2. Dans la liste des stratégies de groupe qui s'ouvre, cochez la case en regard du nom de la stratégie que vous souhaitez déplacer vers un autre groupe d'administration, puis cliquez sur **Déplacer**.

3. Dans l'arborescence des groupes d'administration qui s'ouvre, sélectionnez le groupe cible vers lequel vous souhaitez déplacer la stratégie.

   Vous pouvez créer un nouveau groupe d'administration en sélectionnant un groupe existant, puis en cliquant sur **Ajouter un groupe enfant**.

4. Cliquez sur **Déplacer**.

5. Cliquez sur **OK** pour confirmer l'opération.

Le résultat dépend des propriétés d'héritage de la stratégie :

- Si la stratégie n'est pas héritée dans le groupe source, elle sera déplacée vers le groupe cible.
- Si la stratégie est héritée dans le groupe source, elle ne sera pas déplacée. Au lieu de cela, une copie de cette stratégie sera créée dans le groupe cible.

L'état de chaque stratégie copiée ou déplacée dans le groupe cible sera **Inactif**. Vous pouvez remplacer l'état en **Actif** à tout moment.

Si une stratégie avec un nom identique à celui de la stratégie nouvellement créée ou déplacée existe déjà dans le groupe cible, l'index (<numéro de séquence suivant>) est ajouté au nom de la stratégie nouvellement créée ou déplacée, par exemple : (1).

Suppression d'une stratégie de groupe

Kaspersky Security Center Web Console et Cloud Console vous permettent de supprimer les stratégies de groupe.

Vous ne pouvez supprimer qu'une stratégie qui n'est pas héritée dans le groupe d'administration actuel. Si une stratégie est héritée, vous ne pouvez la supprimer que dans le groupe de niveau supérieur pour lequel elle a été créée.

Pour supprimer une stratégie de groupe, procédez comme suit :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**.
2. Dans la liste des stratégies de groupe qui s'ouvre, cochez la case en regard du nom de la stratégie que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Cliquez sur **OK** pour confirmer l'opération.

La stratégie de groupe sera supprimée.

Définition des paramètres de stratégie

Cette section décrit comment définir les paramètres des stratégies de Kaspersky Security Center pour la gestion des appareils mobiles.

Vous pouvez définir des paramètres de stratégie lors de la création ou de la modification d'une stratégie.

Configuration de la protection antivirus

Pour détecter les menaces à temps, pour réaliser une recherche de virus ou d'autres apps malveillantes, il faut configurer la protection en temps réel et le lancement automatique de la recherche de virus.

Kaspersky Endpoint Security for Android détecte les types d'objets suivants :

- virus, vers, chevaux de Troie, les outils malveillants ;
- applications publicitaires ;
- applications que les individus malintentionnés peuvent utiliser pour nuire à l'appareil ou aux données personnelles de l'utilisateur.

En raison de restrictions techniques, Kaspersky Endpoint Security for Android n'est pas capable d'analyser les fichiers de 2 Go ou plus. Dans le cadre de l'analyse, l'application ignore les fichiers et ne vous signale pas cette action.

Configuration de la protection en temps réel

Pour configurer la protection en temps réel :

1. Ouvrez la fenêtre des propriétés de la stratégie :

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**

2. Dans la fenêtre des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **Protection essentielle**.

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

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

   - Précisez le niveau de protection :

     - Si vous souhaitez que Kaspersky Endpoint Security for Android analyse uniquement les nouveaux fichiers et applications du dossier Téléchargements, sélectionnez **Analyser uniquement les nouvelles applications**.

     - Pour activer la protection étendue de l'appareil mobile contre les menaces, sélectionnez **Analyser toutes les applications et surveiller les actions avec les fichiers**.

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

       Sur les appareils gérés par le système d'exploitation Android 8.0 et version ultérieures, Kaspersky Endpoint Security for Android analyse les fichiers que l'utilisateur modifie, transfère, installe et enregistre, ainsi que les copies des fichiers. Kaspersky Endpoint Security for Android n'analyse pas les fichiers lors de leur ouverture, ni les fichiers d'origine en cours de copie.

   - Pour activer l'analyse complémentaire des nouvelles applications avant leur premier lancement sur l'appareil de l'utilisateur à l'aide du service cloud Kaspersky Security Network, cochez la case **Protection supplémentaire par Kaspersky Security Network**.

   - Pour bloquer les applications publicitaires et les applications susceptibles d'être exploitées par des criminels pour nuire à l'appareil ou aux données de l'utilisateur, cochez la case **Détecter les applications publicitaires, les numéroteurs automatiques et les applications que des cybercriminels peuvent utiliser pour nuire à l'appareil et aux données de l'utilisateur**.

4. Dans la section **Paramètres de l'Antivirus**, sélectionnez l'action à effectuer suite à la détection d'une menace :

   - **Supprimer et enregistrer une copie de sauvegarde du fichier en quarantaine**

     Les objets détectés sont automatiquement supprimés. L'utilisateur n'a besoin d'effectuer aucune action supplémentaire. Avant de supprimer un objet, Kaspersky Endpoint Security for Android crée une copie de sauvegarde du fichier et l'enregistre dans la Quarantaine.

   - **Supprimer**

Les objets détectés sont automatiquement supprimés. L'utilisateur n'a besoin d'effectuer aucune action supplémentaire. Avant la suppression, Kaspersky Endpoint Security for Android affiche une notification temporaire sur la détection de l'objet.

- **Ignorer**

  Si des objets détectés ont été ignorés, Kaspersky Endpoint Security for Android avertit l'utilisateur de la présence de problèmes dans la protection de l'appareil. Les informations sur les objets ignorés s'affichent dans la section **État** de l'app. Pour chaque menace ignorée, l'utilisateur a le choix entre plusieurs actions pour l'éliminer. Le contenu de la liste des objets ignorés peut changer, par exemple si un fichier malveillant est supprimé ou déplacé. Pour obtenir la liste actuelle des menaces, lancez une analyse complète de l'appareil. Afin de vraiment garantir la protection des données, il est conseillé de supprimer tous les objets détectés.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Configuration du lancement automatique de la recherche de virus sur l'appareil mobile

Pour configurer le lancement automatique de la recherche de virus sur l'appareil mobile :

1. Ouvrez la fenêtre des propriétés de la stratégie :

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**

2. Dans la fenêtre des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **Protection essentielle**.

3. Pour bloquer les applications publicitaires et les applications susceptibles d'être exploités par des criminels pour nuire à l'appareil ou aux données de l'utilisateur, cochez la case **Détecter les applications publicitaires, les numéroteurs automatiques et les applications que des cybercriminels peuvent utiliser pour nuire à l'appareil et aux données de l'utilisateur** dans la section **Analyse de l'appareil**.

4. Sélectionnez une des options suivantes dans la liste **Action en cas de détection d'une menace** :

   - **Supprimer et enregistrer une copie de sauvegarde du fichier en quarantaine**

     Les objets détectés sont automatiquement supprimés. L'utilisateur n'a besoin d'effectuer aucune action supplémentaire. Avant de supprimer un objet, Kaspersky Endpoint Security for Android crée une copie de sauvegarde du fichier et l'enregistre dans la Quarantaine.

   - **Supprimer**

Les objets détectés sont automatiquement supprimés. L'utilisateur n'a besoin d'effectuer aucune action supplémentaire. Avant la suppression, Kaspersky Endpoint Security for Android affiche une notification temporaire sur la détection de l'objet.

- **Ignorer**

  Si des objets détectés ont été ignorés, Kaspersky Endpoint Security for Android avertit l'utilisateur de la présence de problèmes dans la protection de l'appareil. Les informations sur les objets ignorés s'affichent dans la section **État** de l'app. Pour chaque menace ignorée, l'utilisateur a le choix entre plusieurs actions pour l'éliminer. Le contenu de la liste des objets ignorés peut changer, par exemple si un fichier malveillant est supprimé ou déplacé. Pour obtenir la liste actuelle des menaces, lancez une analyse complète de l'appareil. Afin de vraiment garantir la protection des données, il est conseillé de supprimer tous les objets détectés.

- **Confirmer**

  L'application Kaspersky Endpoint Security for Android affiche une notification qui propose à l'utilisateur de choisir l'action à exécuter sur l'objet détecté : **Ignorer** ou **Supprimer**.

  L'option **Confirmer** permet à l'utilisateur de l'appareil lors de la détection de quelques objets d'appliquer l'action choisie à chaque fichier à l'aide de la case **Appliquer à toutes les menaces**.

  Pour l'affichage de la notification sur les appareils mobiles tournant sous Android version 10.0 et suivantes, Kaspersky Endpoint Security for Android doit être installé en tant que service des Fonctionnalités d'accessibilité. Kaspersky Endpoint Security for Android propose à l'utilisateur d'installer l'app comme service des Fonctionnalités d'accessibilité pendant l'exécution de l'Assistant de configuration initiale. L'utilisateur peut ignorer cette étape ou désactiver ultérieurement le service dans les paramètres de l'appareil. Dans ce cas, Kaspersky Endpoint Security for Android affiche une fenêtre système Android qui propose à l'utilisateur de choisir l'action sur l'objet détecté : Ignorer ou Supprimer. Pour appliquer l'action à plusieurs objets, ouvrez Kaspersky Endpoint Security.

5. La section **Analyse programmée** permet de configurer le lancement automatique de l'analyse complète du système de fichiers de l'appareil.

   Sélectionnez une des options suivantes :

   - **Désactivée**

     L'analyse du système de fichiers de l'appareil n'est pas lancée automatiquement.

   - **Après la mise à jour des bases de données**

     L'analyse automatique du système de fichiers de l'appareil a lieu après chaque mise à jour des bases antivirus.

   - **Une fois par jour**

     L'analyse automatique du système de fichiers de l'appareil a lieu chaque jour.

     Si vous sélectionnez cette option, vous pouvez également renseigner l'heure de l'analyse dans le champ **Heure du lancement**.

   - **Une fois par semaine le**

     L'analyse automatique du système de fichiers de l'appareil a lieu une fois par semaine.

     Si vous sélectionnez cette option, vous pouvez également sélectionner le jour de la semaine où vous souhaitez exécuter l'analyse dans la liste déroulante et renseigner l'heure de l'analyse dans le champ **Heure du lancement**.

Sur Android 12 ou une version ultérieure, l'application peut effectuer cette tâche plus tard que prévu si l'appareil est en mode d'économie de la batterie.

6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Configuration des mises à jour des bases antivirus

Pour configurer les mises à jour des bases antivirus :

1. Ouvrez la fenêtre des propriétés de la stratégie :

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**

2. Dans la fenêtre des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **Mise à jour des bases de données**.

3. Dans le groupe **Mise à jour des bases de données**, planifiez la mise à jour automatique des bases antivirus sur l'appareil de l'utilisateur.

   Sélectionnez une des options suivantes :

   - **Désactivée**

     Les mises à jour automatiques des bases antivirus sont désactivées.

   - **Une fois par jour**

     La mise à jour des bases antivirus a lieu chaque jour.

     Si vous sélectionnez cette option, vous pouvez également renseigner l'heure de la mise à jour dans le champ **Heure de la mise à jour**.

   - **Une fois par semaine**

     La mise à jour des bases antivirus a lieu une fois par semaine.

     Si vous sélectionnez cette option, vous pouvez également renseigner l'heure de mise à jour dans le champ **Heure de la mise à jour** et le jour de la semaine auquel vous souhaitez exécuter la mise à jour dans la liste déroulante **Jour de la semaine**

Sur Android 12 ou une version ultérieure, l'application peut effectuer cette tâche plus tard que prévu si l'appareil est en mode d'économie de la batterie.

4. Indiquez dans le groupe **Source des mises à jour des bases de données** la source des mises à jour à partir de laquelle Kaspersky Endpoint Security for Android va copier et installer les mises à jour des bases antivirus de l'app :

   - **Serveurs de Kaspersky**

     Kaspersky Endpoint Security for Android utilisera un serveur de mise à jour de Kaspersky comme source des mises à jour pour télécharger les bases antivirus sur l'appareil de l'utilisateur.

   - **Serveur d'administration**

     Disponible uniquement si vous utilisez Kaspersky Security Center Web Console.

     Kaspersky Endpoint Security for Android utilisera un référentiel du Serveur d'administration de Kaspersky Security Center comme source des mises à jour pour télécharger les bases antivirus sur l'appareil de l'utilisateur.

   - **Autre source**

     Kaspersky Endpoint Security for Android utilisera un serveur tiers comme source des mises à jour pour télécharger les bases antivirus sur l'appareil de l'utilisateur.

     Si vous sélectionnez cette option, vous devez spécifier l'adresse d'un serveur HTTP dans le champ **Utiliser un autre serveur comme source de mise à jour des bases antivirus**.

5. Pour que Kaspersky Endpoint Security for Android télécharge la mise à jour des bases antivirus selon une programmation quand l'appareil est en itinérance, cochez la case **Autoriser la mise à jour des bases de données en itinérance** dans le groupe **Mettre à jour les bases antivirus en itinérance**.

6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Définition des paramètres de déverrouillage de l'appareil

Pour assurer la sécurité de l'appareil mobile, il est nécessaire de configurer l'utilisation d'un mot de passe à saisir quand l'appareil sort du mode veille.

Vous pouvez définir des restrictions sur l'utilisation de l'appareil par un utilisateur si le mot de passe de déverrouillage n'est pas assez complexe (par exemple, verrouiller l'appareil). Vous pouvez définir de telles limites à l'aide du composant Contrôle de conformité.

Sur certains appareils Samsung tournant sous le système d'exploitation Android 7.0 et version ultérieure, si l'utilisateur tente de configurer des modes de déverrouillage de l'appareil non pris en charge (par exemple, mot de passe graphique), l'appareil peut être verrouillé si les conditions suivantes sont réunies : la protection contre la suppression de Kaspersky Endpoint Security for Android est activée et les exigences de la sécurité du mot de passe de déverrouillage de l'écran sont définies. Pour déverrouiller l'appareil, il faut lui envoyer une commande spéciale.

Pour configurer la robustesse du mot de passe de déverrouillage de l'appareil :

1. Ouvrez la fenêtre des propriétés de la stratégie :

- Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.

- Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**

2. Dans la fenêtre des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **Protection essentielle**.

3. Si vous souhaitez que l'application recherche l'existence d'un mot de passe de déverrouillage, sélectionnez l'option **Imposer la définition d'un mot de passe de déverrouillage de l'écran** dans le groupe **Protection par mot de passe**.

   Si l'application détecte qu'aucun mot de passe n'a été défini sur l'appareil, l'utilisateur devra en choisir un. Le mot de passe est défini en tenant compte des paramètres définis par l'administrateur.

4. Définissez le nombre minimum de caractères du mot de passe.

   Valeurs possibles : de 4 à 16.

   Par défaut, le mot de passe de l'utilisateur contient 4 symboles.

   > Sur les appareils tournant sous Android 10.0 ou une version ultérieure, Kaspersky Endpoint Security résout les exigences de force du mot de passe en une des valeurs du système : moyenne ou élevée.

   Les valeurs pour les appareils tournant sous Android 10.0 ou une version ultérieure sont déterminées par les règles suivantes :

   - Si la longueur du mot de passe requise est de 1 à 4 symboles, l'application invite l'utilisateur à définir un mot de passe de force moyenne. Il doit être soit numérique (PIN) sans séquence répétée ou ordonnée (par exemple 1234), soit alphanumérique. Le code PIN ou le mot de passe doit comporter au moins 4 caractères.

   - Si la longueur du mot de passe requise est d'au moins 5 symboles, l'application invite l'utilisateur à définir un mot de passe de force élevée. Il doit être soit numérique (PIN) sans séquence répétée ou ordonnée, soit alphanumérique (mot de passe). Le code PIN doit comporter au moins 8 chiffres ; le mot de passe doit comporter au moins 6 caractères.

5. Si vous voulez que l'utilisateur ait la possibilité d'utiliser les empreintes digitales pour déverrouiller l'écran, cochez la case **Autoriser l'utilisation des empreintes digitales (pour les appareils tournant sous Android 9 ou versions antérieures)**. Si le mot de passe de déverrouillage ne correspond pas aux exigences de sécurité de l'entreprise, il est impossible d'utiliser le scanner d'empreintes digitales pour déverrouiller l'écran.

   > Sur les appareils tournant sous Android 10.0 ou une version ultérieure, l'utilisation de l'empreinte digitale pour déverrouiller l'écran n'est pas prise en charge.

   > Kaspersky Endpoint Security for Android ne limite pas l'utilisation du scanner d'empreintes digitales pour l'accès aux applications ou la confirmations des achats.

   > Sur certains appareils Samsung, il est impossible d'interdire l'utilisation des empreintes digitales pour le déverrouillage de l'écran.

Aussi, sur certains appareils Samsung, si le mot de passe de déverrouillage n'est pas conforme aux exigences de sécurité de l'entreprise, Kaspersky Endpoint Security for Android n'interdit pas l'utilisation des empreintes digitales pour le déverrouillage de l'écran.

Après l'ajout de l'empreinte digitale dans les paramètres de l'appareil, l'utilisateur peut déverrouiller l'écran via les moyens suivants :

- mettre le doigt sur le scanner d'empreintes, soit le moyen habituel ;
- saisir le mot de passe de déverrouillage, le moyen de secours.

6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

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

Pour protéger les données d'entreprise en cas de perte ou de vol d'un appareil mobile, vous devez configurer la protection contre l'accès non autorisé.

Pour garantir la protection des données sur un appareil perdu ou volé, Kaspersky Endpoint Security for Android doit être installé en tant que service des Fonctionnalités d'accessibilité. Kaspersky Endpoint Security for Android propose à l'utilisateur d'installer l'app comme service des Fonctionnalités d'accessibilité pendant l'exécution de l'Assistant de configuration initiale. L'utilisateur peut ignorer cette étape ou désactiver ultérieurement le service dans les paramètres de l'appareil.

Pour configurer la Protection des données en cas de perte ou de vol de l'appareil :

1. Ouvrez la fenêtre des propriétés de la stratégie :
   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.
   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**
2. Dans la fenêtre des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **Protection essentielle**.
3. Dans la section **Antivol** , configurez le verrouillage de l'appareil :
   - Précisez le nombre de caractères dans le code de déverrouillage.
   - Précisez le texte à afficher lors du verrouillage de l'appareil.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Configuration du contrôle des applications

Le *Contrôle des applications* vérifie si les apps installées sur l'appareil mobile répondent aux exigences de sécurité de l'entreprise. L'administrateur dresse dans Kaspersky Security Center les listes des applications autorisées, interdites, nécessaires et recommandées conformément aux exigences de sécurité de l'entreprise. Pendant son utilisation, le Contrôle des applications de Kaspersky Endpoint Security propose à l'utilisateur d'installer les applications nécessaires et recommandées et de supprimer les applications interdites. Le lancement d'une applications interdite sur l'appareil mobile de l'utilisateur est alors impossible.

Kaspersky Security Center Web Console et Cloud Console permettent de gérer les applications sur les appareils des utilisateurs en appliquant des règles prédéfinies. Vous pouvez configurer deux types de règles de **Contrôle des applications** : les règles d'application et les règles de catégorie.

Une **Règle d'application** s'applique à une application spécifique, tandis qu'une **Règle de la catégorie** s'applique à toute application appartenant à une catégorie prédéfinie. Les catégories d'applications sont spécifiées par les experts de Kaspersky.

*Pour configurer le **Contrôle des applications** :*

1. Ouvrez la fenêtre des propriétés de la stratégie :

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**

2. Dans la page des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **Contrôles de sécurité**.

3. Dans le tableau sous la section **Contrôle des applications**, ajoutez les règles qui définiront les applications qui seront contrôlées.

   - Pour ajouter une règle pour une application spécifique :

     a. Dans le tableau, cliquez sur **Règle d'application**.

     b. Dans la fenêtre **Règle d'application** qui s'ouvre, choisissez l'action qui sera exécutée pour les applications couvertes par la règle créée.

     c. Spécifiez l'application qui sera soumise à la règle en remplissant **Lien vers le paquet d'installation (par exemple, https://play.google.com/store/apps/details?id=com.kaspersky.kes)** , **Nom du paquet (par exemple, katana.facebook.com)** et **Nom de l'application** .

     d. Cliquez sur **Enregistrer**.

La règle s'ajoute à la liste des règles du **Contrôle des applications**

- Pour ajouter une règle pour une catégorie d'applications :

  a. Dans le tableau sous la section **Contrôle des applications**, cliquez sur **Règle de la catégorie**.

  b. Dans la fenêtre **Règle de la catégorie** qui s'ouvre, sélectionnez une catégorie d'application dans la liste déroulante.

  La règle créée s'applique alors aux applications de la catégorie sélectionnée.

  c. Dans la section **Mode de fonctionnement**, sélectionnez l'action qui sera effectuée lors de la tentative de lancement d'une application de la catégorie sélectionnée : **Applications interdites** ou **Applications autorisées** .

  d. Le cas échéant, remplissez le champ **Commentaire supplémentaire affiché sur l'appareil de l'utilisateur lorsqu'une application d'une catégorie donnée est détectée**.

  e. Cliquez sur **Enregistrer**.

  La règle s'ajoute à la liste des règles du **Contrôle des applications**

4. Dans la section **Actions sur les applications interdites**, choisissez l'action à effectuer sur les applications interdites :

   - Si vous souhaitez que Kaspersky Endpoint Security for Android bloque le lancement des applications interdites sur l'appareil mobile de l'utilisateur, sélectionnez **Bloquer le lancement d'applications**.

   - Pour que Kaspersky Endpoint Security for Android envoie les données relatives aux applications interdites dans le journal des événements sans les bloquer, cochez la case **Ne pas bloquer les applications interdites, rapport uniquement**.

5. Dans la section **Mode de fonctionnement**, déterminez si les règles que vous ajoutez vont définir des applications autorisées ou des applications interdites :

   - Si vous souhaitez que les règles définissent les applications autorisées, sélectionnez **Applications interdites** .

     Pour que Kaspersky Endpoint Security for Android bloque l'exécution des apps système (par exemple, calendrier, appareil photo, paramètres) sur l'appareil mobile de l'utilisateur en mode **Applications interdites**, cochez la case **Bloquer les apps système**.

     > Les experts de Kaspersky ne recommandent pas de bloquer les apps système, puisque cela peut entraîner des défaillances dans le fonctionnement de l'appareil.

   - Si vous souhaitez que les règles définissent les applications interdites, sélectionnez **Applications autorisées** .

6. Pour recevoir des informations sur toutes les applications installées sur les appareils mobiles, dans la section **Rapport d'application**, cochez la case **Envoyer une liste des applications installées sur tous les appareils mobiles**.

   Kaspersky Endpoint Security for Android envoie les données dans le journal des événements après chaque installation ou suppression d'une app sur l'appareil.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Configuration du contrôle de conformité des appareils mobile aux exigences de sécurité de l'entreprise

Le contrôle de conformité vous permet de surveiller la conformité des appareils Android aux exigences de sécurité de l'entreprise et de prendre des mesures en cas de non-conformité. Les exigences de sécurité de l'entreprise régissent l'utilisation de l'appareil par l'utilisateur. Par exemple, la protection en temps réel doit être activée sur l'appareil, les bases antivirus doivent être à jour et le mot de passe de l'appareil doit être suffisamment complexe. La vérification de la conformité s'opère sur la base d'une liste de règles. Une règle de conformité contient les éléments suivants :

- Le critère de non-conformité de l'appareil.
- L'action qui sera exécutée sur l'appareil si l'utilisateur ne l'a pas rendu conforme à l'issue du délai octroyé.
- délai octroyé à l'utilisateur de l'appareil pour rendre son appareil conforme (par exemple, 24 heures) ;

  Une fois le délai octroyé écoulé, l'action sélectionnée est exécutée sur l'appareil de l'utilisateur.

  > Sur Android 12 ou une version ultérieure, l'application peut effectuer cette tâche plus tard que prévu si l'appareil est en mode d'économie de la batterie.

Pour configurer le contrôle de conformité, vous pouvez effectuer les actions suivantes :

- Activer ou désactiver les règles de conformité existantes.
- Modifier une règle de conformité existante.
- Ajouter une nouvelle règle.
- Supprimer une règle.

Activation et désactivation des règles de conformité

Pour activer ou désactiver les règles existantes de contrôle de conformité des appareils mobiles aux exigences de sécurité de l'entreprise :

1. Ouvrez la fenêtre des propriétés de la stratégie :
   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.
   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**

2. Dans la page des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **Contrôles de sécurité**.

3. Dans la section **Contrôle de conformité**, activez ou désactivez les règles de conformité existantes à l'aide des boutons bascule de la colonne **État**

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Modification des règles de conformité

Pour modifier une règle de contrôle de conformité des appareils mobiles aux exigences de sécurité de l'entreprise :

1. Ouvrez la fenêtre des propriétés de la stratégie :

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**

2. Dans la page des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **Contrôles de sécurité**.

3. Dans la section **Contrôle de conformité**, sélectionnez la règle que vous souhaitez modifier, puis cliquez sur **Modifier** .

4. Dans la fenêtre **Règle** qui s'ouvre, modifiez la règle comme suit :

   a. Dans la colonne **Action**, configurez la liste des actions à effectuer en cas de non-respect de la règle en ajoutant de nouvelles actions, en modifiant les actions existantes ou en les supprimant.

   b. Vous pouvez éventuellement spécifier le délai pendant lequel un utilisateur peut corriger la non-conformité en utilisant la colonne **Délai de correction** pour chaque action.

   c. Cliquez sur le bouton **Enregistrer** pour enregistrer la règle.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Ajout de règles de conformité

Pour ajouter une règle de contrôle de conformité des appareils mobiles aux exigences de sécurité de l'entreprise :

1. Ouvrez la fenêtre des propriétés de la stratégie :

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**

2. Dans la page des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **Contrôles de sécurité**.

3. Dans la section **Contrôle de conformité**, cliquez sur **Règle**.

4. Dans la fenêtre **Règle** qui s'ouvre, définissez la règle comme suit :

   a. Sélectionnez le critère de non-conformité pour la règle.

   b. Cliquez sur **Ajouter**, puis sélectionnez l' action à effectuer en cas de non-respect de la règle dans la colonne **Action**.

   Vous pouvez ajouter plusieurs actions.

   c. Spécifiez le délai pendant lequel un utilisateur peut corriger la non-conformité en utilisant la colonne **Délai de correction** pour chaque action.

   d. Cliquez sur le bouton **Enregistrer** pour enregistrer la règle.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Suppression des règles de conformité

Pour supprimer une règle de contrôle de conformité des appareils mobiles aux exigences de sécurité de l'entreprise :

1. Ouvrez la fenêtre des propriétés de la stratégie :

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**

2. Dans la page des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **Contrôles de sécurité**.

3. Dans la section **Contrôle de conformité**, sélectionnez la règle que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Liste des critères de non-conformité

Pour s'assurer qu'un appareil Android répond aux exigences de sécurité de l'entreprise, Kaspersky Endpoint Security for Android peut vérifier l'appareil selon les critères suivants :

- **Protection en temps réel désactivée**.

  La protection en temps réel doit être activée.

  Pour en savoir plus sur la configuration de la protection en temps réel, consultez la section "Configuration de la protection en temps réel".

- **Bases antivirus obsolètes**.

  Les bases antivirus de Kaspersky Endpoint Security for Android doivent être régulièrement mises à jour.

  Pour en savoir plus sur la configuration des paramètres des mises à jour des bases antivirus, consultez la section "Configuration de la protection contre les virus".

- **Des applications interdites sont installées**.

  Aucune application classée comme **Bloquer le lancement**, tel que spécifié dans la section **Contrôle des applications** ne peut être installée sur l'appareil.

  Pour en savoir plus sur la création de règles pour les applications, consultez la section "Configuration du contrôle des applications".

- **Des applications de catégories bloquées ont été installées**.

  Aucune application appartenant à une catégorie classée comme **Bloquer le lancement**, tel que spécifié dans la section **Contrôle des applications** ne peut être installée sur l'appareil.

  Pour en savoir plus sur la création de règles pour les catégories d'applications, consultez la section "**Configuration du contrôle des applications**".

- **Toutes les applications nécessaires ne sont pas installées**.

  Certaines applications classées comme **Forcer l'installation**, tel que spécifié dans la section **Contrôle des applications** doivent être installées sur l'appareil.

  Pour en savoir plus sur la création de règles pour les applications, consultez la section "Configuration du contrôle des applications".

- **La version du système d'exploitation est obsolète**.

  L'appareil doit avoir une version autorisée du système d'exploitation.

  Pour utiliser ce critère de non-conformité, vous devez spécifier la plage de versions de système d'exploitation autorisées dans les listes déroulantes **Version minimale du système d'exploitation** et **Version maximale du système d'exploitation**.

- **L'appareil n'a pas été synchronisé depuis longtemps**.

  Il faut synchroniser régulièrement L'appareil avec le Serveur d'administration.

  Pour utiliser ce critère de non-conformité, vous devez spécifier l'intervalle de temps maximum entre les synchronisations des appareils dans la liste déroulante **Période de synchronisation**.

- **Autorisations root reçues sur l'appareil**.

  L'appareil ne peut avoir l'autorisation root.

  Pour en savoir plus, consultez la section "Détection d'une attaque contre l'appareil (root)".

- **Le mot de passe de déverrouillage n'est pas conforme aux exigences de sécurité**.

  L'appareil doit être protégé par un mot de passe de déverrouillage conforme aux exigences de robustesse du mot de passe de déverrouillage.

Liste des actions en cas de non-conformité

Les actions suivantes sont proposées si l'utilisateur ne règle pas un problème de conformité dans le délai imparti :

- **Bloquer le lancement de toutes les applications sauf les applications système**.

  Le lancement de toutes les applications, à part les apps système, sur l'appareil mobile de l'utilisateur est bloqué.

- **Verrouiller l'appareil**.

  L'appareil mobile est verrouillé. Pour accéder aux données, il faut déverrouiller l'appareil. Si la cause du verrouillage n'est pas éliminée après le déverrouillage, l'appareil se verrouille à nouveau après la période indiquée.

- **Supprimer les données d'entreprise**.

  Les données du conteneur, le compte utilisateur d'email d'entreprise, les paramètres de connexion au réseau Wi-Fi de l'entreprise, les réseaux VPN, le point d'accès (APN) sont supprimés.

- **Rétablir les paramètres d'usine de l'appareil**.

  Toutes les données sont supprimées sur l'appareil mobile et les paramètres de configuration sont réinitialisés à leurs valeurs par défaut.

Configuration de l'accès des utilisateurs aux sites Internet

Pour protéger les données personnelles et d'entreprise stockées sur les appareils mobiles pendant la navigation sur Internet, vous pouvez configurer l'accès des utilisateurs de Kaspersky Endpoint Security for Android aux sites Internet à l'aide de la Protection Internet. La Protection Internet analyse les sites Internet avant qu'un utilisateur ne les ouvre, puis bloque les sites qui diffusent du code malveillant et les sites Internet de phishing conçus pour voler des données confidentielles et accéder aux comptes bancaires. Cette fonction prend en charge le filtrage des sites Internet par catégorie, selon les catégories définies dans le service cloud de Kaspersky Security Network. Le filtrage permet de limiter l'accès des utilisateurs à certains sites Internet ou catégories de sites Internet (par exemple, aux sites Internet de la catégorie "**Jeux de hasard, loterie, tirages au sort**" ou "**Communication via Internet**").

La Protection Internet fonctionne seulement dans les navigateurs Google Chrome, Huawei Browser et Samsung Internet Browser.

Pour garantir la Protection Internet sur un appareil perdu ou volé, Kaspersky Endpoint Security for Android doit être installé en tant que service des Fonctionnalités d'accessibilité. Kaspersky Endpoint Security for Android propose à l'utilisateur d'installer l'app comme service des Fonctionnalités d'accessibilité pendant l'exécution de l'Assistant de configuration initiale. L'utilisateur peut ignorer cette étape ou désactiver ultérieurement le service dans les paramètres de l'appareil.

Pour configurer l'accès des utilisateurs aux sites Internet :

1. Ouvrez la fenêtre des propriétés de la stratégie :
   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.
   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**
2. Dans la page des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **Contrôles de sécurité**.
3. Dans la **Protection Internet** , cochez la **Activer la Protection Internet** pour activer la fonctionnalité.
4. Sélectionnez une des options suivantes :
   - Pour restreindre l'accès des utilisateurs aux sites Internet en fonction de leur contenu :
     a. Sélectionnez **Bloquer les sites Internet des catégories spécifiées**.
     b. Cochez les cases à côté des catégories de sites Internet auxquels Kaspersky Endpoint Security for Android bloquera l'accès.

     Si la Protection Internet est activée, l'utilisateur ne pourra jamais accéder aux sites Internet des catégories **Phishing** et **Sites malveillants**.
   - Pour définir la liste des sites Internet autorisés :
     a. Sélectionnez **Autoriser uniquement les sites Internet spécifiés**.
     b. Créez une liste de sites Internet en ajoutant les adresses des sites Internet auxquels l'application ne bloquera pas l'accès. Kaspersky Endpoint Security for Android prend en charge uniquement les expressions rationnelles. Lors de la saisie de l'adresse du site Internet autorisé, utilisez les modèles suivants :
        - `http:\/\/www\.example\.com.*` : autorisation pour toutes les pages enfants de la page Internet (par exemple, `http://www.example.com/about`).
        - `https:\/\/.*example\.com` : autorisation pour tous les sous-domaines de la page Internet (par exemple, `https://pictures.example.com`).

     c. Vous pouvez utiliser aussi l'expression `https?` pour choisir HTTP et HTTPS. Pour en savoir plus sur les expressions rationnelles, consultez le site du Support Technique Oracle.

- Pour bloquer l'accès des utilisateurs à tous les sites Internet, sélectionnez **Bloquer tous les sites Internet** .

5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Configuration des restrictions de fonctionnalité

Kaspersky Security Center Web Console permet de configurer l'accès des utilisateurs aux fonctionnalités suivantes des appareils mobiles :

- Wi-Fi
- Appareil photo
- Bluetooth

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 des propriétés de la stratégie :
   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.
   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**
2. Dans la page des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **Contrôles de sécurité**.
3. Dans le groupe **Gestion des fonctionnalités**, configurez l'utilisation du module Wi-Fi, de l'appareil photo et du Bluetooth :
   - Pour désactiver le module Wi-Fi sur l'appareil mobile de l'utilisateur, cochez la case **Interdire l'utilisation du Wi-Fi**.

     Sur les appareils tournant sous Android 10.0 ou version ultérieure, l'interdiction d'utiliser les réseaux Wi-Fi n'est pas prise en charge.

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

Sur les appareils tournant sous Android 10.0 ou version ultérieure, l'utilisation de la caméra ne peut pas être totalement interdite.

Sur les appareils tournant sous Android 11 et suivantes, Kaspersky Endpoint Security for Android doit être installé en tant que service des fonctionnalités d'accessibilité. Kaspersky Endpoint Security for Android propose à l'utilisateur d'installer l'app comme service des Fonctionnalités d'accessibilité pendant l'exécution de l'Assistant de configuration initiale. L'utilisateur peut ignorer cette étape ou désactiver ultérieurement le service dans les paramètres de l'appareil. Si tel est le cas, vous ne pourrez pas restreindre l'utilisation de l'appareil photo.

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

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Protection de Kaspersky Endpoint Security for Android contre la suppression

Pour la protéger l'appareil mobile et respecter les exigences de sécurité de l'entreprise, vous pouvez activer la protection de Kaspersky Endpoint Security for Android contre la suppression. Dans ce cas, l'utilisateur ne peut pas supprimer l'application via l'interface de Kaspersky Endpoint Security for Android. En cas de suppression de l'application via les outils du système d'exploitation Android, une demande de désactivation des autorisations d'administrateur pour Kaspersky Endpoint Security for Android s'affiche. Après que les autorisations ont été désactivées, l'appareil mobile est verrouillé.

Pour activer la protection de Kaspersky Endpoint Security for Android contre la suppression, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie :

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**

2. Dans la page des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **Contrôles de sécurité**.

3. Dans la section **Administrer l'application sur un appareil mobile**, décochez la case **Autoriser la suppression de l'application Kaspersky Endpoint Security for Android sur l'appareil**

Sur les appareils tournant sous le système d'exploitation Android version 7.0 et suivantes, Kaspersky Endpoint Security for Android doit être installé en tant que service des Fonctionnalités d'accessibilités pour protéger l'app contre la suppression. Pendant le fonctionnement de l'Assistant de configuration initiale, Kaspersky Endpoint Security for Android propose à l'utilisateur d'accorder les autorisations requises à l'app. L'utilisateur peut ignorer ces étapes ou désactiver les droits ultérieurement dans les paramètres de l'appareil. Dans ce cas, la protection de l'app contre la suppression ne fonctionne pas.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

En cas de tentative de suppression de l'app, l'appareil mobile est verrouillé.

Configuration de la synchronisation des appareils mobiles avec Kaspersky Security Center

Pour l'administration des appareils mobiles et la réception des rapports ou des statistiques des appareils mobiles, vous devez définir les paramètres de synchronisation. La synchronisation des appareils mobiles avec Kaspersky Security Center peut être exécutée des manières suivantes :

- **Planification**. La synchronisation est exécutée d'après l'horaire planifié via HTTP. Vous pouvez configurer l'horaire de la synchronisation dans les propriétés de la stratégie. Les modifications des paramètres de la stratégie, les commandes et les tâches seront exécutées pendant la synchronisation de l'appareil avec Kaspersky Security Center d'après l'horaire, à savoir avec du retard. Par défaut, les appareils mobiles se synchronisent automatiquement avec Kaspersky Security Center toutes les six heures.

  Sur Android 12 ou une version ultérieure, l'application peut effectuer cette tâche plus tard que prévu si l'appareil est en mode d'économie de la batterie.

- **Forcée**. La synchronisation forcée est exécutée à l'aide des notifications push du service FCM (Firebase Cloud Messaging). La synchronisation forcée, en premier lieu, est destinée à l'envoi opportun des commandes à l'appareil mobile. Si vous voulez utiliser la synchronisation forcée, assurez-vous que les paramètres FCM dans Kaspersky Security Center sont configurés.

Pour configurer la synchronisation des appareils mobiles avec Kaspersky Security Center, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie :

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**

2. Dans la page des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **Synchronisation**.

3. Dans la section **Synchronisation à l'aide du Serveur d'administration**, utilisez la liste déroulante **Période de synchronisation** pour sélectionner la période de synchronisation.

   Par défaut, la synchronisation a lieu toutes les six heures.

4. Vous pouvez désactiver la synchronisation lorsque l'appareil est en itinérance. Pour ce faire, cochez la case **Désactiver la synchronisation en itinérance**.

   Par défaut, la synchronisation en itinérance est activée.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Kaspersky Security Network

Pour renforcer l'efficacité de la protection des périphériques mobiles, Kaspersky Endpoint Security for Android utilise des données acquises 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 sur la réputation des fichiers, des ressources Internet et du logiciel. L'utilisation des données de Kaspersky Security Network permet aux applications de Kaspersky 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 d'acquérir 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. 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 sont obtenues lors du fonctionnement de Kaspersky Endpoint Security for Android sur l'ordinateur de l'utilisateur et elles sont envoyées automatiquement à Kaspersky. 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 pour un examen complémentaire.

Pour le fonctionnement de Kaspersky Endpoint Security for Android, l'utilisation de Kaspersky Security Network est obligatoire. KSN est utilisé pour le fonctionnement des composants fondamentaux de l'application : Antivirus, Protection Internet et Contrôle des applications. Le refus de la participation à KSN réduit le niveau de protection du périphérique, ce qui peut amener à l'infection du périphérique et à la perte des informations. Afin de pouvoir utiliser Kaspersky Security Network, vous devez accepter les conditions du Contrat de licence utilisateur final lors de l'utilisation de l'application. Le Contrat de licence utilisateur final présente les types de données que Kaspersky Endpoint Security for Android transmet à Kaspersky Security Network.

Pour améliorer le fonctionnement de l'application, vous pouvez aussi expédier à Kaspersky Security Network les données statistiques. La participation à Kaspersky Security Network pour le traitement des données statistiques est volontaire.

Échange d'informations avec Kaspersky Security Network

Pour améliorer la protection en temps réel, Kaspersky Security for Mobile utilise le service cloud de Kaspersky Security Network pour les composants suivants :

- **Antivirus.** L'application a accès à la base opérationnelle de connaissances de Kaspersky sur la réputation des fichiers et des applications. L'analyse est effectuée sur les menaces dont les informations ne figurent pas encore dans les bases antivirus mais se trouvent déjà dans KSN. Le service cloud de Kaspersky Security Network assure le bon fonctionnement de l'Antivirus et réduit la probabilité de faux positifs.

- **Protection Internet.** L'application utilise les données reçues de la part de KSN pour analyser les sites Internet avant leur ouverture. L'application définit aussi la catégorie du site Internet pour contrôler l'accès des utilisateurs au réseau Internet sur la base des listes de catégories autorisées et interdites (par exemple, la catégorie "Communication via Internet").

- **Contrôle des applications.** L'application définit la catégorie de l'application pour la restriction du lancement de l'application qui ne satisfait pas aux exigences de sécurité de l'entreprise, à partir des listes de catégories autorisées et interdites (par exemple, catégorie "Jeux").

Le Contrat de licence utilisateur final détaille la nature des données transmises à Kaspersky lorsque le KSN est utilisé parallèlement Anti-Virus et Contrôle des applications. En acceptant les termes du Contrat de licence, vous consentez à transmettre les informations suivantes.

Les informations sur le type de données soumises à Kaspersky lors de l'utilisation de KSN pendant le fonctionnement de la Protection Internet sont disponibles dans la Déclaration concernant le traitement des données pour la Protection Internet. En acceptant les termes de la Déclaration, vous consentez à transmettre les informations suivantes.

Afin de détecter les menaces nouvelles et difficiles à détecter pour la sécurité de l'information et leurs sources, les menaces d'intrusion, ainsi que pour augmenter le niveau de protection des informations conservées et traitées sur l'appareil, vous pouvez étendre la participation au KSN.

Afin de pouvoir échanger les données avec le KSN pour améliorer la qualité d'exécution de l'application, les conditions suivantes doivent être remplies :

- L'utilisateur de l'appareil doit accepter les conditions de la Déclaration de Kaspersky Security Network.

- Vous devez autoriser la transmission des données statistiques à KSN dans les paramètres de la stratégie de groupe (voir ci-dessous).

Vous pouvez à tout moment refuser l'envoi des données statistiques à KSN. La Déclaration de Kaspersky Security Network détaille la nature des données statistiques transmises à Kaspersky lorsque le KSN est utilisé parallèlement à l'application mobile Kaspersky Endpoint Security for Android sur les appareils des utilisateurs.

Pour en savoir plus à propos de la collecte des données dans KSN, reportez-vous à la section "Collecte des données".

La fourniture de données à KSN est volontaire. Si vous le souhaitez, vous pouvez désactiver l'échange de données avec KSN.

Activation et désactivation de Kaspersky Security Network

Pour le fonctionnement des composants de Kaspersky Endpoint Security for Android utilisant Kaspersky Security Network, l'application envoie les demandes aux services cloud. Les demandes contiennent les données telles que décrites dans la section "Collecte des données".

L'utilisation de Kaspersky Security Network est activée par défaut.

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 et leurs paramètres ne sont plus accessibles.

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

1. Ouvrez la fenêtre des propriétés de la stratégie :

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**

2. Dans la page des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **KSN et statistiques**.

3. Pour activer ou désactiver l'utilisation de Kaspersky Security Network, cochez ou décochez la case **Utiliser Kaspersky Security Network**.

4. Si l'utilisation de Kaspersky Security Network est activée et si vous acceptez de soumettre des données à Kaspersky, cochez la case **Autoriser le transfert des données statistiques dans Kaspersky Security Network** Les données permettront d'augmenter la vitesse de la réaction de l'application Kaspersky Endpoint Security for Android face aux menaces, d'améliorer les performances des composants de protection et de réduire la probabilité des faux positifs.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Échange d'informations avec les services Google Analytics pour Firebase, SafetyNet Attestation, Firebase Performance Monitoring et Crashlytics

Kaspersky Endpoint Security for Android échange des données avec les services Google Analytics pour Firebase, SafetyNet Attestation, Firebase Performance Monitoring et Crashlytics afin d'améliorer la qualité, l'apparence et les performances des logiciels, produits, services et infrastructures de Kaspersky via l'analyse de l'expérience des utilisateurs et de l'utilisation des fonctionnalités, de l'état et des paramètres de l'appareil.

L'échange d'informations avec les services Google Analytics pour Firebase, SafetyNet Attestation, Firebase Performance Monitoring, et Crashlytics est désactivé par défaut.

Pour activer l'échange de données :

1. Ouvrez la fenêtre des propriétés de la stratégie :

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**

2. Dans la page des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **KSN et statistiques**.

3. Dans le groupe **Envoi de statistiques**, décochez la case **Autoriser le transfert de données afin d'améliorer la qualité, l'apparence et les performances de l'application**.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Configuration des notifications sur les appareils mobiles

Si vous souhaitez que l'utilisateur de l'appareil mobile ne soit pas distrait par les notifications de Kaspersky Endpoint Security for Android, vous pouvez désactiver certaines notifications.

Kaspersky Endpoint Security utilise les outils suivants pour afficher l'état de protection des appareils :

- **Notification de l'état de protection**. Cette notification est épinglée à la barre de notifications. Il est impossible de supprimer une notification de l'état de protection. La notification affiche l'état de protection des appareils (par exemple,) et le nombre de problèmes, le cas échéant. L'utilisateur de l'appareil peut appuyer sur l'état de protection des appareils et afficher les problèmes de la liste dans l'application.

- **Notifications sur l'application**. Ces notifications informent l'utilisateur de l'appareil sur l'application (par exemple, la détection des menaces).

- **Messages contextuels**. Les messages contextuels nécessitent une action de l'utilisateur de l'appareil (par exemple, une action à effectuer en cas de menace détectée).

Toutes les notifications de Kaspersky Endpoint Security for Android sont activées par défaut.

L'utilisateur de l'appareil Android peut désactiver toutes les notifications de Kaspersky Endpoint Security for Android dans les paramètres du volet de notifications. Si les notifications sont désactivées, l'utilisateur ne contrôle pas le fonctionnement de l'application et peut ignorer des informations importantes (par exemple, sur les défaillances lors la synchronisation de l'appareil avec Kaspersky Security Center). Pour connaître l'état de fonctionnement de l'application, l'utilisateur doit ouvrir Kaspersky Endpoint Security for Android.

Pour configurer l'affichage des notifications relatives au fonctionnement de Kaspersky Endpoint Security for Android sur un appareil mobile, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de la stratégie :

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**

2. Dans la page des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **Notifications et rapports**.

3. Dans la section **Notifications**, configurez l'affichage des notifications :

   - Pour masquer toutes les notifications et les messages contextuels, désactivez l'option **Afficher les notifications lorsque Kaspersky Endpoint Security fonctionne en arrière-plan**.

     Kaspersky Endpoint Security for Android affichera uniquement la notification de l'état de protection. La notification affiche l'état de protection des appareils (par exemple,) et le nombre de problèmes. L'application affiche également des notifications lorsque l'utilisateur travaille avec l'application (par exemple, l'utilisateur met à jour les bases antivirus manuellement).

     > Les experts de Kaspersky vous recommandent d'activer les notifications et les messages contextuels. Si vous désactivez les notifications et les messages contextuels lorsque l'application est en mode arrière-plan, l'application n'avertira pas les utilisateurs des menaces en temps réel. Les utilisateurs d'appareils mobiles ne peuvent en savoir plus sur l'état de protection de l'appareil que lorsqu'ils ouvrent l'application.

   - Dans **Liste des problèmes de sécurité affichés sur les appareils des utilisateurs**, sélectionnez les problèmes de Kaspersky Endpoint Security for Android que vous souhaitez afficher sur l'appareil mobile de l'utilisateur.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Détection d'une attaque contre l'appareil (root)

Kaspersky Security Center Web Console permet de détecter le piratage de l'appareil (root). Quand un appareil a été débridé, les fichiers système ne sont pas protégés et peuvent dès lors être modifiés. Il est également possible dans ce cas d'installer des applications tierces sur l'appareil. Après la détection de l'effraction, il est recommandé de restaurer le travail normal de l'appareil.

Pour la détection de la réception des droits root par l'utilisateur, Kaspersky Endpoint Security for Android utilise les services suivants :

- *Service intégré de Kaspersky Endpoint Security for Android.* Un service de Kaspersky qui analyse la réception des droits root par l'utilisateur de l'appareil mobile (Kaspersky Mobile Security SDK).

- *SafetyNet Attestation.* Un service de Google qui analyse l'intégrité du système d'exploitation, analyse le logiciel et le matériel de l'appareil, et définit les autres problèmes de sécurité. Pour en savoir plus sur le fonctionnement de SafetyNet Attestation, consultez le site Internet de l'assistance technique Android.

En cas de piratage de l'appareil, vous recevrez une notification. Vous pouvez afficher les notifications de piratage dans Kaspersky Security Center Web Console sous l'onglet **SURVEILLANCE ET RAPPORTS** > **TABLEAU DE BORD**. Vous pouvez également désactiver la notification relatives à l'effraction dans les paramètres de notifications d'événements.

Sur les appareils Android, vous pouvez imposer des limites sur l'utilisation de l'appareil par l'utilisateur (par exemple, verrouiller l'appareil) si l'appareil a été piraté. Vous pouvez définir de telles limites à l'aide du composant Contrôle de conformité. Pour ce faire, créez une règle de conformité avec le critère **Autorisations root reçues sur l'appareil**

Définition des paramètres de licence

Pour administrer les appareils mobiles dans Kaspersky Security Center Web Console ou Cloud Console, vous devez activer l'application Kaspersky Endpoint Security for Android sur les appareils mobiles. L'activation de l'application Kaspersky Endpoint Security for Android sur un appareil mobile s'effectue en fournissant des informations de licence valides à l'application. Les informations sur la licence sont transmises à l'appareil mobile avec la stratégie lors de la synchronisation de l'appareil avec Kaspersky Security Center.

Si Kaspersky Endpoint Security for Android n'est pas activé dans les 30 jours qui suivent l'installation sur l'appareil mobile, l'application passe automatiquement en mode limité. Dans ce mode de fonctionnement, la majorité des composants de l'app est inopérationnelle. Lorsque l'application passe en mode limité, elle ne réalise plus la synchronisation automatique avec Kaspersky Security Center. Dès lors, si l'application n'est pas activée pour une raison quelconque dans les 30 jours qui suivent l'installation, l'utilisateur doit synchroniser l'appareil avec Kaspersky Security Center manuellement.

Pour définir les paramètres de licence d'une stratégie de groupe :

1. Ouvrez la fenêtre des propriétés de la stratégie :

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **STRATÉGIES ET PROFILS**. Dans la liste des stratégies de groupe qui s'ouvre, cliquez sur le nom de la stratégie que vous souhaitez configurer.

   - Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, sélectionnez **APPAREILS** > **MOBILE** > **APPAREILS**. Cliquez sur l'appareil mobile qui relève de la stratégie que vous souhaitez configurer, puis sélectionnez la stratégie dans l'onglet **POLITIQUES ACTIVES ET PROFILS DE POLITIQUES.**

2. Dans la page des propriétés de la stratégie, sélectionnez **PARAMÈTRES DE L'APPLICATION** > **Licences**.

3. Utilisez la liste déroulante pour sélectionner la clé de licence requise dans le stockage des clés du Serveur d'administration.

   Les détails de la clé de licence s'affichent dans les champs ci-dessous.

   Vous pouvez remplacer la clé d'activation existante sur l'appareil mobile si elle est différente de celle sélectionnée dans la liste déroulante ci-dessus. Pour cela, cochez la case **Si la clé sur l'appareil diffère, replacez-la par cette clé**.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications que vous avez apportées à la stratégie et quitter la fenêtre des propriétés de la stratégie.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Configuration des événements

Vous pouvez définir les paramètres de stockage et de notification des événements qui surviennet sur les appareils de vos utilisateurs et qui sont envoyés à Kaspersky Security Center.

Vous pouvez configurer des événements uniquement lors de la modification d'une stratégie.

Les événements sont répartis par niveau d'importance sous les onglets suivants :

- **Critique**

  Un événement critique indique un problème pouvant entraîner une perte de données, un dysfonctionnement ou une erreur critique.

- **Panne de fonction**

  Une panne de fonction indique un problème grave, une erreur ou un dysfonctionnement qui s'est produit pendant le fonctionnement de l'application.

- **Avertissement**

  Un avertissement n'est pas nécessairement grave, mais indique néanmoins un problème potentiel futur.

- **Info**

  Un événement informatif signale la réussite d'une opération ou d'une procédure ou le fonctionnement adéquat de l'application.

Dans chaque section, la liste reprend les types d'événements et la durée de stockage des événements par défaut dans Kaspersky Security Center (en jours).

Vous pouvez effectuer les opérations suivantes au départ de la liste des événements :

- Ajouter ou supprimer un type d'événement dans la liste des types d'événements envoyés à Kaspersky Security Center.

- Définir les paramètres de stockage et de notification pour chaque type d'événement, par exemple : la durée de stockage des événements de ce type dans la base de données du Serveur d'administration ou la notification des événements de ce type par email.

Pour en savoir plus sur l'administration des stratégies et des groupes d'administration dans Kaspersky Security Center Web Console et Cloud Console :

- Si vous utilisez Kaspersky Security Center Web Console, veuillez consulter l'*Aide de Kaspersky Security Center*.

- Si vous utilisez Kaspersky Security Center Cloud Console, veuillez vous reporter à l'*Aide de Kaspersky Security Center Cloud Console*.

Configuration d'événements relatifs à l'installation, à la mise à jour et à la suppression d'applications sur les appareils des utilisateurs

Si vous utilisez Kaspersky Security Center Cloud Console, la liste des types d' événements qui surviennent sur les appareils de vos utilisateurs et qui sont envoyés à Kaspersky Security Center n'inclut pas l'installation, la mise à jour et la suppression des applications sur les appareils. En effet, de tels événements se produisent souvent et pourraient remplacer d'autres événements importants dans la base de données de Kaspersky Security Center en cas d'atteinte de la limite du nombre d'événements. Ils peuvent également affecter les performances du Serveur d'administration ou du SGBD et la bande passante de la connexion Internet avec Kaspersky Security Center Cloud Console.

Si vous souhaitez néanmoins conserver les événements de ce type et en être averti, suivez les instructions fournies ci-après.

Pour configurer les événements relatifs à l'installation, à la mise à jour et à la suppression d'applications sur les appareils des utilisateurs :

1. Dans les paramètres d'une stratégie, accédez à l'onglet **CONFIGURATION DES ÉVÉNEMENTS**, ajoutez le type d'événement d'information **Application installée ou supprimée (liste des applications installées)** à la liste des événements stockés dans la base de données du Serveur d'administration.

   Pour en savoir plus sur la configuration des événements, reportez-vous à *l'aide de Kaspersky Security Center Cloud Console*.

2. Activez l'option **Envoyer une liste des applications installées sur tous les appareils mobiles** option.

Les événements concernant l'installation, la mise à jour et la suppression des applications sur les appareils des utilisateurs sont stockés dans la base de données de Kaspersky Security Center. Vous êtes informé de ces événements.

Charge sur le réseau

Cette section contient des informations sur le volume du trafic réseau qu'échangent entre eux-mêmes les appareils mobiles et Kaspersky Security Center lors du fonctionnement.

Débit du trafic

Tâche	Trafic sortant	Trafic entrant	Trafic général
Déploiement initial de l'application, Mo	0.08	17.76	17.84
Mise à jour initiale des bases antivirus (le volume du trafic peut varier à cause de la taille des bases antivirus), Mo	0.04	2.21	2.25
Synchronisation de l'appareil mobile avec Kaspersky Security Center, Mo	0.03	0.02	0.05
Mise à jour régulière des bases antivirus (le volume du trafic peut varier à cause de la taille des bases antivirus), Mo	0.08	3.06	3.14
Exécution des commandes d'Antivol. Géolocaliser (le volume du trafic peut varier à cause des caractéristiques de l'appareil-photo intégré et de la qualité des images), Mo	0.09	0.8	0.17
Exécution des commandes d'Antivol. Prise de photos, Mo	1.0	0.02	1.02
Exécution des commandes d'Antivol. Verrouillage de l'appareil, Mo	0.06	0.05	0.11

Volume moyen par jour, Mo	0.22	6.96	7.18

Utilisation de la console d'administration basée sur MMC

Cette section d'aide décrit la protection et l'administration des appareils mobiles à l'aide de la Console d'administration basée sur MMC de Kaspersky Security Center.

Principaux cas d'utilisation

INSTALLATION

Comment puis-je installer Kaspersky Endpoint Security for Android à distance ?

Comment puis-je empêcher qu'un utilisateur ne supprime Kaspersky Endpoint Security for Android ?

Comment puis-je activer Kaspersky Endpoint Security for Android ?

PROTECTION

Comment-puis verrouiller un appareil en cas de perte ou de vol ?

Comment se protéger contre les menaces Internet ?

Comment interdire l'utilisation d'un mot de passe vide ?

UTILISATION DE SOLUTIONS TIERCES

Android Enterprise (Applications avec un "portefeuille", Configuration du profil de travail Android)

VMware AirWatch, MobileIron, IBM Maas360, SOTI MobiControl

CONTRÔLE

Comment puis-je empêcher qu'un utilisateur ne joue avec l'appareil ?

Comment configurer l'accès aux sites Internet sur un appareil ?

Comment puis-je détecter les privilèges root ?

ADMINISTRATION

Comment puis-je configurer une boîte aux lettres sur un appareil ?

Comment puis-je connecter un appareil mobile au réseau Wi-Fi ?

Comment puis-je installer une application d'entreprise ?

A propos de Kaspersky Security for Mobile

Kaspersky Security 10 for Mobile est une solution intégrée de protection et d'administration des appareils mobiles d'entreprise ainsi que des appareils mobiles personnels des employés utilisés dans un but professionnel.

Kaspersky Security for Mobile comprend les modules suivants :

- Application mobile Kaspersky Endpoint Security for Android.

  L'application Kaspersky Endpoint Security for Android assure la protection des appareils mobiles contre les menaces Internet, les virus et autres programmes qui constituent des menaces.

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

Le plug-in d'administration de Kaspersky Endpoint Security for Android assure l'administration par interface des appareils mobiles et de leurs applications via la Console d'administration de Kaspersky Security Center.

- Plug-in d'administration de Kaspersky Device Management for iOS

  Le plug-in d'administration Kaspersky Device Management for iOS permet de configurer les paramètres de configuration des appareils connectés à Kaspersky Security Center selon le protocole MDM iOS (ci-après les appareils MDM iOS) et Exchange ActiveSync (ci-après les appareils EAS), sans utiliser iPhone Configuration Utility et les consoles de gestion Exchange.

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.

L'application mobile Kaspersky Endpoint Security for Android peut également fonctionner au sein du système d'administration à distance *Kaspersky Endpoint Security Cloud*. Pour en savoir plus sur l'utilisation des apps via Kaspersky Endpoint Security Cloud, consultez l'aide en *ligne de Kaspersky Endpoint Security Cloud*.

L'application mobile Kaspersky Endpoint Security for Android peut aussi fonctionner comme partie des solutions EMM tierces des participants d'AppConfig Community.

Principales fonctionnalités de l'administration des appareils mobiles dans la console d'administration basée sur MMC

Kaspersky Security for Mobile fournit les fonctionnalités suivantes :

- Diffusion d'emails pour la connexion d'appareils tournant sous Android à Kaspersky Security Center sous la forme de liens vers Google Play ;
- Connexion à distance des appareils mobiles des utilisateurs à Kaspersky Security Center et d'autres systèmes EMM tiers (par exemple, VMWare AirWatch, MobileIron, IBM Maas360, SOTI MobiControl) ;
- Configuration à distance de l'application Kaspersky Endpoint Security for Android, ainsi que des services, des applications et des fonctions des appareils Android ;
- configuration à distance des appareils mobiles conformément aux exigences de sécurité de l'entreprise ;
- Prévention des fuites de données de l'entreprise stockées sur les appareils mobiles en cas de perte ou de vol de ceux-ci (Antivol) ;
- vérification du respect des exigences de sécurité de l'entreprise (Contrôle de conformité) ;
- Contrôle de l'utilisation d'Internet sur les appareils mobiles (Protection Internet) ;
- Configuration de la messagerie professionnelle sur les appareils mobiles, y compris si le serveur de messagerie Microsoft Exchange est déployé dans l'entreprise (uniquement pour les appareils iOS et Samsung) ;
- Configuration du réseau de l'entreprise (Wi-Fi, VPN) permettant l'utilisation du VPN sur les appareils mobiles ; Le VPN peut être configuré uniquement sur les appareils iOS et Samsung ;
- configuration de l'affichage de l'état de l'appareil mobile dans Kaspersky Security Center en cas de violation des règles de la stratégie : Critique, Avertissement, OK ;

- Configuration des notifications présentées à l'utilisateur dans l'application Kaspersky Endpoint Security for Android ;
- configuration des paramètres des appareils compatibles avec Samsung KNOX 2.6 et suivants ;
- Configuration des paramètres sur les appareils prenant en charge les profils de travail Android ;
- Déploiement de l'application Kaspersky Endpoint Security for Android via la console Samsung KNOX Mobile Enrollment. Samsung KNOX Mobile Enrollment est destiné à l'installation en masse et à la configuration initiale d'applications sur des appareils Samsung obtenus auprès de revendeurs officiels ;
- Mise à jour de l'application Kaspersky Endpoint Security for Android jusqu'à la version définie à l'aide de stratégies de Kaspersky Security Center ;
- Notification de l'administrateur sur l'état et les événements dans le fonctionnement de l'application Kaspersky Endpoint Security for Android dans Kaspersky Security Center ou par email ;
- Contrôle des modifications des paramètres de la stratégie (Historique des révisions).

Kaspersky Security for Mobile comprend les modules de protection et d'administration suivants :

- Antivirus (pour les appareils Android) ;
- Antivol (pour les appareils Android) ;
- Protection Internet (pour les appareils Android et iOS) ;
- Contrôle des Applications (pour les appareils Android) ;
- Contrôle de conformité (pour les appareils Android) ;
- Détection des privilèges root sur les appareils (pour les appareils Android).

A propos de l'app Kaspersky Endpoint Security for Android

L'application Kaspersky Endpoint Security for Android assure la protection des appareils mobiles contre les menaces Internet, les virus et autres programmes qui constituent des menaces.

L'app Kaspersky Endpoint Security for Android inclut les modules suivants :

- **Antivirus**. 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 cloud du Kaspersky Security Network. L'Antivirus présente les composants suivants :
  - Protection. La protection permet de découvrir les menaces dans les fichiers ouverts, d'analyser les nouvelles app et de prévenir l'infection du périphérique en temps réel.
  - Analyse. Lancée à la demande pour l'ensemble du système de fichiers, uniquement pour les apps installées ou le fichier ou le dossier sélectionné.
  - Mise à jour. La mise à jour permet de télécharger les nouvelles bases antivirus de l'app.
- **Antivol.** Ce composant protège les informations de l'appareil contre tout accès non autorisé en cas de perte ou de vol de l'appareil. Ce composant vous permet d'envoyer les commandes suivantes à l'appareil :

- **Géolocaliser** pour obtenir les coordonnées de l'emplacement de l'appareil.
- **Alarme** pour faire sonner l'appareil.
- **Photographier** pour que l'appareil prenne des photos avec la caméra avant si quelqu'un tente de le déverrouiller.
- **Suppression** des données d'entreprise pour protéger les informations sensibles de l'entreprise.

- **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 ligne 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 cloud 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 cloud 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, loterie, tirages au sort" ou "Communication via Internet", par exemple).

- **Contrôle des applications.** Ce composant vous permet d'installer les apps recommandées et requises sur votre appareil à l'aide d'un lien direct vers la distribution ou vers Google Play. Grâce au Contrôle des applications, vous pouvez supprimer les applications interdites, non conformes aux exigences à la sécurité corporative.

- **Contrôle de conformité.** Ce composant permet de vérifier la conformité des appareils gérés par rapport aux exigences de sécurité de l'entreprise et d'imposer des restrictions sur certaines fonctions des appareils non conformes.

A propos de Kaspersky Device Management for iOS

Kaspersky Device Management for iOS assure la protection et le contrôle des appareils mobiles qui sont connectés à Kaspersky Security Center et comprend des fonctions de gestion des appareils, telles que :

- **Protection par mot de passe**. Cette fonction vous permet de définir des exigences de complexité des mots de passe afin que les utilisateurs utilisent des mots de passe complexes conformes à la stratégie de l'entreprise en la matière.

- **Gestion du réseau**. Cette fonction vous permet d'ajouter des réseaux VPN et Wi-Fi approuvés ou de restreindre l'accès à d'autres.

- **Suppression des données d'entreprise**. En cas de perte ou de vol de l'appareil, vous pouvez lui envoyer la commande Suppression pour protéger les informations sensibles de l'entreprise.

- **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 ligne 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 cloud 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 cloud 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, loterie, tirages au sort" ou "Communication via Internet", par exemple).

- **Restrictions des applications.** Ce composant vous permet de contrôler si les applications natives d'un appareil, telles que iTunes, Safari ou Game Center peuvent être utilisées sur un appareil contrôlé.

- **Restrictions des fonctionnalités.** Ce composant permet de vérifier la conformité des appareils gérés par rapport aux exigences de sécurité de l'entreprise et d'imposer des restrictions sur certaines fonctions des appareils non conformes.

A propos de la boîte aux lettres Exchange

La *boîte aux lettres Exchange* est une app client du service Exchange ActiveSync. L'application permet aux utilisateurs en entreprise de gérer l'email, le calendrier, les contacts et les tâches. La boîte aux lettres Exchange permet de connecter l'appareil mobile au serveur Microsoft Exchange. Pour en savoir plus sur le service Exchange ActiveSync, consultez le site Internet de *l'assistance technique de Microsoft*.

L'administration des appareils mobiles à l'aide du protocole Exchange ActiveSync requiert le déploiement du Serveur Exchange sur le serveur Microsoft Exchange. Pour en savoir plus sur l'installation d'un Serveur Exchange, veuillez vous reporter à l'*Aide de Kaspersky Security Center*. Aucune configuration complémentaire n'est requise sur les appareils mobiles.

La boîte aux lettres Exchange vous permet de configurer à distance les appareils EAS à l'aide de stratégies de groupe et d'envoyer une commande de suppression des données. Le protocole Exchange ActiveSync prend en charge les systèmes d'exploitation suivants :

- Windows Mobile ;
- Windows CE ;
- Windows Phone ;
- Android ;
- Bada ;
- BlackBerry 10 ;
- iOS ;
- Symbian.

L'ensemble de paramètres d'administration d'un appareil Exchange ActiveSync dépend du système d'exploitation sous lequel l'appareil mobile fonctionne. La documentation pour ce système d'exploitation reprend les particularités de prise en charge du protocole Exchange ActiveSync pour un système d'exploitation concret.

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

Le plug-in d'administration de Kaspersky Endpoint Security for Android 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 for Android permet de :

- Créer une stratégie de sécurité de groupe pour les périphériques mobiles ;

- configurer à distance les paramètres de fonctionnement de l'application Kaspersky Endpoint Security for Android sur les appareils mobiles des utilisateurs ;
- recevoir les rapports et les statistiques sur le fonctionnement de Kaspersky Endpoint Security for Android sur les appareils des utilisateurs.

Le plug-in d'administration Kaspersky Endpoint Security for Android s'installe par défaut lors du déploiement de Kaspersky Security Center. Le plug-in ne requiert pas une installation distincte.

A propos du plug-in d'administration de Kaspersky Device Management for iOS

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

- Créer une stratégie de sécurité de groupe pour les périphériques mobiles ;
- Configurer à distance les appareils connectés selon le protocole Exchange ActiveSync (ci-après, les appareils EAS) ;
- Configurer à distance les appareils connectés selon le protocole iOS MDM (ci-après, les appareils iOS MDM) ;
- Recevoir des rapports et des statistiques sur le fonctionnement des appareils mobiles des utilisateurs.

Pour en savoir plus sur la connexion d'appareils mobiles au Kaspersky Security Center selon les protocoles MDM iOS et Exchange ActiveSync, consultez *l'Aide de Kaspersky Security Center*.

Le plug-in d'administration Kaspersky Device Management for iOS s'installe par défaut lors du déploiement de Kaspersky Security Center. Le plug-in ne requiert pas d'installation séparée.

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 l'aide de *Kaspersky Security Center*.

Pour le fonctionnement du plug-in d'administration de Kaspersky Endpoint Security for Android, la Console d'administration de Kaspersky Security Center 12 ou version supérieure doit être installée sur l'ordinateur de l'administrateur.

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

- Console d'administration de Kaspersky Security Center 12 ou version supérieure ;
- composant serveur Exchange ;
- Serveur des appareils 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 12 ou version supérieure ;
- Plug-in d'administration de Kaspersky Endpoint Security for Android.

Pour le déploiement de l'application mobile Kaspersky Endpoint Security for Android à partir des boutiques en ligne correspondantes, la configuration requise pour l'ordinateur de l'administrateur n'est pas précisée.

L'application mobile Kaspersky Endpoint Security for Android peut également fonctionner au sein du système d'administration à distance Kaspersky Endpoint Security Cloud 6.0 et plus. Pour en savoir plus sur l'utilisation des apps via Kaspersky Endpoint Security Cloud, consultez l'*aide de Kaspersky Endpoint Security Cloud*.

L'application mobile Kaspersky Endpoint Security for Android peut aussi fonctionner comme partie des systèmes EMM tiers :

- VMWare AirWatch 9.3 et suivant ;
- MobileIron 10.0 et version supérieure ;
- IBM MaaS360 10.68 et version supérieure ;
- Microsoft Intune 1908 et version supérieure ;
- SOTI MobiControl 14.1.4 (1693) et version supérieure.

Configurations matérielle et logicielle requises sur l'appareil mobile de l'utilisateur pour prendre en charge l'installation de l'application Kaspersky Endpoint Security for Android

L'application 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 ;
- Android 5.0 à 12 (y compris Android 12L, sauf Go Edition) ;
- processeur d'architecture x86, x86-64, ARM5, ARM6, ARM7, ARM8.

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

Configurations logicielles et matérielles de l'appareil mobile de l'utilisateur pour le profil iOS MDM

Le profil iOS MDM requiert les configurations logicielles et matérielles suivantes :

- iOS 10.0 à 15.0 ou iPadOS 13 à 15 ;
- connexion à Internet.

Questions et éléments particuliers à prendre en considération connues

Kaspersky Endpoint Security for Android comporte une série de problèmes connus non critiques pour le fonctionnement de l'application.

Problèmes connus lors de l'installation des applications

- Kaspersky Endpoint Security for Android s'installe seulement dans la mémoire principale de l'appareil.
- Sur les appareils tournant sous Android 7.0, lors de la tentative de désactivation des privilèges d'administrateur pour Kaspersky Endpoint Security for Android dans les paramètres de l'appareil, un échec peut survenir si la superposition de fenêtres est interdite pour Kaspersky Endpoint Security for Android. Le problème est lié à un défaut connu dans Android 7.
- L'app Kaspersky Endpoint Security for Android sur les appareils tournant sous Android 7.0 et suivant ne prend pas en charge le mode d'affichage de plusieurs fenêtres.
- Kaspersky Endpoint Security for Android ne fonctionne pas sur les appareils Chromebook tournant sous Chrome.
- Kaspersky Endpoint Security for Android ne fonctionne pas sur les appareils tournant sous Android (Go edition).
- Lors de l'utilisation de l'application Kaspersky Endpoint Security for Android avec des systèmes EMM tiers (par exemple, VMWare AirWatch), seuls les composants Antivirus et Protection Internet sont accessibles. L'administrateur peut configurer les paramètres de l'Antivirus et de Protection Internet dans la console du système EMM. Dans ce cas, les notifications du fonctionnement de l'application sont accessibles seulement dans l'interface de l'application Kaspersky Endpoint Security for Android (Rapports).

Problèmes connus lors de la mise à jour de la version de l'application

- Vous pouvez mettre à jour Kaspersky Endpoint Security for Android uniquement jusqu'à la version la plus récente de l'application. Il est impossible de mettre à jour Kaspersky Endpoint Security for Android vers une version plus ancienne.
- Pour réaliser la mise à jour de Kaspersky Endpoint Security for Android à l'aide d'un paquet d'installation autonome sur l'appareil mobile de l'utilisateur, le système doit autoriser l'installation d'apps depuis des sources inconnues.
- La mise à jour à l'aide de Google Play est accessible si Kaspersky Endpoint Security for Android est installé depuis Google Play. Si l'application est installée d'une autre manière, la mise à jour à l'aide de Google Play est impossible.
- La mise à jour via Kaspersky Security Center est accessible si Kaspersky Endpoint Security for Android est installé via Kaspersky Security Center. Si l'application est installée depuis Google Play, la mise à jour via Kaspersky Security Center est impossible.

- Après l'installation de la version technique 33 des plug-ins d'administration, il faut également installer la version technique 33 de l'application Kaspersky Endpoint Security for Android. Dans le cas contraire, vous ne pourrez pas activer Samsung KNOX sur certains appareils de vos utilisateurs.

Problèmes connus dans le fonctionnement de l'Antivirus

- En raison de restrictions techniques, Kaspersky Endpoint Security for Android n'est pas capable d'analyser les fichiers de 2 Go ou plus. Dans le cadre de l'analyse, l'app ignore ces fichiers et ne les signale pas.
- Pour une analyse supplémentaire de l'appareil afin d'y détecter des nouvelles menaces dont les informations ne sont pas encore entrées dans les bases antivirus, vous devez activer l'utilisation de Kaspersky Security Network. *Kaspersky Security Network (KSN)* est une infrastructure de services cloud offrant un accès à la base opérationnelle de connaissances de Kaspersky sur la réputation des fichiers, des ressources Internet et du logiciel. L'utilisation de KSN nécessite la connexion de l'appareil mobile à Internet.
- Dans certains cas, la mise à jour des bases antivirus à partir du Serveur d'administration sur un appareil mobile peut échouer. Dans ce cas, exécutez la tâche de mise à jour de la base antivirus sur le Serveur d'administration.
- Sur certains appareils, Kaspersky Endpoint Security for Android ne détecte pas les appareils connectés via USB OTG. Il est impossible d'exécuter la recherche de virus sur ces appareils.
- Sur les appareils exécutant Android 11.0 ou une version ultérieure, l'utilisateur doit accorder l'autorisation " Autoriser l'accès pour gérer tous les fichiers ".
- Sur les appareils tournant sous Android 7.0 et suivant, la fenêtre de programmation de la recherche de virus peut ne pas s'afficher correctement (les éléments d'administration ne sont pas affichés). Le problème est lié à un défaut connu dans Android 7.
- Sur les appareils exécutant Android 7.0, la protection en temps réel en mode étendu ne détecte pas les menaces dans les fichiers stockés sur une carte SD externe.
- Sur les appareils tournant sous Android 6.0, Kaspersky Endpoint Security for Android ne détecte pas le téléchargement d'un fichier malveillant dans la mémoire de l'appareil. Un fichier malveillant peut être détecté par l'Antivirus lors du lancement du fichier ou lors de la recherche de virus sur l'appareil. Le problème est lié à un défaut connu dans Android 6.0. Pour assurer la sécurité de l'appareil, il est recommandé de configurer le lancement de la recherche de virus d'après l'horaire planifié.

Problèmes connus dans le fonctionnement de la Protection Internet

- La Protection Internet sur les appareils Android fonctionne seulement dans les navigateurs Google Chrome (y compris la fonction Onglets personnalisés), Huawei Browser et Samsung Internet Browser. La Protection Internet pour le navigateur Samsung Internet ne bloque pas les sites sur un appareil mobile si un profil de travail est utilisé et que la Protection Internet est activée uniquement pour ce profil de travail.
- Kaspersky Endpoint Security dans le profil de travail analyse uniquement le domaine de site Internet dans le trafic HTTPS. Les sites Internet malveillants et de phishing peuvent rester déverrouillés si l'application est installée dans le profil de travail. Si le domaine est un domaine de confiance, la Protection Internet peut ignorer une menace (par exemple, `https://trusted.domain.com/phishing/`). Si le domaine n'est pas un domaine de confiance, la Protection Internet bloque les sites Internet malveillants et de phishing.
- Pour le fonctionnement de la Protection Internet, vous devez activer l'utilisation de Kaspersky Security Network. La Protection Internet bloque les sites Internet à la base des données sur la réputation et les catégories des sites Internet, qui se trouvent dans KSN.

- Sur les appareils tournant sous Android 6.0 avec le navigateur installé Google Chrome version 51 ou les versions précédentes, les sites internet interdits peuvent ne pas être bloqués par la Protection Internet s'ils sont ouverts par les moyens suivants (le problème est liée à un défaut connu dans Google Chrome) :
  - suite à une requête de recherche ;
  - à partir de la liste des signets ;
  - à partir de l'historique des requêtes de recherche ;
  - lors de l'utilisation de la fonction de remplissage automatique de l'adresse Internet ;
  - lors de l'ouverture du site Internet dans un nouvel onglet dans Google Chrome.
- Les Sites internet interdits peuvent ne pas être bloqués dans le navigateur Google Chrome de la version 50 ou antérieures si le site Internet est ouvert depuis les résultats de recherche Google et que l'option "**Fusionner les onglets et les applications**" a été cochée dans les paramètres du navigateur. Le problème est lié à un défaut connu dans Google Chrome.
- Il se peut que les sites Internet des catégories interdites ne soient pas bloqués dans Google Chrome si l'utilisateur les ouvre depuis des applications tierces (par exemple, depuis un client IM). Le problème est lié aux particularités du fonctionnement du service des fonctions d'accessibilité avec la fonction Chrome Custom Tabs.
- Les sites internet interdits ne peuvent être bloqués dans Samsung Internet Browser si l'utilisateur les ouvre en mode d'arrière-plan via un menu contextuel ou depuis des applications tierces (par exemple, depuis un client IM).
- Pour que Protection Internet fonctionne, Kaspersky Endpoint Security for Android doit être installé en tant que service des Fonctionnalités d'accessibilité.
- Lors de la saisie de l'adresse du site Internet dans les paramètres de la Protection Internet, observez les règles suivantes :
  - Pour les appareils Android, indiquez l'adresse dans le format des expressions régulières (par exemple, `http:\/\/www\.example\.com.*`).
  - Pour les appareils MDM iOS, indiquez le protocole de transfert de données HTTP ou HTTPS (par exemple, `http://www.example.com`).
- Les sites Internet autorisés peuvent être bloqués dans Samsung Internet Browser en mode de Protection Internet **Seuls les sites Internet répertoriés sont autorisés** lors de la mise à jour de la page. Les sites Internet sont bloqués si l'expression régulière contient des paramètres supplémentaires (par exemple, `^https?:\/\/example\.com\/pictures\/`). Il est recommandé d'utiliser des expressions régulières sans paramètres supplémentaires (par exemple, `^https?:\/\/example\.com`).

Problèmes connus dans le fonctionnement de l'Antivol

- Pour un envoi opportun des commandes aux appareils Android, l'application utilise le service Firebase Cloud Messaging (FCM). Si FCM n'est pas configuré, les commandes seront envoyées à l'appareil seulement lors de la synchronisation avec Kaspersky Security Center d'après l'horaire spécifié dans la stratégie par exemple, toutes les 24 heures.
- Pour le verrouillage de l'appareil, Kaspersky Endpoint Security for Android doit être installé en tant qu'administrateur de l'appareil.

- Sur les appareils tournant sous le système d'exploitation Android version 7.0 et suivantes pour le verrouillage de l'appareil, Kaspersky Endpoint Security for Android doit être installé en tant que service des Fonctionnalités d'accessibilité.
- Sur certains appareils, les commande d'Antivol ne peuvent pas être exécutées si le mode d'économie d'énergie est activé. Ce défaut est confirmé sur Alcatel 5080X.
- Pour localiser des appareils tournant sous Android 10.0 ou une version ultérieure, l'utilisateur doit accorder l'autorisation "Tout le temps" à la localisation de l'appareil.
- Pour prendre une photo avec des appareils tournant sous Android 11.0 ou une version ultérieure, l'utilisateur doit accorder l'autorisation "Pendant l'utilisation de l'application" pour accéder à la caméra.

Problèmes connus dans le fonctionnement du Contrôle des applications

- Pour que le contrôle des applications fonctionne, Kaspersky Endpoint Security for Android doit être installé en tant que service des Fonctionnalités d'accessibilité.
- Pour le fonctionnement du contrôle des applications (catégorie des applications), l'utilisation de Kaspersky Security Network doit être activée. Le contrôle des applications définit des catégories d'applications en fonction des données contenues dans KSN. L'utilisation de KSN nécessite la connexion de l'appareil mobile à Internet. Pour le fonctionnement du contrôle des applications, vous pouvez ajouter des applications séparées dans les listes des applications bloquées et des applications autorisées. Dans ce cas, KSN n'est pas obligatoire.
- Lors de la configuration du contrôle des applications, il est recommandé de décocher la case **Bloquer les apps système**. Le blocage des apps système peut donner lieu à des défaillances dans le fonctionnement de l'appareil.

Problèmes connus lors de la configuration de l'email

- La configuration à distance de la boîte aux lettres est accessible seulement sur les appareils suivants :
  - appareils MDM iOS ;
  - appareils Samsung (Exchange ActiveSync).
  - appareils Android avec le client de messagerie installé TouchDown.

    Dans les versions précédentes de Kaspersky Endpoint Security for Android, vous pouvez configurer à distance les paramètres du profil TouchDown sur l'appareil de l'utilisateur à l'aide de Kaspersky Security Center. Sur Kaspersky Endpoint Security for Android Service Pack 4, TouchDown n'est plus pris en charge. Pour plus de détails, consultez le *site du Support Technique Symantec*.

    Après la mise à jour du plug-in Kaspersky Endpoint Security for Android, les paramètres TouchDown dans la stratégie sont masqués mais sont enregistrés. Lors de la connexion de nouveaux appareils, les paramètres TouchDown seront configurés après l'application de la stratégie.

    Après la modification et la conservation de la stratégie, les paramètres TouchDown seront supprimés. Les paramètres TouchDown sur les appareils des utilisateurs seront supprimés après l'application de la stratégie.

Problèmes connus lors de la configuration de la sécurité du mot de passe de déverrouillage de l'appareil

- Sur les appareils tournant sous Android 10.0 ou une version ultérieure, Kaspersky Endpoint Security résout les exigences de force du mot de passe en une des valeurs du système : moyenne ou élevée.

  Si la longueur du mot de passe requise est de 1 à 4 symboles, l'application invite l'utilisateur à définir un mot de passe de force moyenne. Elle doit être soit numérique (PIN) sans séquence répétée ou ordonnée (par exemple 1234), soit alphanumérique. Le code PIN ou le mot de passe doit comporter au moins 4 caractères.

  Si la longueur du mot de passe requise est d'au moins 5 symboles, l'application invite l'utilisateur à définir un mot de passe de force élevée. Elle doit être soit numérique (PIN) sans séquence répétée ou ordonnée, soit alphanumérique (mot de passe). Le code PIN doit comporter au moins 8 chiffres ; le mot de passe doit comporter au moins 6 caractères.

- Sur les appareils tournant sous Android 10.0 ou une version ultérieure, l'utilisation de l'empreinte digitale pour déverrouiller l'écran peut être administrée pour le profil de travail uniquement.

- Sur appareils tournant sous Android 7.1.1, si le mot de passe de déverrouillage ne respecte pas les exigences de sécurité de l'entreprise (Contrôle de conformité), l'app système Paramètres peut ne pas fonctionner correctement lors d'une tentative de modification du mot de passe de déverrouillage via Kaspersky Endpoint Security for Android. Le problème est lié à un défaut connu dans Android 7.1.1. Pour modifier le mot de passe de déverrouillage dans ce cas, utilisez uniquement l'app système Paramètres.

- Sur certains appareils sous Android 6.0 ou suivant, une erreur peut se produire lors de la saisie du mot de passe de déverrouillage de l'écran si les données de l'appareil sont chiffrées. Le problème est lié aux particularités du fonctionnement du service des fonctionnalités d'accessibilité avec le firmware MIUI.

Problèmes connus lors de la configuration du Wi-Fi

- · Sur les appareils fonctionnant sous le système d'exploitation Android version 8.0 ou supérieure, il est impossible de configurer les paramètres du serveur proxy pour le réseau Wi-Fi à l'aide d'une stratégie. Vous pouvez configurer les paramètres du serveur proxy pour le réseau Wi-Fi sur l'appareil mobile manuellement.

Problèmes connus lors de la configuration de l'APN

- La configuration à distance d'APN est accessible seulement sur les appareils MDM iOS ou les appareils Samsung.

- Configurez APN pour les appareils MDM iOS dans la section **Communication cellulaire**. La section **APN** est dépassée. Avant la configuration des paramètres d'APN, assurez-vous que la case **Appliquer les paramètres à l'appareil** est décochée dans la section **APN**.

Problèmes connus avec le Pare-feu

- L'utilisation du pare-feu est disponible uniquement sur les appareils Samsung.

Problèmes connus lors de la configuration de l'VPN

- La configuration à distance de VPN est accessible seulement sur les appareils suivants :

  - appareils MDM iOS ;

- Appareils Samsung.

Problèmes connus lors de l'utilisation des conteneurs

- Sur Kaspersky Security for Android Service Pack 3 Maintenance Release 2, la création de conteneurs pour les applications mobiles n'est plus prise en charge. Cependant vous pouvez livrer sur les appareils Android les conteneurs créés dans les versions antérieures de l'application.
- Pour installer des apps dans des conteneurs sur l'appareil mobile de l'utilisateur, il faut autoriser l'installation d'apps depuis des sources inconnues. Pour en savoir plus sur l'installation d'apps qui ne proviennent pas de Google Play, consultez l'*aide d'Android*.
- La conteneurisation des applications n'est pas prise en charge pour les appareils Android contenant plus de 65 536 méthodes (multidex configuration).

Problèmes connus avec la protection contre la suppression de l'application

- Kaspersky Endpoint Security for Android doit être installé avec les droits de l'administrateur de l'appareil.
- Sur les appareils tournant sous le système d'exploitation Android version 7.0 et suivantes, Kaspersky Endpoint Security for Android doit être installé en tant que service des Fonctionnalités d'accessibilités pour protéger l'app contre la suppression.
- Sur certains appareils Xiaomi et Huawei, la protection de Kaspersky Endpoint Security for Android contre la suppression ne fonctionne pas. Le problème est lié aux particularités du firmware MIUI 7 et 8 sur Xiaomi et du firmware EMUI sur Huawei.

Problèmes connus lors de la configuration des restrictions de l'appareil

- Sur les appareils tournant sous Android 10.0 ou version ultérieure, l'interdiction d'utiliser les réseaux Wi-Fi n'est pas prise en charge.
- Sur les appareils tournant sous Android 10.0 ou version ultérieure, l'utilisation de la caméra ne peut pas être totalement interdite.
- Sur les appareils tournant sous Android 11 et suivantes, Kaspersky Endpoint Security for Android doit être installé en tant que service des fonctionnalités d'accessibilité. Kaspersky Endpoint Security for Android propose à l'utilisateur d'installer l'app comme service des Fonctionnalités d'accessibilité pendant l'exécution de l'Assistant de configuration initiale. L'utilisateur peut ignorer cette étape ou désactiver ultérieurement le service dans les paramètres de l'appareil. Si tel est le cas, vous ne pourrez pas restreindre l'utilisation de l'appareil photo.

Problèmes connus lors de l'envoi de commandes vers des appareils mobiles

- Sur les appareils tournant sous Android 12 ou version ultérieure, si l'utilisateur a accordé l'autorisation "Utiliser l'emplacement approximatif", l'application Kaspersky Endpoint Security for Android essaie d'abord d'obtenir l'emplacement précis de l'appareil. En cas d'échec, l'emplacement approximatif de l'appareil n'est renvoyé que s'il n'a pas été reçu plus de 30 minutes plus tôt. Sinon, la commande **Géolocaliser l'appareil** échoue.

Problèmes connus avec le profil de travail Android

- Si vous créez un profil de travail Android à l'aide d'une stratégie, l'utilisateur doit accorder l'autorisation "Autoriser l'accès pour gérer tous les fichiers" à Kaspersky Endpoint Security for Android qui est installé sur les appareils tournant sous Android 11 ou version supérieure et qui est associe au profil de travail.

Problèmes connus avec des appareils spécifiques

- Sur certains appareils (par exemple, Huawei, Meizu et Xiaomi), vous devez accorder à Kaspersky Endpoint Security for Android une autorisation de démarrage automatique ou l'ajouter manuellement à la liste des applications qui sont lancées au démarrage du système d'exploitation. Si l'application n'est pas ajoutée à la liste, Kaspersky Endpoint Security for Android cesse d'exécuter toutes les fonctions après le redémarrage de l'appareil mobile. Aussi, si l'appareil a été bloqué, il est impossible de le déverrouiller à l'aide d'une commande. Vous pouvez déverrouiller l'appareil seulement à l'aide du code à usage unique de déblocage.

- Sur certains appareils (par exemple, Meizu, Asus) tournant sous Android 6.0 et suivant, il faut saisir un mot de passe numérique pour déverrouiller l'appareil après le chiffrement des données et le redémarrage de l'appareil. Si l'utilisateur utilise un mot de passe graphique pour le déverrouillage, ce mot de passe graphique doit être converti au format chiffré. Pour savoir comment convertir le schéma en chiffres, consultez le site Internet d'assistance technique du fabricant de l'appareil mobile. Le problème est lié aux particularités du fonctionnement du service des Fonctionnalités d'accessibilité.

- Sur certains appareils Huawei sous Android 5.X, après l'installation de Kaspersky Endpoint Security for Android en tant que services des fonctions d'accessibilité, un message incorrect qui indique l'absence de ces droits s'affiche. Pour masquer ce message, ajoutez l'application aux applications protégées dans les paramètres de l'appareil.

- Sur certains appareils Huawei tournant sous Android 5.X et 6.x, l'utilisateur peut quitter lui-même l'application quand le mode d'économie d'énergie pour Kaspersky Endpoint Security for Android est activé. L'appareil de l'utilisateur n'est pas protégé dans ce cas. Le problème est lié aux particularités du logiciel Huawei. Pour rétablir la protection de l'appareil, lancez Kaspersky Endpoint Security for Android manuellement. Il est recommandé de désactiver le mode Économie d'énergie pour Kaspersky Endpoint Security for Android dans les paramètres de l'appareil.

- Sur les appareils Huawei avec surcouche EMUI sous Android 7.0, l'utilisateur peut masquer la notification sur l'état de la protection de Kaspersky Endpoint Security for Android. Le problème est lié aux particularités du logiciel Huawei.

- Sur certains appareils Xiaomi, lors de la mise en place dans la stratégie d'une longueur de mot de passe dépassant 5 caractères, il sera proposé à l'utilisateur de modifier le mot de passe de déverrouillage de l'écran, et non le code PIN. Il est impossible de définir un code PIN d'une longueur de plus de 5 caractères. Le problème est lié aux particularités du logiciel Xiaomi.

- Sur les appareils Xiaomi, avec surcouche MIUI sous Android 6.0, l'icône de Kaspersky Endpoint Security for Android peut être masquée dans la barre d'état. Le problème est lié aux particularités du logiciel Xiaomi. Il est recommandé d'autoriser l'affichage des icônes de notification dans les paramètres des notifications.

- Sur certains appareils Nexus tournant sous Android 6.0.1, il est impossible d'octroyer les autorisations nécessaires au bon fonctionnement pendant l'utilisation de l'Assistant de configuration initiale de Kaspersky Endpoint Security for Android. Le problème est lié à un défaut connu dans Security Patch pour Android de Google. Pour le fonctionnement correct de l'application, les droits nécessaires doivent être attribués normalement dans les paramètres de l'appareil.

- Sur certains appareils Samsung tournant sous le système d'exploitation Android 7.0 et version ultérieure, si l'utilisateur tente de configurer des modes de déverrouillage de l'appareil non pris en charge (par exemple, mot de passe graphique), l'appareil peut être verrouillé si les conditions suivantes sont réunies : la protection contre la suppression de Kaspersky Endpoint Security for Android est activée et les exigences de la sécurité du mot de passe de déverrouillage de l'écran sont définies. Pour déverrouiller l'appareil, il faut lui envoyer une commande spéciale.

- Sur certains appareils Samsung, il est impossible d'interdire l'utilisation des empreintes digitales pour le déverrouillage de l'écran.
- Sur certains appareils Samsung, Protection Internet ne fonctionne pas si l'appareil est connecté à un réseau 3G/4G, si le mode d'économie d'énergie est activé sur l'appareil et si les données d'arrière-plan sont limitées. Il est recommandé de désactiver la fonction de restriction des processus d'arrière-plan dans l'Économie d'énergie.
- Aussi, sur certains appareils Samsung, si le mot de passe de déverrouillage n'est pas conforme aux exigences de sécurité de l'entreprise, Kaspersky Endpoint Security for Android n'interdit pas l'utilisation des empreintes digitales pour le déverrouillage de l'écran.
- Sur certains appareils Samsung, après l'exécution des commandes d'Antivol (recherche, verrouillage, le déverrouillage et prise de photos), le certificat commun et le certificat VPN peuvent être supprimés. Pour poursuivre l'utilisation, les certificats devront être réinstallés. Le problème est lié au standard de sécurité MDFPP (Mobile Device Fundamentals Protection Profile).
- Sur certains appareils Honor et Huawei, vous ne pouvez pas restreindre l'utilisation du Bluetooth. Lorsque Kaspersky Endpoint Security for Android tente de restreindre l'utilisation du Bluetooth, le système d'exploitation affiche une notification avec les options suivantes : rejeter ou autoriser. Ainsi, l'utilisateur peut refuser la restriction et continuer à utiliser le Bluetooth.
- Sur certains appareils Samsung, après l'installation ou la mise à jour de Kaspersky Endpoint Security à partir d'un paquet d'installation autonome, l'activation du profil KNOX MDM n'est pas disponible.
- Sur les appareils Blackview, l'utilisateur peut effacer la mémoire de l'application Kaspersky Endpoint Security for Android. Par conséquent, la protection et l'administation des appareils sont désactivées, tous les paramètres définis deviennent inefficaces et l'application Kaspersky Endpoint Security for Android est supprimée des fonctionnalités d'accessibilité. En effet, les appareils de ce fournisseur fournissent à l'application Écrans récents personnalisée des privilèges élevés. Cette application peut remplacer les paramètres de Kaspersky Endpoint Security for Android et ne peut pas être remplacée, car elle fait partie du système d'exploitation Android.
- Sur certains appareils fonctionnant sous Android 11, l'application Kaspersky Endpoint Security for Android se bloque immédiatement après le démarrage. Le problème est lié à un défaut bien connu dans Android 11.

Déploiement

Cette section est destinée au experts spécialisés dans l'installation de Kaspersky Security for Mobile et aux experts qui assurent l'assistance technique dans les organisations qui ont choisi de travailler avec Kaspersky Security for Mobile.

Architecture de la solution

Kaspersky Security for Mobile comprend les modules suivants :

- Application mobile Kaspersky Endpoint Security for Android.

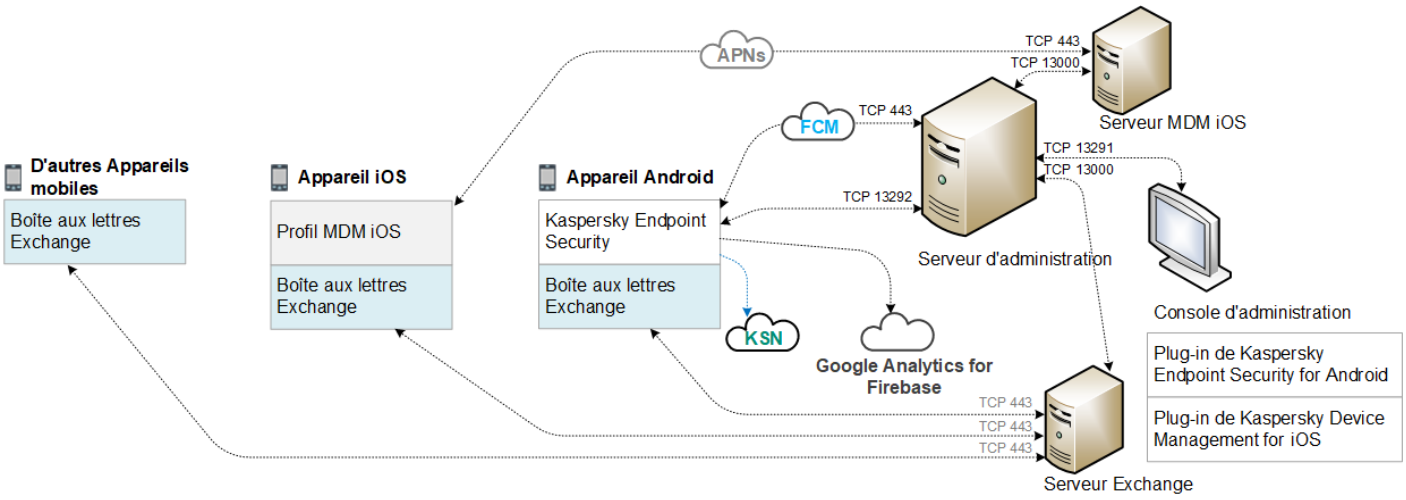
  L'application Kaspersky Endpoint Security for Android assure la protection des appareils mobiles contre les menaces Internet, les virus et autres programmes qui constituent des menaces. Assure l'interaction entre l'appareil mobile et le Serveur d'administration Kaspersky Security Center à l'aide de Firebase Cloud Messaging.
- Plug-in d'administration de Kaspersky Endpoint Security for Android.

Le plug-in d'administration de Kaspersky Endpoint Security for Android assure l'administration par interface des appareils mobiles et de leurs applications via la Console d'administration de Kaspersky Security Center.

- Plug-in d'administration de Kaspersky Device Management for iOS

  Le plug-in d'administration de Kaspersky Device Management for iOS constitue une interface d'administration des appareils mobiles connectés via les protocoles MDM iOS et Exchange ActiveSync sur la Console d'administration de Kaspersky Security Center.

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



Architecture de Kaspersky Security for Mobile

Pour en savoir plus sur la Console d'administration, le Serveur d'administration, le Serveur Exchange et le Serveur MDM iOS, consultez l'*aide de Kaspersky Security Center*.

Schémas types de déploiement de la solution complète

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

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

Schémas de déploiement de Kaspersky Endpoint Security for Android

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

Pour en savoir plus sur le déploiement de Kaspersky Endpoint Security for Android dans Kaspersky Endpoint Security Cloud, consultez l'*aide de Kaspersky Endpoint Security Cloud*.

Schémas de déploiement de Kaspersky Endpoint Security for Android via Kaspersky Security Center

Le déploiement de Kaspersky Endpoint Security for Android via Kaspersky Security Center peut être réalisé selon une des méthodes suivantes :

- Diffusion de messages contenant un lien vers Google Play (recommandé).
- Diffusion de messages contenant un lien vers un paquet d'installation autonome de l'app.

Le déploiement de Kaspersky Endpoint Security for Android via Google Play consiste à envoyer des messages contenant un lien vers Google Play aux utilisateurs des appareils depuis la Console d'administration.

Le déploiement de Kaspersky Endpoint Security for Android via la diffusion d'un paquet autonome correspond à la réalisation des étapes suivantes par l'administrateur :

1. Création du paquet d'installation de l'application.
2. Configuration du paquet d'installation.
3. Création d'un paquet autonome d'installation.
4. Envoi d'un message contenant un lien pour télécharger le paquet autonome d'installation aux utilisateurs d'appareils Android. La diffusion massive est prise en charge.

L'utilisateur installe Kaspersky Endpoint Security for Android sur l'appareil mobile une fois qu'il a reçu le message contenant le lien vers Google Play ou le lien permettant de télécharger le fichier de distribution depuis le serveur Web de Kaspersky Security Center. L'app peut être utilisée directement sans aucune autre préparation.

Schéma de déploiement de Kaspersky Endpoint Security for Android depuis Google Play

Il est recommandé d'appliquer le schéma de déploiement depuis Google Play si l'installation à distance est impossible.

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

Schéma de déploiement de Kaspersky Endpoint Security for Android via KNOX Mobile Enrollment

Le déploiement de Kaspersky Endpoint Security for Android consiste à ajouter un profil MDM KNOX sur les appareils mobiles. Le profil MDM KNOX contient un lien vers l'application installée sur le Serveur Web de Kaspersky Security Center ou un autre serveur. Après l'installation de l'application sur l'appareil mobile, vous devez en plus installer le certificat commun.

Vous pouvez vous renseigner sur l'installation par le biais KNOX Mobile Enrollment dans la section Samsung KNOX section.

Schémas de déploiement du profil iOS MDM

Le *profil iOS MDM* est un profil qui reprend les paramètres de connexion des appareils mobiles iOS à Kaspersky Security Center. Après l'installation d'un profil iOS MDM et la synchronisation avec Kaspersky Security Center, l'appareil devient un appareil contrôlé. L'administration des appareils mobiles s'opère à l'aide d'Apple Push Notification service (APNs). Pour en savoir plus sur l'installation d'un profil MDM iOS et sur l'utilisation des APNs, consultez l'*Aide de Kaspersky Security Center*.

Avec un profil iOS MDM, vous pouvez exécuter les actions suivantes :

- Configuration à distance des paramètres d'un appareil iOS MDM à l'aide de stratégies de groupe.
- Envoi des commandes de verrouillage et de suppression des données.
- Installation à distance d'apps de Kaspersky, ainsi que des applications tierces.

Il existe plusieurs méthodes pour déployer un profil iOS MDM sur des appareils mobiles du réseau de l'organisation. Vous pouvez sélectionner la méthode de déploiement qui convient le mieux à votre organisation, et utiliser plusieurs méthodes de déploiement simultanément.

Avant de déployer un profil iOS MDM, l'administrateur doit réaliser les opérations suivantes :

1. Installer le serveur des appareils mobiles iOS MDM.
2. Obtenir le certificat Apple Push Notification Service (certificat APNs).
3. Installer le certificat APNs sur le Serveur des appareils mobiles iOS MDM.

Pour en savoir plus sur l'installation d'un Serveur des appareils mobiles MDM iOS et sur l'utilisation d'un certificat APNs, consultez *l'Aide de Kaspersky Security Center*.

Pour en savoir plus sur le déploiement d'un profil MDM iOS dans Kaspersky Endpoint Security Cloud, consultez *l'Aide de Kaspersky Endpoint Security Cloud*.

Schémas de déploiement d'un profil iOS MDM via Kaspersky Security Center

Il est possible de déployer un profil iOS MDM via Kaspersky Security Center en envoyant des messages qui contiennent un lien de téléchargement du profil iOS MDM. La diffusion massive est prise en charge.

L'utilisateur installe le profil iOS MDM sur l'appareil mobile après avoir reçu le message contenant le lien vers le Serveur Web de Kaspersky Security Center. Le profil iOS MDM installé de cette manière peut être utilisé directement.

Pour en savoir plus sur la création d'un profil MDM iOS, consultez *l'Aide de Kaspersky Security Center*.

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

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

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

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

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

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

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

2. Choisissez la section **Paramètres de connexion serveur** → **Ports Supplémentaires**.

3. Cochez la case **Ouvrir le port pour les appareils mobiles**.

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

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

5. Dans le champ **Port d'activation des clients mobiles**, indiquez le port par lequel les appareils mobiles se connecteront au serveur d'administration pour l'activation de l'application Kaspersky Endpoint Security for Android. Le port 17100 est le port choisi par défaut.

6. Cliquez sur **OK**.

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

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

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

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

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

3. Cliquez sur **OK**.

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

Création d'un groupe d'administration

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

Pour appliquer une stratégie au groupe d'appareils, il est conseillé de créer un groupe d'administration dédié à ces appareils dans le dossier **Appareils administrés** avant l'installation des applications mobiles sur les appareils des utilisateurs.

Après la création du groupe d'administration, il est recommandé de configurer le placement automatique dans ce groupe des appareils sur lesquels vous voulez installer les apps. Il faut ensuite définir les paramètres communs à l'ensemble des périphériques à l'aide d'une stratégie de groupe.

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

1. Dans l'arborescence de la console, sélectionnez le dossier **Appareils administrés**.
2. Dans l'espace de travail du dossier **Appareils administrés** ou dans un sous-dossier, sélectionnez l'onglet **Appareils**.
3. Cliquez sur le bouton **Créer un groupe**.

   La fenêtre de création d'un nouveau groupe s'ouvrira alors.
4. Dans la fenêtre **Nom du groupe** qui s'ouvre, saisissez le nom du groupe, puis cliquez sur le bouton **OK**.

A l'issue de la procédure, un nouveau dossier du groupe d'administration au nom défini sera affiché dans l'arbre de la console. Pour en savoir plus sur l'utilisation des groupes d'administration, consultez *l'Aide de Kaspersky Security Center*.

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

L'administration centralisée des paramètres de l'application Kaspersky Endpoint Security for Android installées sur les appareils mobiles des utilisateurs n'est possible que si ces appareils se trouvent dans un groupe d'administration déjà créé pour lequel une stratégie de groupe a été définie.

Si la règle du transfert automatique des appareils mobiles détectés sur le réseau vers le groupe d'administration n'est pas définie, l'appareil sera automatiquement placé lors de sa première configuration avec le Serveur d'administration dans la Console d'administration dans le dossier **Avancé** → **Requête réseau** → **Domaines** → **KES10**. La stratégie de groupe n'est pas appliquée à cet appareil.

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

1. Dans l'arborescence de la console, sélectionnez le dossier **Périphériques non définis**.
2. Dans le menu contextuel du dossier **Périphériques non définis**, choisissez l'option **Propriétés**.

   La fenêtre **Propriétés : Périphériques non définis** s'ouvre.
3. Dans la section **Déplacement d'appareils**, cliquez sur le bouton **Ajouter** pour lancer la procédure de création des règles de déplacement automatique des appareils vers le groupe d'administration.

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

4. Spécifiez le nom de la règle.

5. Indiquez le groupe d'administration dans lequel il faut placer les appareils après l'installation sur ceux-ci de l'application Kaspersky Endpoint Security for Android. Pour ce faire, cliquez sur le bouton **Parcourir** qui se trouve à droite du champ **Groupe destiné au déplacement d'appareils** et sélectionnez le groupe dans la fenêtre qui s'ouvre.

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

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

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

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

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

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

10. Cliquez sur **OK**.

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

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

Création d'un certificat commun

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

Pour créer un certificat commun, procédez comme suit :

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

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

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

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

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

   - Pour créer un certificat commun automatiquement à l'aide des outils du Serveur d'administration, sélectionnez l'option **Délivrer le certificat à l'aide des outils du Serveur d'administration**.

- Pour indiquer à l'utilisateur le certificat créé précédemment, sélectionnez l'option **Indiquer le fichier du certificat**. Cliquez sur le bouton **Indiquer** pour ouvrir la fenêtre **Certificat** et y indiquer le fichier du certificat.

  Décochez la case **Publier le certificat** si vous ne souhaitez pas indiquer le type d'appareil mobile et le mode de notification de l'utilisateur concernant la création du certificat.

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

7. Dans la fenêtre **Génération du certificat** de l'assistant, cliquez sur le bouton **Prêt** pour fermer l'assistant d'installation de certificats.

Au terme de l'exécution de l'assistant d'installation de certificats, un certificat commun sera créé et pourra être installé par un utilisateur sur un périphérique mobile. Afin d'obtenir un certificat, il est nécessaire de lancer la synchronisation du périphérique mobile avec le Serveur d'administration. Pour en savoir plus sur la création des certificats et la configuration des règles de leur exécution, consultez *l'Aide de Kaspersky Security Center*.

Installation de Kaspersky Endpoint Security for Android

Cette section décrit les méthodes de déploiement de Kaspersky Endpoint Security for Android sur le réseau d'une organisation.

Autorisations

Pour toutes les fonctions des applications, Kaspersky Endpoint Security for Android demande à l'utilisateur les autorisations indispensables. Kaspersky Endpoint Security for Android demande les autorisations obligatoires pendant l'exécution de l'Assistant d'installation, ainsi qu'après l'installation avant l'utilisation des fonctions distinctes des applications. Sans octroi des autorisations obligatoires, il est impossible d'installer Kaspersky Endpoint Security for Android.

Sur certains appareils (par exemple, Huawei, Meizu, Xiaomi) il faut ajouter manuellement Kaspersky Endpoint Security for Android à la liste des applications lancées au chargement du système d'exploitation dans les paramètres de l'appareil. Si l'application n'est pas ajoutée à la liste, Kaspersky Endpoint Security for Android cesse d'exécuter toutes les fonctions après le redémarrage de l'appareil mobile.

Sur les appareils exécutant Android 11 ou version ultérieure, vous devez désactiver le paramètre système **Supprimer les autorisations si l'application n'est pas utilisée**. Sinon, après quelques mois d'inutilisation de l'application, le système réinitialise automatiquement les autorisations que l'utilisateur a accordées à l'application.

Le Filtre des appels et SMS et la Surveillance SIM ne sont plus pris en charge dans Kaspersky Endpoint Security for Android Service Pack 4 Update 4 (version 10.8.0.103). Dans ce cas, Kaspersky Endpoint Security for Android ne demande pas à l'utilisateur l'autorisation de l'Administration SMS. Pour que le Filtre des appels et SMS et que toutes les fonctions de la Surveillance SIM fonctionnent, utilisez les versions antérieures de Kaspersky Endpoint Security for Android.

Autorisations demandées par Kaspersky Endpoint Security for Android

Autorisation	Fonction de l'application
Téléphone (obligatoire uniquement pour Android 5.0 à 9.X)	Connexion à Kaspersky Security Center (identifiant de l'appareil)
Stockage (obligatoire)	Anti-Virus
Accès pour gérer tous les fichiers	Antivirus (seulement pour Android 11 et version ultérieure)
Administrateur de l'appareil (obligatoire)	Antivol : verrouillage de l'appareil (seulement pour Android 5.0 à 6.X)
	Antivol – prendre une photo avec la caméra avant
	Antivol – reproduction de l'alarme
	Antivol – rétablissement des paramètres par défaut
	Protection par mot de passe
	Protection contre la suppression de l'application
	Installation des certificats de sécurité
	Contrôle des applications installées
	Administration KNOX (seulement pour les appareils Samsung)
	Configuration Wi-Fi
	Configuration Exchange ActiveSync
	Restriction de l'utilisation de la caméra, Bluetooth, Wi-Fi
Appareil photo	Antivol – prendre une photo avec la caméra avant Sur les appareils tournant sous Android 11.0 ou une version ultérieure, l'utilisateur doit accorder la permission "Pendant l'utilisation de l'application" lorsqu'il y est invité.
Localisation	Antivol – définition de l'emplacement de l'appareil Sur les appareils tournant sous Android 10.0 ou une version ultérieure, l'utilisateur doit accorder l'autorisation "Tout le temps" lorsqu'il y est invité
Fonctionnalités d'accessibilité	Antivol – verrouillage de l'appareil (seulement pour Android 7.0 et version ultérieure)
	Protection Internet
	Contrôle des applications installées
	Protection de la suppression de l'application (seulement pour Android 7.0 et version ultérieure)
	Affichage des avertissements de Kaspersky Endpoint Security for Android (seulement Android 10.0 et version ultérieure)
	Restreindre l'utilisation de l'appareil photo (uniquement pour Android 11 ou version ultérieure)

Installation de Kaspersky Endpoint Security for Android à l'aide d'un lien Google Play

L'installation de Kaspersky Endpoint Security for Android a lieu sur les appareils mobiles des utilisateurs dont le compte a été ajouté à Kaspersky Security Center. Pour en savoir plus sur l'utilisation des comptes utilisateurs dans Kaspersky Security Center, consultez l'Aide de Kaspersky Security Center.

Kaspersky Security for Mobile permet d'installer l'application via Kaspersky Security Center via un lien Google Play (méthode recommandée).

L'utilisateur reçoit un lien vers Google Play. L'installation s'effectue selon la méthode classique sur la plateforme Android. Il n'est pas nécessaire de réaliser une configuration complémentaire de Kaspersky Endpoint Security for Android après l'installation.

Certains appareils Huawei et Honor qui ne disposent pas des services Google et donc d'un accès aux applications de Google Play. Si certains utilisateurs d'appareils Huawei et Honor ne peuvent pas installer l'application à partir de Google Play, il faut leur demander d'installer l'application à partir de Huawei App Gallery.

Le lien contient les données suivantes :

- Paramètres de synchronisation de Kaspersky Security Center.
- Certificat commun.
- Indicateur d'acceptation des Conditions générales du Contrat de licence utilisateur final et des Dispositions supplémentaires pour Kaspersky Endpoint Security for Android. Si l'administrateur accepte les dispositions du Contrat et des Dispositions supplémentaires dans la Console d'administration, Kaspersky Endpoint Security for Android ignore l'étape d'acceptation lors de l'installation de l'application.

Pour installer Kaspersky Endpoint Security for Android via Kaspersky Security Center à l'aide d'un lien Google Play :

1. Dans l'arborescence de la console, sélectionnez le dossier **Administration des appareils mobiles → Appareils mobiles**.
2. Dans l'espace de travail du dossier **Appareils mobiles**, cliquez sur le bouton **Ajouter un appareil mobile**.

   L'Assistant de connexion d'un nouvel appareil mobile démarre. Il faut suivre ses indications.
3. Dans la fenêtre **Système d'exploitation** de l'Assistant, choisissez **Android**.

   Kaspersky Security Center vérifie les mises à jour des plug-ins d'administration. Si Kaspersky Security Center détecte des mises à jour, vous pouvez installer la nouvelle version du plug-in d'administration. Une fois que le plug-in d'administration a été mis à jour, vous pouvez accepter les conditions générales du Contrat de licence utilisateur final (CLUF) et des Dispositions supplémentaires pour Kaspersky Endpoint Security for Android. Si l'administrateur accepte le Contrat de licence utilisateur final et les Dispositions supplémentaires dans la Console d'administration, Kaspersky Endpoint Security for Android ignore l'étape d'acceptation lors de l'installation de l'application. Cette fonction est disponible dans Kaspersky Security Center version 12.
4. Sur la page de la **Méthode d'installation de Kaspersky Endpoint Security for Android**, sélectionnez la méthode d'installation de l'application **En utilisant un lien Google Play**.
5. Sur la page **Sélection des utilisateurs** de l'Assistant, sélectionnez un ou plusieurs utilisateurs en vue de l'installation de Kaspersky Endpoint Security for Android sur leurs appareils.

Si un utilisateur ne figure pas dans la liste, vous pouvez ajouter un nouveau compte utilisateur sans quitter l'Assistant d'ajout de nouvel appareil mobile.

6. Sur la page **Source du certificat** de l'Assistant, choisissez la source du certificat pour la protection des échanges de données entre Kaspersky Endpoint Security for Android et Kaspersky Security Center :

   - **Délivrer le certificat à l'aide des outils du Serveur d'administration.** Dans ce cas, le certificat est ajouté automatiquement.

   - **Indiquer le fichier du certificat**. Dans ce cas, il convient préalablement de préparer un certificat dédié et de le sélectionner dans la fenêtre de l'Assistant. Cette option ne peut être choisie si vous souhaitez installer Kaspersky Endpoint Security for Android sur plusieurs appareils mobiles. Il convient de créer un certificat distinct pour chaque utilisateur.

7. Sur la page **Mode de notification des utilisateurs** de l'Assistant, choisissez le canal à utiliser pour transmettre le lien d'installation de l'application :

   - Pour envoyer le lien par email, choisissez **Envoyer le lien vers Kaspersky Endpoint Security** et configurez les paramètres dans le groupe **Par email**. Confirmez que l'adresse email est reprise dans les paramètres des comptes des utilisateurs.

   - Pour envoyer le lien via un message SMS, choisissez **Envoyer le lien vers Kaspersky Endpoint Security** et configurez les paramètres dans le groupe **Via SMS**. Confirmez que le numéro de téléphone est repris dans les paramètres des comptes des utilisateurs.

   - Pour installer Kaspersky Endpoint Security for Android à l'aide d'un QR code, choisissez **Afficher le lien vers le paquet d'installation** et lisez le QR code à l'aide de l'appareil photo de l'appareil mobile.

   - Si aucune des méthodes proposées ne vous convient, choisissez l'option **Afficher le lien vers le paquet d'installation** → **Copier** afin de copier le lien d'installation de Kaspersky Endpoint Security for Android dans le Presse-papiers. Envoyez le lien d'installation de l'app à l'aide de n'importe quelle méthode disponible. Vous pouvez également utiliser d'autres méthodes d'installation de Kaspersky Endpoint Security for Android.

8. Cliquez sur **Terminer** pour quitter l'Assistant de connexion d'un nouvel appareil mobile.

Après que Kaspersky Endpoint Security for Android a été installé sur les appareils mobiles des utilisateurs, vous pouvez configurer les paramètres des appareils et des applications à l'aide de stratégies de groupe. Vous pouvez également envoyer des commandes aux appareils mobiles pour protéger les données en cas de perte ou de vol des appareils.

Autres méthodes d'installation de Kaspersky Endpoint Security for Android

Vous pouvez installer Kaspersky Endpoint Security for Android à l'aide d'un lien vers votre propre serveur Internet ou demander aux utilisateurs d'installer l'application manuellement.

Installation manuelle à partir de Google Play ou Huawei AppGallery

Les utilisateurs peuvent installer manuellement Kaspersky Endpoint Security for Android depuis Google Play ou Huawei AppGallery. L'installation s'effectue selon la méthode classique pour la plate-forme Android. L'utilisateur utilise son propre compte Google pour installer l'application.

Pour en savoir plus sur la procédure d'installation de Kaspersky Endpoint Security for Android à partir de Google Play, consultez le site du support technique de Google.

Pour en savoir plus sur la procédure d'installation de Kaspersky Endpoint Security for Android à partir de Huawei AppGallery, consultez le site du support technique de HUAWEI.

Certains appareils Huawei et Honor qui ne disposent pas des services Google et donc d'un accès aux applications de Google Play. Si certains utilisateurs d'appareils Huawei et Honor ne peuvent pas installer l'application à partir de Google Play, il faut leur demander d'installer l'application à partir de Huawei App Gallery.

Après l'installation de Kaspersky Endpoint Security for Android depuis Google Play ou Huawei AppGallery, il faut préparer l'app en vue de son utilisation. La préparation de l'application comprend les étapes suivantes :

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

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

3. L'administrateur crée un certificat commun pour l'utilisateur de l'appareil mobile.

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

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

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

Au terme de la synchronisation suivante de l'appareil mobile avec le Serveur d'administration, l'appareil mobile sur lequel Kaspersky Endpoint Security for Android est installé est placé dans le dossier **Avancé** → **Requête réseau** → **Domaines** dans le groupe d'administration indiqué lors de l'installation de l'application (par défaut, il s'agit du groupe **KES10**). Vous pouvez déplacer l'appareil mobile dans le dossier Appareils administrés du groupe d'administration que vous avez créé manuellement ou à l'aide des règles de transfert automatique.

Cette méthode d'installation est pratique si vous souhaitez installer une version particulière de Kaspersky Endpoint Security for Android.

Pour installer Kaspersky Endpoint Security for Android via un lien vers un serveur dédié, procédez comme suit :

1. Créez un package d'installation et configurez ses paramètres.

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

2. Créez un paquet d'installation autonome.

   Un *paquet autonome d'installation* est un fichier d'installation de l'application mobile contenant les paramètres de connexion de l'application au Serveur d'administration et un indicateur d'acceptation des Conditions générales du Contrat de licence utilisateur final (CLUF) pour l'application Kaspersky Endpoint Security for Android. Il est créé au départ du paquet d'installation pour Kaspersky Endpoint Security for Android. Le paquet autonome d'installation constitue un cas particulier de paquet d'applications mobiles.

L'utilisateur reçoit un lien vers un serveur Web qui héberge le paquet d'installation autonome de Kaspersky Endpoint Security for Android. Pour installer l'app, l'utilisateur doit lancer le fichier apk. Il n'est pas nécessaire de réaliser une configuration complémentaire de Kaspersky Endpoint Security for Android après l'installation.

L'installation de Kaspersky Endpoint Security for Android sur l'appareil mobile de l'utilisateur à l'aide d'un lien vers un serveur dédié requiert l'autorisation de l'installation d'apps depuis des sources inconnues.

Création et configuration d'un paquet d'installation

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

- `adb.exe`, `AdbWinApi.dll`, `AdbWinUsbApi.dll` — ensemble des fichiers nécessaires à l'installation de Kaspersky Endpoint Security for Android.
- `installer.ini` — fichier de configuration contenant les paramètres de connexion du Serveur d'administration.
- `KES10_xx_xx_xxx.apk` — fichier d'installation de Kaspersky Endpoint Security for Android.
- `kmlisten.exe` — utilitaire de distribution du paquet d'installation de l'application via le poste de travail.
- `kmlisten.ini` — fichier de configuration contenant les paramètres de l'utilitaire de distribution du paquet d'installation.
- `kmlisten.kpd` — fichier de description de l'application.

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

1. Dans l'arborescence de la console choisissez le dossier **Avancé → Installation à distance → Paquets d'installation**.
2. Dans l'espace de travail du dossier **Paquets d'installation**, cliquez sur le bouton **Créer un paquet d'installation**.

   L'Assistant de création du paquet d'installation se lance. Il faut suivre ses indications.
3. Dans la fenêtre de l'assistant, **Sélection du type de paquet d'installation**, appuyez sur le bouton **Créer le paquet d'installation pour l'application Kaspersky**.
4. Dans la fenêtre **Définition du nom du paquet d'installation** de l'assistant, saisissez le nom du paquet d'installation, avec lequel il s'affichera dans l'espace de travail du dossier **Paquets d'installation**.
5. Dans la fenêtre **Sélection du paquet d'installation de l'application à installer**, sélectionnez l'archive auto-extractible `sc_package.exe` incluse dans le kit de distribution.

   Si l'archive a été décompressée auparavant, vous pouvez sélectionner un fichier faisant partie de l'archive avec la description de l'application `kmlisten.kpd`. Le nom de l'application ainsi que le numéro de la version vont apparaitre dans le champ de saisie.
6. Dans la fenêtre **Accepter le CLUF** de l'assistant, lisez, assimilez et acceptez les termes et conditions du Contrat de licence utilisateur final.

   Vous devez accepter les termes et conditions du Contrat de licence utilisateur final pour créer le paquet d'installation. Si vous acceptez les dispositions du Contrat de licence dans la Console d'administration, Kaspersky Endpoint Security for Android ignore l'étape d'acceptation lors de l'installation de l'application.

   Si vous décidez d'arrêter la protection des appareils mobiles, vous pouvez désinstaller l'application Kaspersky Endpoint Security for Android et révoquer votre Contrat de licence utilisateur final (CLUF) pour celle-ci. Pour en savoir plus sur la révocation du CLUF, consultez *l'aide de Kaspersky Security Center*.

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

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

1. Dans l'arborescence de la console choisissez le dossier **Avancé → Installation à distance → Paquets d'installation**.

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

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

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

     Selon le format du nom du Serveur d'administration pour le module **Prise en charge des périphériques mobiles,** indiquez le nom DNS ou l'adresse IP du Serveur d'administration. Dans le champ **Numéro du port SSL**, indiquez le numéro du port qui est ouvert sur le Serveur d'administration pour connecter les appareils mobiles. Le port 13292 est le port choisi par défaut.

   - Dans le groupe **Répartition des ordinateurs selon les groupes** dans le champ **Nom du groupe**, saisissez le nom du groupe où les appareils mobiles seront ajoutés après la première synchronisation avec le Serveur d'administration (par défaut **KES10**).

     Le groupe indiqué sera automatiquement créé dans le dossier **Avancé → Requête réseau → Domaines**.

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

     L'adresse e-mail de l'utilisateur est utilisée pour créer le nom des périphériques mobiles lorsqu'ils sont ajoutés à un groupe d'administration.

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

Création d'un paquet autonome d'installation

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

1. Dans l'arborescence de la console choisissez le dossier **Avancé → Installation à distance → Paquets d'installation**.

2. Spécifiez le paquet d'installation pour l'application Kaspersky Endpoint Security for Android.

3. Dans le menu contextuel du paquet d'installation, choisissez **Créer un paquet autonome d'installation**.

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

4. Configurez les méthodes de diffusion du paquet autonome :

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

message électronique.

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

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

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

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

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

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

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

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

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

Configuration des paramètres de la synchronisation

Pour l'administration des appareils mobiles et la réception des rapports ou des statistiques des appareils mobiles des utilisateurs, vous devez configurer les paramètres de synchronisation. La synchronisation de l'appareil mobile avec Kaspersky Security Center peut être exécutée par les moyens suivants :

- **Planification**. La synchronisation est exécutée d'après l'horaire planifié à l'aide du protocole HTTP. Vous pouvez configurer l'horaire de la synchronisation dans les paramètres de la stratégie de groupe. Les modifications des paramètres de la stratégie de groupe, les commandes et les tâches seront exécutées pendant la synchronisation de l'appareil avec Kaspersky Security Center d'après l'horaire, à savoir avec du retard. Par défaut, les appareils mobiles se synchronisent automatiquement avec Kaspersky Security Center toutes les six heures.

  Sur Android 12 ou une version ultérieure, l'application peut effectuer cette tâche plus tard que prévu si l'appareil est en mode d'économie de la batterie.

- **Forcée**. La synchronisation forcée est exécutée à l'aide des notifications push du service FCM (Firebase Cloud Messaging). La synchronisation forcée, en premier lieu, est destinée à l'envoi opportun des commandes à l'appareil mobile. Si vous voulez utiliser la synchronisation forcée, assurez-vous que les paramètres GSM dans Kaspersky Security Center sont configurés. Pour en savoir plus, consultez l'Aide de Kaspersky Security Center.

Pour configurer les paramètres de synchronisation des appareils mobiles avec Kaspersky Security Center, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Synchronisation**.
5. Sélectionnez la fréquence de lancement de la synchronisation dans la liste déroulante **Lancer la synchronisation**.
6. Pour interdire la synchronisation de l'appareil avec Kaspersky Security Center en itinérance, cochez la case **Désactiver la synchronisation en itinérance**.

   L'utilisateur de l'appareil peut exécuter la synchronisation manuellement dans les paramètres de l'application (→ **Paramètres** → **Synchronisation** → **Synchroniser**).
7. Pour masquer à l'utilisateur les paramètres de synchronisation (adresse du serveur, port et groupe d'administration) dans les paramètres de l'application, décochez la case **Afficher les paramètres de synchronisation sur l'appareil**. Il est impossible de modifier les paramètres masqués.
8. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center. Vous pouvez forcer la synchronisation de l'appareil mobile à l'aide d'une commande spéciale. Pour en savoir plus sur l'utilisation des commandes pour les appareils mobiles, consultez *l'aide de Kaspersky Security Center*.

Activation de l'application Kaspersky Endpoint Security for Android

Dans Kaspersky Security Center, la licence peut couvrir différents groupes fonctionnels. Pour être sûr que l'application Kaspersky Endpoint Security for Android est entièrement fonctionnelle, la licence Kaspersky Security Center achetée par l'organisation doit couvrir la fonction **Administration des appareils mobiles**. La fonction **Gestion des appareils mobiles** permet de connecter des appareils mobiles à Kaspersky Security Center et de les gérer.

Pour en savoir plus sur la licence de Kaspersky Security Center et les options de la licence, consultez *l'aide de Kaspersky Security Center*.

L'activation de l'application Kaspersky Endpoint Security for Android sur un appareil mobile s'effectue en fournissant des informations de licence valides à l'application. Les informations sur la licence sont transmises à l'appareil mobile avec la stratégie lors de la synchronisation de l'appareil avec Kaspersky Security Center.

Si Kaspersky Endpoint Security for Android n'est pas activé dans les 30 jours qui suivent l'installation sur l'appareil mobile, l'application passe automatiquement en mode limité. Dans ce mode de fonctionnement, la majorité des composants de l'app est inopérationnelle. Lorsque l'application passe en mode limité, elle ne réalise plus la synchronisation automatique avec Kaspersky Security Center. Dès lors, si l'application n'est pas activée pour une raison quelconque dans les 30 jours qui suivent l'installation, l'utilisateur doit synchroniser l'appareil avec Kaspersky Security Center manuellement.

Si Kaspersky Security Center n'est pas déployé dans votre organisation ou s'il n'est pas accessible aux appareils mobiles, les utilisateurs peuvent activer manuellement l'application Kaspersky Endpoint Security for Android sur leurs appareils.

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

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Licence**.
5. 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 de 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.
6. Cochez la case **Activer à l'aide d'une clé provenant du stockage de Kaspersky Security Center**.

   Si l'app a été activée sans clé du stockage de Kaspersky Security Center, Kaspersky Security for Mobile remplace cette clé par la clé d'activation sélectionnée dans la liste **Clé** qui s'affiche.
7. Afin d'activer l'application sur le périphérique mobile de l'utilisateur, verrouillez la modification des paramètres.
8. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

   Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Installation d'un profil iOS MDM

Cette section décrit les différentes méthodes de déploiement de profils IOS MDM sur le réseau de l'organisation.

Avant de déployer un profil iOS MDM, l'administrateur doit réaliser les opérations suivantes :

1. Installer le serveur des appareils mobiles iOS MDM.
2. Obtenir le certificat Apple Push Notification Service (certificat APNs).
3. Installer le certificat APNs sur le Serveur des appareils mobiles iOS MDM.

Pour en savoir plus sur l'installation d'un Serveur des appareils mobiles MDM iOS et sur l'utilisation d'un certificat APNs, consultez *l'Aide de Kaspersky Security Center*.

Pour en savoir plus sur le déploiement d'un profil MDM iOS dans Kaspersky Endpoint Security Cloud, consultez *l'Aide de Kaspersky Endpoint Security Cloud*.

A propos des modes de gestion des appareils iOS

Le déploiement du système de gestion des appareils iOS peut être exécuté par plusieurs moyens. Le mode de gestion dépend du propriétaire de l'appareil mobile (personnel ou professionnel) et des exigences de sécurité de l'entreprise. Vous pouvez choisir le mode de gestion plus adapté aux entreprise et utiliser plusieurs modes simultanément.

Appareils incontrôlés

Les appareils iOS incontrôlés sont les appareils personnels des collaborateurs connectés à Kaspersky Security Center. Dans ce mode, l'utilisateur est autorisé à utiliser son identifiant Apple personnel, à utiliser n'importe quelles applications et à conserver des données personnelles sur l'appareil. Vous pouvez configurer l'accès aux ressources de l'entreprise, les paramètres de sécurité et d'autres paramètres à l'aide de la stratégie de groupe Kaspersky Device Management for iOS. Par défaut, tous les appareils iOS sont incontrôlés.

Appareils contrôlés

Les appareils iOS contrôlés sont les appareils professionnels connectés à Kaspersky Security Center. La configuration initiale de l'appareil mobile est exécutée dans Apple Configurator. *Apple Configurator* est l'application de la préparation et de configuration des appareils iOS. Apple Configurator s'installe sur un ordinateur tournant sous OS X. Pour en savoir plus sur le fonctionnement d'Apple Configurator, consultez le site Internet de l'assistance technique d'Apple. La modification ultérieure des paramètres est accessible à l'aide de la stratégie de groupe Kaspersky Device Management for iOS. Sur les appareils contrôlés un ensemble avancé de paramètres est accessible : Proxy HTTP global, restrictions supplémentaires (par exemple, l'interdiction d'utiliser iMessage, Game Center) ou l'interdiction de modifier le compte utilisateur.

Pour utiliser les appareils iOS contrôlés et incontrôlés, le certificat APNs doit être installé sur le Serveur MDM iOS, et le profil MDM iOS sur les appareils mobiles des utilisateurs.

Installation via Kaspersky Security Center

L'installation du profil iOS MDM a lieu sur les appareils mobiles des utilisateurs dont le compte a été ajouté à Kaspersky Security Center. Pour en savoir plus sur l'utilisation des comptes utilisateurs dans Kaspersky Security Center, consultez *l'Aide de Kaspersky Security Center*.

Pour installer un profil iOS MDM, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Administration des appareils mobiles → Appareils mobiles**.
2. Dans l'espace de travail du dossier **Appareils mobiles**, cliquez sur le bouton **Ajouter un appareil mobile**.

   L'Assistant de connexion d'un nouvel appareil mobile démarre. Il faut suivre ses indications.
3. Dans la fenêtre **Système d'exploitation** de l'Assistant, choisissez **iOS**.
4. Dans la fenêtre **Méthode de protection de l'appareil iOS MDM**, choisissez **Utiliser le profil iOS MDM du Serveur des appareils mobiles iOS MDM** et choisissez un profil iOS MDM dans la liste.

5. Dans la fenêtre **Sélection des utilisateurs** de l'Assistant, sélectionnez un ou plusieurs utilisateurs en vue de l'installation d'un profil iOS MDM sur leurs appareils.

   Si l'utilisateur ne figure pas dans la liste, vous pouvez ajouter un nouveau compte utilisateur sans quitter l'Assistant d'ajout de nouvel appareil mobile.

6. Dans la fenêtre **Source du certificat** de l'Assistant, choisissez la source du certificat pour la protection des échanges de données entre l'appareil mobile et Kaspersky Security Center :

   - **Délivrer le certificat à l'aide des outils du Serveur d'administration**. Dans ce cas, le certificat est ajouté automatiquement.

   - **Indiquer le fichier du certificat**. Dans ce cas, il convient préalablement de préparer un certificat dédié et de le sélectionner dans la fenêtre de l'Assistant. Cette option ne peut être choisie si vous souhaitez installer un profil iOS MDM sur plusieurs appareils mobiles. Il convient de créer un certificat distinct pour chaque utilisateur.

7. Dans la fenêtre **Mode de notification des utilisateurs** de l'Assistant, choisissez le canal à utiliser pour transmettre le lien d'installation de l'app :

   - Pour envoyer le lien par email, choisissez **Envoyer le lien vers le profil iOS MDM** et configurez les paramètres dans le groupe **Par email**. Confirmez que l'adresse email est reprise dans les paramètres des comptes des utilisateurs.

   - Pour envoyer le lien via un message SMS, choisissez **Envoyer le lien vers profil iOS MDM** et configurez les paramètres dans le groupe **Via SMS**. Confirmez que le numéro de téléphone est repris dans les paramètres des comptes des utilisateurs.

   - Pour installer un profil iOS MDM à l'aide d'un QR code, choisissez **Afficher le lien vers le paquet d'installation** et lisez le QR code à l'aide de l'appareil photo de l'appareil mobile.

   - Si aucune des méthodes proposées ne vous convient, choisissez l'option **Afficher le lien vers le paquet d'installation** → **Copier** afin de copier le lien d'installation du profil iOS MDM dans le Presse-papiers. Envoyez le lien d'installation de l'app à l'aide de n'importe quelle méthode disponible.

8. Quittez l'Assistant de connexion d'un nouvel appareil mobile.

Après que le profil iOS MDM a été installé sur les appareils mobiles des utilisateurs, vous pouvez configurer les paramètres des apps à l'aide de stratégies de groupe. Vous pouvez également envoyer des commandes aux appareils mobiles pour protéger les données en cas de perte ou de vol des appareils.

Sur les appareils mobiles tournant sous iOS 12.1 et supérieure, vous devez confirmer manuellement l'installation du profil MDM iOS sur l'appareil mobile. Vous devez accorder l'autorisation d'administration à distance de l'appareil.

Installation des plug-ins d'administration

Pour administrer les appareils mobiles sur le poste de travail de l'administrateur, il faut installer les plug-ins d'administration suivants :

- Le plug-in d'administration de Kaspersky Endpoint Security for Android 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 Device Management for iOS constitue une interface d'administration des appareils mobiles connectés via les protocoles MDM iOS et Exchange ActiveSync sur la Console d'administration de Kaspersky Security Center.

Vous pouvez installer des plug-ins d'administration à l'aide des méthodes suivantes :

- Installez un plug-in d'administration à l'aide de l'Assistant de démarrage rapide de Kaspersky Security Center.

  L'application vous invite automatiquement à exécuter l'Assistant de démarrage rapide une fois le Serveur d'administration installé et lorsque vous vous connectez à celui-ci pour la première fois. Vous pouvez également lancer l'Assistant de démarrage rapide manuellement à tout moment.

  > L'Assistant de démarrage rapide vous permet d'accepter les Conditions générales du Contrat de licence utilisateur final (CLUF) pour l'application Kaspersky Endpoint Security for Android dans la Console d'administration. Si l'administrateur accepte les conditions du Contrat de licence dans la Console d'administration, Kaspersky Endpoint Security for Android ignore l'étape d'acceptation lors de l'installation de l'application. Pour plus d'informations sur l'Assistant de démarrage rapide pour Kaspersky Security Center, veuillez consulter *l'Aide de Kaspersky Security Center*.

- Installez le plug-in d'administration en utilisant la liste des paquets de distribution disponibles dans la Console d'administration de Kaspersky Security Center.

  La liste des paquets de distribution disponibles est mise à jour automatiquement après la sortie des nouvelles versions des applications Kaspersky.

- Téléchargez le paquet de distribution à partir d'une source externe et installez le plug-in d'administration à l'aide du fichier EXE.

  Le paquet de distribution du plug-in d'administration peut par exemple être téléchargé sur le site de Kaspersky.

Installation des plug-ins d'administration à partir de la liste dans la Console d'administration

Pour installer les plug-ins d'administration, procédez comme suit :

1. Dans l'arborescence de la console, choisissez le dossier **Avancé** → **Installation à distance** → **Paquets d'installation**.
2. Dans l'espace de travail, sélectionnez **Actions supplémentaires** → **Afficher les versions actuelles des applications Kaspersky**.

   Cette opération ouvre la liste des versions mises à jour des applications Kaspersky.
3. Dans la section **Appareils mobiles**, sélectionnez le plug-in **Kaspersky Endpoint Security for Android** ou **Kaspersky Device Management for iOS**.
4. Cliquez sur le bouton **Télécharger les paquets de distribution**.

   Une distribution de plug-in sera téléchargée dans la mémoire de l'ordinateur (fichier EXE).
5. Exécutez le fichier EXE et suivez les instructions de l'Assistant d'installation.

Installation des plug-ins d'administration à partir du paquet de distribution

Pour installer le plug-in d'administration de Kaspersky Endpoint Security for Android,

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

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

Pour installer le plug-in d'administration de Kaspersky Device Management for iOS,

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

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

Vous pouvez confirmer l'installation des plug-ins d'administration en consultant la liste des plug-ins d'administration d'applications installés dans la fenêtre des propriétés du Serveur d'administration, accessible dans la section **Avancé → Informations concernant les plug-ins d'administration d'applications installés**.

Mise à jour de la version précédente de l'application

Il faut réaliser la mise à jour de l'application en tenant compte des exigences suivantes :

- La version du plug-in d'administration de Kaspersky Endpoint Security et celle de l'app mobile Kaspersky Endpoint Security for Android doivent correspondre.

  Le numéro de version du plug-in d'administration et de l'app mobile est repris dans les notes de version de Kaspersky Security for Mobile.

- Confirmez que Kaspersky Security Center satisfait à la configuration logicielle de Kaspersky Security for Mobile.

- La mise à jour automatique des plug-ins d'administration de Kaspersky Endpoint Security 10.0 Service Pack 2 (version 10.6.0.1801) et de Kaspersky Device Management for iOS 10.0 Service Pack 2 (version 10.6.0.1767) et suivantes est possible. La mise à jour des plug-ins d'administration des versions plus anciennes n'est pas prise en charge.

  Pour la mise à jour des plug-ins d'administration des versions plus anciennes, il faut tout d'abord supprimer les plug-ins d'administration installés et les stratégies de groupe créées à l'aide de ceux-ci. Ensuite, installez les nouvelles versions des plug-ins d'administration. Pour en savoir plus sur la suppression des plug-ins d'administration, consultez le *site Internet du Support Technique de Kaspersky*.

- Utilisez la même version de Kaspersky Endpoint Security for Android sur tous les appareils mobiles de l'organisation.

Pour connaître les délais et les conditions d'intervention de l'assistance technique pour les différentes versions de Kaspersky Security for Mobile, consultez le *site Internet du Support Technique de Kaspersky*.

Pour afficher la version et le numéro des plug-ins d'administration, procédez comme suit :

1. Dans le menu contextuel Serveur d'administration dans l'arborescence de la console, choisissez l'option **Propriétés**.
2. Dans la fenêtre de propriétés du Serveur d'administration, sélectionnez **Avancé → Détails des plug-ins d'administration des applications installés**.

L'espace de travail affiche les informations relatives aux plug-ins d'administration installés selon le format `<Nom du plug-in> <Version> <Numéro de version>`.

Vous pouvez obtenir la version et le numéro de l'app Kaspersky Endpoint Security for Android selon une des méthodes suivantes :

- Si Kaspersky Endpoint Security for Android a été installé à l'aide d'un paquet d'installation autonome, vous pouvez consulter la version et le numéro dans les propriétés du paquet.
- Si Kaspersky Endpoint Security for Android a été installé via Google Play, vous pouvez consulter le numéro de version dans les paramètres de l'app (→ **Infos sur l'application**).

Mise à jour de la version antérieure de Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android peut être mis à jour selon une des méthodes suivantes :

- A l'aide de Google Play. L'utilisateur du périphérique mobile télécharge la nouvelle version de l'application depuis Google Play et l'installe sur son périphérique.
- A l'aide de Kaspersky Security Center. Vous mettez à jour à distance la version de l'application sur le périphérique à l'aide du système d'administration à distance Kaspersky Security Center.

Vous pouvez choisir la méthode de mise à jour de l'app la mieux adaptée à votre organisation. Vous pouvez utiliser un seul mode de mise à jour.

Mise à jour à l'aide de Google Play

La mise à jour à l'aide de Google Play s'effectue par un moyen classique compatible avec la plateforme Android. Pour la mise à jour de l'application, les conditions suivantes doivent être remplies :

- L'utilisateur de l'appareil mobile doit disposer d'un compte Google.
- Le périphérique doit être associé au compte Google.
- L'appareil doit disposer d'une connexion à Internet.

Après avoir téléchargé l'application sur Google Play, Kaspersky Endpoint Security for Android vérifie les Conditions générales du Contrat de licence utilisateur final (CLUF). Si les conditions du CLUF sont mises à jour, l'application envoie une demande à Kaspersky Security Center. Si l'administrateur accepte le CLUF dans la Console d'administration, Kaspersky Endpoint Security for Android ignore l'étape d'acceptation lors de l'installation de l'application. Si l'administrateur utilise une version dépassée du plug-in d'administration, Kaspersky Security Center vous demande de mettre à jour ce plug-in. Lors de la mise à jour du plug-in d'administration, un administrateur peut accepter les dispositions du CLUF dans la Console d'administration de Kaspersky Endpoint Security for Android.

Vous pouvez mettre à jour l'application à l'aide de Google Play si Kaspersky Endpoint Security for Android est installé depuis Google Play. Si l'application est installée d'une autre manière, vous pouvez la mettre à jour à l'aide de Google Play.

Mise à jour de l'application à l'aide de Kaspersky Security Center

La mise à jour de Kaspersky Endpoint Security for Android à l'aide de Kaspersky Security Center s'effectue après l'application d'une stratégie de groupe. Sélectionnez dans les paramètres de la stratégie de groupe le paquet d'installation autonome de la version de Kaspersky Endpoint Security for Android qui répond aux exigences de sécurité de l'entreprise.

La mise à jour via Kaspersky Security Center est accessible si Kaspersky Endpoint Security for Android est installé via Kaspersky Security Center. Si l'application est installée depuis Google Play, la mise à jour via Kaspersky Security Center est impossible.

Pour réaliser la mise à jour de Kaspersky Endpoint Security for Android à l'aide d'un paquet d'installation autonome sur l'appareil mobile de l'utilisateur, le système doit autoriser l'installation d'apps depuis des sources inconnues. Pour en savoir plus sur l'installation d'apps qui ne proviennent pas de Google Play, consultez l'*aide d'Android*.

Pour mettre à jour la version de l'application, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Avancé**.
5. Dans le groupe **Mise à jour de Kaspersky Endpoint Security for Android**, cliquez sur le bouton **Sélectionner**.

   La fenêtre **Mise à jour de Kaspersky Endpoint Security for Android** s'ouvre alors.
6. Dans la liste des paquets d'installation autonome de Kaspersky Endpoint Security, sélectionnez celui dont la version répond aux exigences de sécurité de l'entreprise.

   Vous pouvez mettre à jour Kaspersky Endpoint Security uniquement jusque la version la plus récente de l'application. Il est impossible de mettre Kaspersky Endpoint Security à jour vers une version plus ancienne.
7. Cliquez sur le bouton **Sélectionner**.

   La description du paquet d'installation autonome sélectionné s'affiche dans le groupe **Mise à jour de Kaspersky Endpoint Security for Android**.
8. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center. L'utilisateur du périphérique mobile est invité à installer la nouvelle version de l'application. Quand la proposition a été acceptée, la nouvelle version de l'application est installée sur le périphérique mobile.

Installation d'une version antérieure de Kaspersky Endpoint Security for Android

Si vous voulez éviter la mise à jour automatique de l'application et utiliser une version particulière de Kaspersky Endpoint Security for Android, désactivez la mise à jour automatique de l'application dans les paramètres de Google Play. Pour plus de détails, consultez le site du Support Technique Google.

La mise à jour automatique de Kaspersky Endpoint Security for Android n'est accessible que lors de l'installation de l'application depuis Google Play ou via Kaspersky Security Center en suivant le lien sur Google Play. Si l'application est installée via Kaspersky Security Center en suivant le lien vers le serveur Web personnel (à l'aide du paquet autonome d'installation), la mise à jour automatique est inaccessible. Dans ce cas mettez à jour Kaspersky Endpoint Security for Android manuellement à l'aide de la stratégie de groupe.

Pour installer une version antérieure de Kaspersky Endpoint Security for Android, procédez comme suit :

1. Supprimez Kaspersky Endpoint Security for Android des appareils mobiles des utilisateurs.

2. Installez Kaspersky Endpoint Security for Android via Kaspersky Security Center en suivant le lien vers le Serveur Web personnel. Pour ce faire, vous avez besoin du paquet d'installation de la version en question. Vous pouvez télécharger le distributif de versions antérieures de Kaspersky Endpoint Security for Android sur le site du Support Technique de Kaspersky.

Pour plus de détails sur les versions antérieures de Kaspersky Endpoint Security for Android, consultez *l'aide sur la version correspondante de Kaspersky Security for Mobile*.

Mise à jour des versions antérieures des plug-ins d'administration

Vous pouvez mettre à niveau les plug-ins d'administration à l'aide des méthodes suivantes :

- Installez la nouvelle version du plug-in d'administration à partir de la liste des paquets de distribution disponibles dans la Console d'administration de Kaspersky Security Center.

  La liste des paquets de distribution disponibles est mise à jour automatiquement après la sortie des nouvelles versions des applications Kaspersky.

- Téléchargez le paquet de distribution à partir d'une source externe et installez le plug-in d'administration de la nouvelle version à l'aide du fichier EXE.

  Pour mettre à jour les plug-ins d'administration de Kaspersky Endpoint Security for Android et de Kaspersky Device Management for iOS, il est nécessaire de télécharger la dernière version de l'application sur la page Kaspersky Security for Mobile et de lancer l'assistant d'installation de chaque plug-in. Les versions précédentes des plug-ins seront automatiquement supprimées lors de l'exécution de l'Assistant d'installation.

Les experts de Kaspersky recommandent d'utiliser la même version de l'application et des plug-ins d'administration. Si l'utilisateur met à niveau l'application à partir de Google Play, Kaspersky Security Center affiche une notification avec une invite pour mettre à jour le plug-in d'administration.

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

Si dans une nouvelle version du plug-in d'administration, de nouveaux paramètres sont ajoutés ou si les valeurs par défaut sont modifiées, les modifications seront appliquées seulement après l'ouverture de la stratégie de groupe. L'administrateur n'ouvrira pas la stratégie de groupe. Les paramètres de la version précédente du plug-in seront appliqués sur les appareils mobiles, même si la version du plug-in a été mise à jour.

Mise à niveau à partir de la liste dans la Console d'administration

Pour mettre à niveau les plug-ins d'administration, procédez comme suit :

1. Dans l'arborescence de la console, choisissez le dossier **Avancé** → **Installation à distance** → **Paquets d'installation**.
2. Dans l'espace de travail, sélectionnez **Actions supplémentaires** → **Afficher les versions actuelles des applications Kaspersky**.

   Cette opération ouvre la liste des versions mises à jour des applications Kaspersky.
3. Dans la section **Appareils mobiles**, sélectionnez le plug-in **Kaspersky Endpoint Security for Android** ou **Kaspersky Device Management for iOS**.
4. Cliquez sur le bouton **Télécharger les paquets de distribution**.

   Une distribution de plug-in sera téléchargée dans la mémoire de l'ordinateur (fichier EXE). Exécutez le fichier EXE. Suivez les instructions de l'Assistant d'installation.

Mise à niveau à partir du paquet de distribution

Pour mettre à niveau le plug-in d'administration de Kaspersky Endpoint Security for Android,

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

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

Pour mettre à niveau le plug-in d'administration de Kaspersky Device Management for iOS,

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

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

Vous pouvez confirmer la mise à niveau des plug-ins d'administration en consultant la liste des plug-ins d'administration d'applications installés dans la fenêtre des propriétés du Serveur d'administration, accessible dans la section **Avancé** → **Informations concernant les plug-ins d'administration d'applications installés**.

Suppression de Kaspersky Endpoint Security for Android

Les méthodes suivantes sont disponibles pour supprimer Kaspersky Endpoint Security for Android :

1. Suppression de l'application par l'utilisateur

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

2. Suppression de l'application par l'administrateur

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

Suppression de l'application à distance

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

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

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

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Avancé**.
5. Dans la section **Désinstallation de l'application Kaspersky Endpoint Security for Android**, cochez la case **Désinstaller l'application Kaspersky Endpoint Security for Android de l'appareil**.
6. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

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

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

1. Dans l'arborescence de la console, sélectionnez **Administration des appareils mobiles → Appareils mobiles**.
2. Dans la liste des appareils, sélectionnez celui sur lequel vous souhaitez supprimer l'application.
3. Double-cliquez pour ouvrir la fenêtre des propriétés de l'appareil.
4. Sélectionnez la section **Applications → Kaspersky Endpoint Security for Android**.
5. Double-cliquez pour ouvrir la fenêtre des propriétés de l'application Kaspersky Endpoint Security.
6. Choisissez la section **Avancé**.

7. Dans la section **Suppression de l'application Kaspersky Endpoint Security for Android**, cochez la case **Désinstaller Kaspersky Endpoint Security for Android de l'appareil**.

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

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

Permettre aux utilisateurs de supprimer l'application

Sur les appareils tournant sous le système d'exploitation Android version 7.0 et suivantes, Kaspersky Endpoint Security for Android doit être installé en tant que service des Fonctionnalités d'accessibilités pour protéger l'app contre la suppression. Pendant le fonctionnement de l'Assistant de configuration initiale, Kaspersky Endpoint Security for Android propose à l'utilisateur d'accorder les autorisations requises à l'app. L'utilisateur peut ignorer ces étapes ou désactiver les droits ultérieurement dans les paramètres de l'appareil. Dans ce cas, la protection de l'app contre la suppression ne fonctionne pas.

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

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

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

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

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.

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

3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie.

4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Avancé**.

5. Dans le groupe **Suppression de l'application Kaspersky Endpoint Security for Android**, cochez la case **Autoriser la suppression de l'application Kaspersky Endpoint Security for Android**.

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

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

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

1. Dans l'arborescence de la console, sélectionnez **Avancé → Administration des appareils mobiles → Appareils mobiles**.

2. Dans la liste des appareils, sélectionnez celui pour lequel vous souhaitez autoriser la suppression de l'application par l'utilisateur.
3. Double-cliquez pour ouvrir la fenêtre des propriétés de l'appareil.
4. Sélectionnez la section **Applications** → **Kaspersky Endpoint Security for Mobile**.
5. Double-cliquez pour ouvrir la fenêtre des propriétés de l'application Kaspersky Endpoint Security.
6. Sélectionnez la section **Avancé**.
7. Dans le groupe **Suppression de l'application Kaspersky Endpoint Security for Android**, cochez la case **Autoriser la suppression de l'application Kaspersky Endpoint Security for Android**.
8. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

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

Suppression de l'application par l'utilisateur

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

1. Dans la fenêtre principale de Kaspersky Endpoint Security for Android, appuyez sur → **Supprimer l'app**.

   Une demande de confirmation apparaît à l'écran.

   Si le bouton **Supprimer l'app** est absent, l'administrateur a activé la protection contre la suppression de Kaspersky Endpoint Security for Android.
2. Confirmer la suppression de Kaspersky Endpoint Security for Android.

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

Configuration et administration

Cette section est destinée au experts spécialisés dans l'administration de Kaspersky Security for Mobile et aux experts qui assurent l'assistance technique dans les organisations qui ont choisi de travailler avec Kaspersky Security for Mobile.

Guide de démarrage

Cette section décrit les actions dont l'exécution est recommandée avant de commencer à utiliser Kaspersky Security for Mobile.

Lancement et arrêt de l'application

Kaspersky Security Center lance et arrête automatiquement les plug-ins d'administration de Kaspersky Endpoint Security et Kaspersky Device Management for iOS.

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'app en désactivant tous les composants de Kaspersky Endpoint Security for Android. Vous pouvez configurer l'accès de l'utilisateur à l'administration des composants de l'application à l'aide de stratégies de groupe.

Sur certains appareils (par exemple, Huawei, Meizu, Xiaomi) il faut ajouter manuellement Kaspersky Endpoint Security for Android à la liste des applications lancées au chargement du système d'exploitation (**Sécurité** → **Autorisations** → **Démarrage automatique**). Si l'application n'est pas ajoutée à la liste, Kaspersky Endpoint Security for Android cesse d'exécuter toutes les fonctions après le redémarrage de l'appareil mobile.

Il faut désactiver également le mode économie d'énergie pour Kaspersky Endpoint Security for Android. Cela est nécessaire pour que l'application fonctionne en arrière-plan, par exemple, pour le lancement de la recherche de virus programmée ou pour la synchronisation de l'appareil avec Kaspersky Security Center. Le problème vient des particularités des logiciels intégrés dans ces appareils.

Création d'un groupe d'administration

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

Pour appliquer une stratégie au groupe d'appareils, il est conseillé de créer un groupe d'administration dédié à ces appareils dans le dossier **Appareils administrés** avant l'installation des applications mobiles sur les appareils des utilisateurs.

Après la création du groupe d'administration, il est recommandé de configurer le placement automatique dans ce groupe des appareils sur lesquels vous voulez installer les apps. Il faut ensuite définir les paramètres communs à l'ensemble des périphériques à l'aide d'une stratégie de groupe.

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

1. Dans l'arborescence de la console, sélectionnez le dossier **Appareils administrés**.
2. Dans l'espace de travail du dossier **Appareils administrés** ou dans un sous-dossier, sélectionnez l'onglet **Appareils**.
3. Cliquez sur le bouton **Créer un groupe**.

   La fenêtre de création d'un nouveau groupe s'ouvrira alors.
4. Dans la fenêtre **Nom du groupe** qui s'ouvre, saisissez le nom du groupe, puis cliquez sur le bouton **OK**.

A l'issue de la procédure, un nouveau dossier du groupe d'administration au nom défini sera affiché dans l'arbre de la console. Pour en savoir plus sur l'utilisation des groupes d'administration, consultez *l'Aide de Kaspersky Security Center*.

Stratégies de groupe pour l'administration des appareils mobiles

Une *stratégie de groupe* est un ensemble unique de paramètres pour l'administration des appareils mobiles appartenant à un groupe d'administration, et des applications mobiles qui y sont installées. Vous pouvez créer une stratégie de groupe à l'aide de l'Assistant de création de stratégie.

Une stratégie permet de configurer les paramètres de appareils 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 appareil peuvent différer de ceux indiqués dans la stratégie du groupe auquel cet appareil appartient.

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

Les valeurs de paramètres définies dans la stratégie et dans les paramètres locaux de l'application sont enregistrées sur le Serveur d'administration. Elles sont diffusées sur les appareils mobiles lors de la synchronisation et sont considérées comme des paramètres actifs. 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 préserver l'actualité de la sécurité d'entreprise sur les appareils mobiles, vous pouvez contrôler la conformité des appareils des utilisateurs à la stratégie de groupe d'administration.

L'indicateur du niveau de sécurité s'affiche dans la partie supérieure de la fenêtre de la stratégie de groupe. L'indicateur du niveau de sécurité vous aidera à configurer la stratégie pour avoir un niveau élevé de protection des appareils. L'indicateur du niveau de protection change l'état en fonction de la configuration de la stratégie :

- **Haut niveau de protection** : la protection des appareils est assurée au niveau requis. Tous les modules de la protection fonctionnent conformément aux paramètres recommandés par les experts de Kaspersky.
- **Niveau de protection moyen** : le niveau de protection est réduit. Certains modules de protection importants sont désactivés (par exemple, la Protection Internet). Les problèmes importants sont marqués par le signe .
- **Bas niveau de protection** : présence de problèmes qui pourraient entraîner l'infection de l'appareil et la perte d'informations. Certains modules de protection critiques sont désactivés (par exemple, la protection en temps réel des appareils est désactivée). Les problèmes critiques sont marqués par le signe .

Pour en savoir plus sur l'administration des stratégies et des groupes d'administration dans la Console d'administration de Kaspersky Security Center, consultez *l'Aide de Kaspersky Security Center*.

Création d'une stratégie de groupe

Cette section décrit la création de stratégies de groupe pour les périphériques dotés de l'application mobile Kaspersky Endpoint Security for Android et de stratégies pour les appareils 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.

Étape 1. 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** for Android, pour les appareils utilisant l'application mobile Kaspersky Endpoint Security for Android.

Il est recommandé de créer une stratégie distincte pour les appareils Huawei et Honor qui ne disposent pas des services Google Play. De cette façon, vous pouvez envoyer des liens vers Huawei AppGallery aux utilisateurs de tous ces appareils.

- **Kaspersky Device Management for iOS**, pour les appareils EAS et les appareils MDM iOS.

Il est possible de créer une stratégie pour des appareils mobiles si le poste de travail de l'administrateur est doté du plug-in d'administration de Kaspersky Endpoint Security for Android et du plug-in d'administration de Kaspersky Device Management for iOS. Si les plug-ins ne sont pas installés, le nom de l'application correspondante ne figure pas dans la liste des applications.

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

Étape 2. Saisie 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.

Étape 3. Création d'une stratégie de groupe pour l'application

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.

Configuration des paramètres de la synchronisation

Pour l'administration des appareils mobiles et la réception des rapports ou des statistiques des appareils mobiles des utilisateurs, vous devez configurer les paramètres de synchronisation. La synchronisation de l'appareil mobile avec Kaspersky Security Center peut être exécutée par les moyens suivants :

- **Planification**. La synchronisation est exécutée d'après l'horaire planifié à l'aide du protocole HTTP. Vous pouvez configurer l'horaire de la synchronisation dans les paramètres de la stratégie de groupe. Les modifications des paramètres de la stratégie de groupe, les commandes et les tâches seront exécutées pendant la synchronisation de l'appareil avec Kaspersky Security Center d'après l'horaire, à savoir avec du retard. Par défaut, les appareils mobiles se synchronisent automatiquement avec Kaspersky Security Center toutes les six heures.

  Sur Android 12 ou une version ultérieure, l'application peut effectuer cette tâche plus tard que prévu si l'appareil est en mode d'économie de la batterie.

- **Forcée**. La synchronisation forcée est exécutée à l'aide des notifications push du service FCM (Firebase Cloud Messaging). La synchronisation forcée, en premier lieu, est destinée à l'envoi opportun des commandes à l'appareil mobile. Si vous voulez utiliser la synchronisation forcée, assurez-vous que les paramètres GSM dans Kaspersky Security Center sont configurés. Pour en savoir plus, consultez l'Aide de Kaspersky Security Center.

Pour configurer les paramètres de synchronisation des appareils mobiles avec Kaspersky Security Center, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Synchronisation**.
5. Sélectionnez la fréquence de lancement de la synchronisation dans la liste déroulante **Lancer la synchronisation**.
6. Pour interdire la synchronisation de l'appareil avec Kaspersky Security Center en itinérance, cochez la case **Désactiver la synchronisation en itinérance**.

   L'utilisateur de l'appareil peut exécuter la synchronisation manuellement dans les paramètres de l'application (→ **Paramètres** → **Synchronisation** → **Synchroniser**).
7. Pour masquer à l'utilisateur les paramètres de synchronisation (adresse du serveur, port et groupe d'administration) dans les paramètres de l'application, décochez la case **Afficher les paramètres de synchronisation sur l'appareil**. Il est impossible de modifier les paramètres masqués.
8. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center. Vous pouvez forcer la synchronisation de l'appareil mobile à l'aide d'une commande spéciale. Pour en savoir plus sur l'utilisation des commandes pour les appareils mobiles, consultez *l'aide de Kaspersky Security Center*.

Utilisation des révisions des stratégies de groupe

Kaspersky Security Center permet de suivre les modifications des stratégies de groupe. Chaque fois que vous enregistrez les modifications d'une stratégie de groupe, une *révision* est créée. Chaque révision a un numéro.

L'utilisation des révisions est accessible uniquement aux stratégies de Kaspersky Endpoint Security for Android. Pour la stratégie de Kaspersky Device Management for iOS les révisions sont inaccessibles.

Vous pouvez exécuter les actions suivantes sur les révisions des stratégies de groupe :

- comparer la révision sélectionnée à la révision en cours ;
- comparer les révisions sélectionnées ;
- comparer la stratégie à la révision sélectionnée d'une autre stratégie ;
- consulter la révision sélectionnée ;
- annuler les modifications de stratégie apportées à révision sélectionnée ;
- enregistrer les révisions dans un fichier au format TXT.

Pour en savoir plus sur l'utilisation des révisions des stratégies de groupe et des autres objets (par exemple, comptes utilisateurs), consultez *l'Aide de Kaspersky Security Center*.

Pour consulter l'historique de révisions d'une stratégie de groupe, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Historique des révisions**.

   Une liste des révisions de stratégie s'affiche. Elle contient les informations suivantes :

   - le numéro de révision de la stratégie ;
   - la date et le heure de modification de la stratégie ;
   - le nom de l'utilisateur ayant modifié la stratégie ;
   - l'action exécutée avec la stratégie ;
   - description de la révision des paramètres de la stratégie.

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.

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

- **Autoriser la modification**. L'utilisateur de la Console d'administration peut modifier les paramètres de la stratégie dans la fenêtre des propriétés.
- **Interdire 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'administration des privilèges et des rôles des utilisateurs dans la Console d'administration de Kaspersky Security Center, consultez l'*Aide de Kaspersky Security Center*.

Protection

Cette section explique comment administrer à distance la protection des appareils mobiles dans la Console d'administration Kaspersky Security Center.

Configuration de la protection antivirus des appareils Android

Pour détecter les menaces à temps, pour réaliser une recherche de virus ou d'autres applications malveillantes, il faut configurer les paramètres de la protection en temps réel et le lancement automatique de la recherche de virus.

Kaspersky Endpoint Security for Android détecte les types d'objets suivants :

- virus, vers, chevaux de Troie, les outils malveillants ;
- applications publicitaires ;
- applications que les individus malintentionnés peuvent utiliser pour nuire à l'appareil ou aux données personnelles de l'utilisateur.

L'Antivirus possède une série de restrictions :

- Lors du fonctionnement de l'Antivirus dans le profil de travail, il est impossible d'éliminer automatiquement la menace détectée dans la mémoire externe de l'appareil (par exemple, sur la carte SD) (Applications avec "portefeuille", Configuration du profil de travail Android). Kaspersky Endpoint Security for Android n'a pas dans le profil de travail accès à la mémoire externe. Les informations sur les objets détectés s'affichent dans la section **État** de l'app. Pour éliminer les objets détectés dans la mémoire externe, il faut supprimer le fichier à la main et lancer à nouveau l'analyse de l'appareil.
- En raison de restrictions techniques, Kaspersky Endpoint Security for Android n'est pas capable d'analyser les fichiers de 2 Go ou plus. Dans le cadre de l'analyse, l'app ignore ces fichiers et ne les signale pas.

Pour configurer les paramètres de la protection en temps réel de l'appareil mobile, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Protection**.
5. 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 for Android analyse uniquement les nouvelles apps et les fichiers du dossier Téléchargements.
   - Pour activer la protection étendue 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, installe et sauvegarde sur l'appareil, ainsi que les applications mobiles juste après leur installation.

     Sur les appareils gérés par le système d'exploitation Android 8.0 et plus, Kaspersky Endpoint Security for Android analyse les fichiers que l'utilisateur modifie, transfère, installe et enregistre, ainsi que les copies des fichiers. Kaspersky Endpoint Security for Android n'analyse pas les fichiers lors de leur ouverture, ni les fichiers d'origine en cours de copie.

- 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 **Protection cloud (KSN)**.

- Pour bloquer les applications publicitaires et les applications susceptibles d'être exploitées par des criminels pour nuire à l'appareil ou aux données de l'utilisateur, cochez la case **Détecter les applications publicitaires, les numéroteurs automatiques et les applications susceptibles d'être utilisés par des criminels pour nuire à l'appareil et aux données de l'utilisateur**.

6. Sélectionnez une des options suivantes dans la liste **Action en cas de détection d'une menace** :

   - **Supprimer**

     Les objets détectés sont automatiquement supprimés. L'utilisateur n'a besoin d'effectuer aucune action supplémentaire. Avant la suppression, Kaspersky Endpoint Security for Android affiche une notification temporaire sur la détection de l'objet.

   - **Ignorer**

     Si des objets détectés ont été ignorés, Kaspersky Endpoint Security for Android avertit l'utilisateur de la présence de problèmes dans la protection de l'appareil. Les informations sur les objets ignorés s'affichent dans la section **État** de l'app. Pour chaque menace ignorée, l'utilisateur a le choix entre plusieurs actions pour l'éliminer. Le contenu de la liste des objets ignorés peut changer, par exemple si un fichier malveillant est supprimé ou déplacé. Pour obtenir la liste actuelle des menaces, lancez une analyse complète de l'appareil. Afin de vraiment garantir la protection des données, il est conseillé de supprimer tous les objets détectés.

   - **Quarantaine**

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

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Pour configurer le lancement automatique de la recherche de virus sur l'appareil mobile, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.

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

3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie.

4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Analyse**.

5. Pour bloquer les applications publicitaires et les applications susceptibles d'être exploitées par des criminels pour nuire à l'appareil ou aux données de l'utilisateur, cochez la case **Détecter les applications publicitaires, les numéroteurs automatiques et les applications susceptibles d'être utilisés par des criminels pour nuire à l'appareil et aux données de l'utilisateur**.

6. Sélectionnez une des options suivantes dans la liste **Action en cas de détection d'une menace** :

   - **Supprimer**

     Les objets détectés sont automatiquement supprimés. L'utilisateur n'a besoin d'effectuer aucune action supplémentaire. Avant la suppression, Kaspersky Endpoint Security for Android affiche une notification temporaire sur la détection de l'objet.

- **Ignorer**

  Si des objets détectés ont été ignorés, Kaspersky Endpoint Security for Android avertit l'utilisateur de la présence de problèmes dans la protection de l'appareil. Les informations sur les objets ignorés s'affichent dans la section **État** de l'app. Pour chaque menace ignorée, l'utilisateur a le choix entre plusieurs actions pour l'éliminer. Le contenu de la liste des objets ignorés peut changer, par exemple si un fichier malveillant est supprimé ou déplacé. Pour obtenir la liste actuelle des menaces, lancez une analyse complète de l'appareil. Afin de vraiment garantir la protection des données, il est conseillé de supprimer tous les objets détectés.

- **Quarantaine**

- **Confirmer l'action.**

  L'application Kaspersky Endpoint Security for Android affiche une notification qui propose à l'utilisateur de choisir l'action à exécuter sur l'objet détecté : **Ignorer** ou **Supprimer**.

  L'option **Confirmer l'action** permet à l'utilisateur de l'appareil lors de la détection de quelques objets d'appliquer l'action choisie à chaque fichier à l'aide de la case **Appliquer à toutes les menaces**.

  Pour l'affichage de la notification sur les appareils mobiles tournant sous Android version 10.0 et suivantes, Kaspersky Endpoint Security for Android doit être installé en tant que service des Fonctionnalités d'accessibilité. Kaspersky Endpoint Security for Android propose à l'utilisateur d'installer l'app comme service des Fonctionnalités d'accessibilité pendant l'exécution de l'Assistant de configuration initiale. L'utilisateur peut ignorer cette étape ou désactiver ultérieurement le service dans les paramètres de l'appareil. Dans ce cas, Kaspersky Endpoint Security for Android affiche une fenêtre système Android qui propose à l'utilisateur de choisir l'action sur l'objet détecté : Ignorer ou Supprimer. Pour appliquer l'action à plusieurs objets, ouvrez Kaspersky Endpoint Security.

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

   Sur Android 12 ou une version ultérieure, l'application peut effectuer cette tâche plus tard que prévu si l'appareil est en mode d'économie de la batterie.

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

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center. Kaspersky Endpoint Security for Android analyse tous les fichiers, y compris le contenu des archives.

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. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.

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

3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie.

4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Mise à jour des bases de données**.

5. Pour que Kaspersky Endpoint Security for Android télécharge la mise à jour des bases de données selon une programmation quand l'appareil est en itinérance, cochez la case **Autoriser la mise à jour des bases de données en itinérance** dans le groupe **Mise à jour des bases de données en itinérance**.

   Même si la case est décochée, l'utilisateur peut lancer manuellement la mise à jour des bases antivirus en itinérance.

6. Indiquez dans le groupe **Source de mise à jour des bases de données** la source des mises à jour à partir de laquelle Kaspersky Endpoint Security for Android va copier et installer les mises à jour des bases antivirus de l'app :

   - **Serveurs Kaspersky**

     Utilisation du serveur de mises à jour de Kaspersky en tant que source des mises à jour pour le téléchargement des bases Kaspersky Endpoint Security for Android sur les appareils mobiles des utilisateurs. Pour la mise à jour des bases des serveurs de Kaspersky, Kaspersky Endpoint Security for Android transmet à Kaspersky les données (par exemple, l'identificateur du lancement de la tâche de mise à jour). Vous pouvez consulter la liste des données transmises lors de la mise à jour des bases dans le Contrat de Licence Utilisateur Final.

   - **Serveur d'administration**

     Utilisation du stockage du Serveur d'administration de Kaspersky Security Center en tant que source des mises à jour pour le téléchargement des bases de l'application Kaspersky Endpoint Security for Android sur les appareils mobiles des utilisateurs.

   - **Autre source**

     Utilisation d'un serveur tiers en tant que source des mises à jour pour le téléchargement des bases de l'application Kaspersky Endpoint Security for Android sur les appareils mobiles des utilisateurs. Pour effectuer la mise à jour, il est nécessaire de définir l'adresse HTTP du serveur dans le champ ci-dessous (par exemple http://domain.com/).

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

   Sur Android 12 ou une version ultérieure, l'application peut effectuer cette tâche plus tard que prévu si l'appareil est en mode d'économie de la batterie.

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

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Protection des appareils Android sur Internet

Pour protéger les données personnelles de l'utilisateur de l'appareil mobile dans Internet, activez la Protection Internet. La Protection Internet bloque les sites Internet malveillants qui distribuent un code malveillant et des sites Internet de phishing servant à voler vos données confidentielles afin d'obtenir un accès à vos comptes bancaires. La Protection Internet analyse les sites Internet avant leur ouverture à l'aide du service cloud du Kaspersky Security Network. Protection Internet permet également de configurer l'accès de l'utilisateur aux sites Internet sur la base des listes de sites autorisés et interdits que vous créez.

Kaspersky Endpoint Security for Android doit être installé en tant que Fonctionnalité d'accessibilité. Kaspersky Endpoint Security for Android propose à l'utilisateur d'installer l'app comme service des Fonctionnalités d'accessibilité pendant l'exécution de l'Assistant de configuration initiale. L'utilisateur peut ignorer cette étape ou désactiver ultérieurement le service dans les paramètres de l'appareil.

La Protection Internet sur les appareils Android fonctionne seulement dans les navigateurs Google Chrome (y compris la fonction Onglets personnalisés), Huawei Browser et Samsung Internet Browser. La Protection Internet pour le navigateur Samsung Internet ne bloque pas les sites sur un appareil mobile si un profil de travail est utilisé et que la Protection Internet est activée uniquement pour ce profil de travail.

Pour activer la Protection Internet dans Google Chrome, Huawei Browser et Samsung Internet Browser, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la **Protection Internet**.
5. Pour utiliser la Protection Internet, vous ou l'utilisateur de l'appareil devez accepter la Déclaration relative au traitement des données aux fins d'utilisation de la Protection Internet (Déclaration sur la Protection Internet) :
   a. Cliquez sur le lien **Déclaration sur la Protection Internet**.

      La fenêtre **Déclaration relative au traitement des données aux fins d'utilisation de la Protection Internet** s'ouvre. Pour accepter la Déclaration sur la Protection Internet, vous devez lire et accepter la Politique de confidentialité.

   b. Cliquez sur le lien Politique de confidentialité. Lisez et acceptez la Politique de confidentialité.

      Si vous n'acceptez pas la Politique de confidentialité, l'utilisateur de l'appareil mobile peut l'accepter dans l'assistant de configuration initiale ou dans l'application (→ **A propos** → **Conditions** → **Politique de confidentialité**).

   c. Sélectionnez le mode d'acceptation de la Déclaration sur la Protection Internet :

      - **J'ai lu et j'accepte la Déclaration sur la Protection Internet**
      - **Demandez l'acceptation de la Déclaration sur la Protection Internet de la part de l'utilisateur de l'appareil**
      - **Je n'accepte pas la Déclaration sur la Protection Internet**
6. Si vous sélectionnez **Je n'accepte pas la Déclaration sur la Protection Internet**, la Protection Internet ne bloque pas de site sur un appareil mobile. L'utilisateur de l'appareil mobile ne peut pas activer la Protection Internet dans Kaspersky Endpoint Security.
7. Cochez la case **Activer la Protection Internet**.
8. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

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

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.

Envoi de commandes sur un appareil mobile

Pour protéger les données sur un appareil mobile en cas de perte ou de vol de ce dernier, vous pouvez envoyer les commandes suivantes (cf. tableau ci-après).

Commandes de protection des données en cas de perte ou de vol d'un appareil

Mode de connexion au Kaspersky Security Center	Commande	Résultat de l'exécution de la commande
Kaspersky Endpoint Security for Android	Verrouiller	L'appareil mobile est verrouillé.
	Déverrouiller	Sur les appareils tournant sous le système d'exploitation Android version 5.0 à 6.X, le mot de passe de déverrouillage de l'écran (code PIN) de l'appareil sera remplacé par "1234" après le déverrouillage de l'appareil mobile. Sur les appareils tournant sous le système d'exploitation Android 7.0 et suivant, le mot de passe de déverrouillage de l'écran reste inchangé après le déverrouillage de l'appareil mobile.
	Géolocaliser l'appareil	La géolocalisation est déterminée et apparaît sur Google Maps. L'opérateur du réseau de téléphonie mobile facture l'envoi de SMS et l'accès Internet. Sur les appareils tournant sous Android 12 ou version ultérieure, si l'utilisateur a accordé l'autorisation "Utiliser l'emplacement approximatif", l'application Kaspersky Endpoint Security for Android essaie d'abord d'obtenir l'emplacement précis de l'appareil. En cas d'échec, l'emplacement approximatif de l'appareil n'est renvoyé que s'il n'a pas été reçu plus de 30 minutes plus tôt. Sinon, la commande **Géolocaliser l'appareil** échoue.
	Photographier	L'appareil mobile est verrouillé. La photo a été prise avec la caméra avant de l'appareil lorsque quelqu'un a essayé de déverrouiller l'appareil. L'opérateur du réseau de téléphonie mobile facture l'envoi de SMS et l'accès Internet. Lorsque vous essayez de déverrouiller l'appareil, l'utilisateur accepte automatiquement de prendre une photo.

		Si l'autorisation d'utiliser la caméra a été révoquée, l'appareil mobile affiche une notification et vous invite à fournir l'autorisation. Sur un appareil mobile tournant sous Android 12 ou version ultérieure, si l'autorisation d'utiliser l'appareil photo a été révoquée via les Paramètres rapides, la notification ne s'affiche pas mais la photo prise est noire.
	Émettre l'alarme	L'appareil mobile émet l'alarme. L'alarme est émise pendant 5 minutes (si le niveau de la batterie est faible, l'alarme est émise pendant une minute).
	Supprimer les données d'entreprise	Les données du conteneur, le compte utilisateur d'email d'entreprise, les paramètres de connexion au réseau Wi-Fi de l'entreprise, les réseaux VPN, le point d'accès (APN), le profil de travail Android, le conteneur KNOX, ainsi que la clé KNOX License Manager sont supprimés.
	Rétablir les paramètres par défaut.	Toutes les données sont supprimées sur l'appareil mobile et les paramètres de configuration sont réinitialisés à leurs valeurs par défaut. Une fois que cette commande a été exécutée, l'appareil ne peut plus recevoir et exécuter les commandes suivantes.
Profil MDM iOS	Verrouiller	L'appareil mobile est verrouillé.
	Déverrouiller	Le verrouillage de l'appareil mobile à l'aide d'un code PIN est désactivé. Le code PIN installé précédemment est réinitialisé.
	Supprimer les données d'entreprise	Suppression de tous les profils de configuration, de tous les profils provisioning, du profil MDM iOS et de toutes les applications dont la case **Supprimer en même temps que le profil iOS MDM** avait été cochée.
	Rétablir les paramètres par défaut.	Toutes les données sont supprimées sur l'appareil mobile et les paramètres de configuration sont réinitialisés à leurs valeurs par défaut. Une fois que cette commande a été exécutée, l'appareil ne peut plus recevoir et exécuter les commandes suivantes.
Boîte aux lettres Exchange	Rétablir les paramètres par défaut.	Toutes les données sont supprimées sur l'appareil mobile et les paramètres de configuration sont réinitialisés à leurs valeurs par défaut. Une fois que cette commande a été exécutée, l'appareil ne peut plus recevoir et exécuter les commandes suivantes.

L'exécution des commandes de Kaspersky Endpoint Security for Android requiert des autorisations et des droits spéciaux. Pendant le fonctionnement de l'Assistant de configuration initiale, Kaspersky Endpoint Security for Android propose à l'utilisateur d'accorder les autorisations et les privilèges requis à l'app. L'utilisateur peut ignorer ces étapes ou désactiver les droits ultérieurement dans les paramètres de l'appareil. Dans ce cas, l'exécution des commandes est impossible.

Sur les appareils tournant sous Android 10.0 ou une version ultérieure, l'utilisateur doit accorder l'autorisation "Tout le temps" pour accéder à la localisation. Sur les appareils tournant sous Android 11.0 ou une version ultérieure, l'utilisateur doit également accorder l'autorisation "Pendant l'utilisation de l'application" pour accéder à la caméra. Sinon, les commandes Antivol ne fonctionnent pas. L'utilisateur sera informé de cette limitation, et sera à nouveau invité à accorder les autorisations du niveau requis. Si l'utilisateur sélectionne l'option "Seulement cette fois" pour l'autorisation de la caméra, l'accès est considéré comme accordé par l'application. Il est recommandé de contacter directement l'utilisateur si l'autorisation de la caméra est à nouveau demandée.

Pour en savoir plus sur l'envoi de commandes au départ de liste des appareils mobiles dans la Console d'administration, consultez *l'Aide de Kaspersky Security Center*.

Déverrouillage de l'appareil mobile

Vous pouvez déverrouiller l'appareil mobile en utilisant une des méthodes suivantes :

- envoyer une commande de déverrouillage de l'appareil mobile ;
- saisir le code à usage unique de déverrouillage sur l'appareil mobile (uniquement pour les appareils Android).

Sur certains appareils (par exemple, Huawei, Meizu, Xiaomi) il faut ajouter manuellement Kaspersky Endpoint Security for Android à la liste des applications lancées au chargement du système d'exploitation. Si l'application n'est pas ajoutée à la liste, vous pouvez déverrouiller l'appareil seulement à l'aide du code de déverrouillage à usage unique. Il est impossible de déverrouiller l'appareil à l'aide des commandes.

Pour en savoir plus sur l'envoi de commandes au départ de liste des appareils mobiles dans la Console d'administration, consultez *l'Aide de Kaspersky Security Center*.

Le *code à usage unique de déverrouillage* est un code secret de l'application qui permet de déverrouiller l'appareil mobile. Ce code à usage unique est généré par l'application et est unique pour chaque appareil mobile. Vous pouvez modifier la longueur du code à usage unique (4, 8 ou 16 chiffres) dans les paramètres de la stratégie de groupe, section **Antivol**.

Pour déverrouiller l'appareil mobile à l'aide du code à usage unique, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez **Administration des appareils mobiles → 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. Sélectionnez la section **Applications → Kaspersky Endpoint Security for Android**.
5. Double-cliquez pour ouvrir la fenêtre des propriétés de l'application Kaspersky Endpoint Security.
6. Choisissez la section **Antivol**.
7. Le champ **Code à usage unique** du groupe **Code à usage unique pour le déverrouillage de l'appareil** contient le code unique pour l'appareil sélectionné.
8. Communiquez le code à usage unique à l'utilisateur de l'appareil mobile verrouillé via une des méthodes disponibles (par exemple, dans un message électronique).
9. L'utilisateur introduit le code à usage unique sur l'écran de l'appareil verrouillé par Kaspersky Endpoint Security for Android.

L'appareil mobile sera déverrouillé. Sur les appareils tournant sous le système d'exploitation Android version 5.0 à 6.X, le mot de passe de déverrouillage de l'écran (code PIN) de l'appareil sera remplacé par "1234" après le déverrouillage de l'appareil mobile. Sur les appareils tournant sous le système d'exploitation Android 7.0 et suivant, le mot de passe de déverrouillage de l'écran reste inchangé après le déverrouillage de l'appareil mobile.

Chiffrement des données

Pour protéger les données contre tout accès non autorisé, il faut activer le chiffrement de toutes les données sur l'appareil (par exemple, les identifiants, les données des périphériques externes et des applications externes, ainsi que celles des messages électroniques, des messages SMS, des contacts, des images et des autres fichiers). L'accès aux données chiffrées requiert la définition d'une clé spéciale, à savoir un mot de passe pour déverrouiller l'appareil. Ainsi, quand les données sont chiffrées, l'accès est octroyé uniquement lorsque l'appareil est déverrouillé.

Sur les appareils iOS, le chiffrement des données est activé par défaut si le mot de passe de déverrouillage de l'appareil a été défini (**Paramètres** → **Touch ID et mot de passe/Face ID et mot de passe** → **Activer le mot de passe)**.

Pour chiffrer toutes les données sur un appareil Android, procédez comme suit :

1. Activez le verrouillage de l'écran de l'appareil Android (**Paramètres** → **Sécurité** → **Verrouillage de l'écran**).
2. Définissez un mot de passe de déverrouillage de l'appareil qui respecte les exigences de sécurité de l'entreprise.

   Il est déconseillé d'utiliser un schéma comme mode de déverrouillage de l'appareil. Sur certains appareils Android tournant sous Android 6.0 et suivant, il faut saisir un mot de passe numérique au lieu du schéma pour déverrouiller l'appareil après le chiffrement des données et le redémarrage de l'appareil. Le problème est lié aux particularités du fonctionnement du service des Fonctionnalités d'accessibilité. Dans ce cas, pour déverrouiller l'écran de l'appareil, convertissez le schéma en chiffres. Pour savoir comment convertir le schéma en chiffres, consultez le site d'assistance technique du fabricant de l'appareil mobile.

3. Activez le chiffrement de toutes les données de l'appareil (**Paramètres** → **Sécurité** → **Chiffrer les données**).

Définition de la fiabilité du mot de passe de déverrouillage de l'appareil

Pour protéger l'appareil mobile de l'utilisateur contre l'accès, il convient d'activer un mot de passe de déverrouillage de l'appareil.

Cette section explique comment configurer la protection par mot de passe des appareils Android et iOS.

Définition de la fiabilité du mot de passe de déverrouillage d'un appareil Android

Pour assurer la sécurité de l'appareil Android il est nécessaire de configurer l'utilisation d'un mot de passe à saisir lors de la sortie de l'appareil du mode veille.

Vous pouvez définir des restrictions sur l'utilisation de l'appareil par un utilisateur si le mot de passe de déverrouillage n'est pas assez complexe (par exemple, verrouiller l'appareil). Vous pouvez définir de telles limites à l'aide du composant Contrôle de conformité. Pour ce faire, accédez aux paramètres de la règle d'analyse et sélectionnez l'option **Le mot de passe de déverrouillage n'est pas conforme aux exigences de sécurité**.

Sur certains appareils Samsung tournant sous le système d'exploitation Android 7.0 et version ultérieure, si l'utilisateur tente de configurer des modes de déverrouillage de l'appareil non pris en charge (par exemple, mot de passe graphique), l'appareil peut être verrouillé si les conditions suivantes sont réunies : la protection contre la suppression de Kaspersky Endpoint Security for Android est activée et les exigences de la sécurité du mot de passe de déverrouillage de l'écran sont définies. Pour déverrouiller l'appareil, il faut lui envoyer une commande spéciale.

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

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.

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

3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie.

4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Gestion de l'appareil**.

5. Si vous souhaitez que l'application recherche l'existence d'un mot de passe de déverrouillage, cochez la case **Imposer la définition d'un mot de passe pour déverrouiller l'écran** dans le groupe **Verrouillage de l'écran**.

   Si l'application détecte qu'aucun mot de passe n'a été défini sur l'appareil, l'utilisateur devra en choisir un. Le mot de passe est défini en tenant compte des paramètres définis par l'administrateur.

6. Indiquez le nombre minimum de caractères dans le mot de passe.

   Nombre minimum de caractères du mot de passe. Valeurs possibles : de 4 à 16.

   Par défaut, le mot de passe de l'utilisateur contient 4 symboles.

   > Sur les appareils tournant sous Android 10.0 ou une version ultérieure, Kaspersky Endpoint Security résout les exigences de force du mot de passe en une des valeurs du système : moyenne ou élevée.

   Les valeurs pour les appareils tournant sous Android 10.0 ou une version ultérieure sont déterminées par les règles suivantes :

   - Si la longueur du mot de passe requise est de 1 à 4 symboles, l'application invite l'utilisateur à définir un mot de passe de force moyenne. Elle doit être soit numérique (PIN) sans séquence répétée ou ordonnée (par exemple 1234), soit alphabétique/alphanumérique. Le code PIN ou le mot de passe doit comporter au moins 4 caractères.

   - Si la longueur du mot de passe requise est d'au moins 5 symboles, l'application invite l'utilisateur à définir un mot de passe de force élevée. Elle doit être soit numérique (PIN) sans séquence répétée ou ordonnée, soit alphabétique/alphanumérique (mot de passe). Le code PIN doit comporter au moins 8 chiffres ; le mot de passe doit comporter au moins 6 caractères.

7. Si vous voulez que l'utilisateur ait la possibilité d'utiliser les empreintes digitales pour déverrouiller l'écran, cochez la case **Autoriser l'utilisation des empreintes digitales**. Si le mot de passe de déverrouillage ne correspond pas aux exigences de sécurité de l'entreprise, il est impossible d'utiliser le scanner d'empreintes digitales pour déverrouiller l'écran.

   > Sur les appareils tournant sous Android 10.0 ou une version ultérieure, l'utilisation de l'empreinte digitale pour déverrouiller l'écran peut être administrée pour le profil de travail uniquement.

   > Kaspersky Endpoint Security for Android ne limite pas l'utilisation du scanner d'empreintes digitales pour l'accès aux applications ou la confirmations des achats

   > Sur certains appareils Samsung, il est impossible d'interdire l'utilisation des empreintes digitales pour le déverrouillage de l'écran. Aussi, sur certains appareils Samsung, si le mot de passe de déverrouillage n'est pas conforme aux exigences de sécurité de l'entreprise, Kaspersky Endpoint Security for Android n'interdit pas l'utilisation des empreintes digitales pour le déverrouillage de l'écran.

Après l'ajout de l'empreinte digitale dans les paramètres de l'appareil, l'utilisateur peut déverrouiller l'écran via les moyens suivants :

- mettre le doigt sur le scanner d'empreintes, soit le moyen habituel ;
- saisir le mot de passe de déverrouillage, le moyen de secours.

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

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Définition de la fiabilité du mot de passe de déverrouillage d'un appareil iOS MDM

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. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Mot de passe**.
5. Dans le groupe **Réglages du mot de passe**, cochez la case **Appliquer les paramètres à l'appareil**.
6. 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 Device Management for iOS 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 Device Management for iOS comparera au nouveau mot de passe lors du changement de mot de passe. Si les mots de passe sont identiques, le nouveau mot de passe n'est pas accepté.

- Dans la liste **Temps maximal pour déverrouiller 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.

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

Kaspersky Device Management for iOS 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.

Définition de la fiabilité du mot de passe de déverrouillage d'un appareil EAS

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 Device Management for iOS ne demande pas de saisir ou de définir un mot de passe pour le déverrouillage lors du démarrage de l'appareil mobile.

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

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils EAS.

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

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

4. Dans la fenêtre Propriétés de la stratégie, sélectionnez la section **Mot de passe**.

5. Dans le groupe **Réglages du mot de passe**, cochez la case **Demander un mot de passe**.

6. 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 Device Management for iOS 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.

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

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center. Kaspersky Device Management for iOS vérifie si un mot de passe est défini sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée. Si le mot de passe pour le déverrouillage n'est pas indiqué, l'utilisateur sera invité à le définir. Le mot de passe doit être défini conformément aux paramètres indiqués dans la stratégie. Si le mot de passe pour le déverrouillage indiqué ne correspond pas aux exigences de la stratégie, l'utilisateur sera invité à le modifier.

Configuration d'un réseau privé virtuel (VPN)

Cette section explique comment configurer les paramètres du réseau virtuel privé (VPN) pour une connexion sûre aux réseaux Wi-Fi.

Configuration de l'VPN sur les appareils Android (Samsung uniquement)

Pour garantir la sécurité de la connexion de l'appareil Android au réseau Wi-Fi et protéger le transfert de données, il faut configurer les paramètres du VPN (Virtual Private Network).

La configuration du VPN n'est possible que pour les appareils Samsung.

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

- L'app qui utilise la connexion VPN doit être autorisée dans les paramètres du Pare-feu.

- 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.

Pour configurer la connexion VPN sur l'appareil mobile de l'utilisateur, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Administration de Samsung KNOX → Administration d'un appareil Samsung**.
5. Dans le groupe **VPN**, cliquez sur le bouton **Configurer**.

   La fenêtre **Réseau VPN** s'ouvre alors.
6. Dans la liste déroulante **Type de connexion**, sélectionnez le type de connexion VPN.
7. Saisissez le nom du tunnel VPN dans le champ **Nom du réseau**.
8. Dans le champ **Adresse du serveur**, saisissez le nom réseau ou l'adresse IP du serveur VPN.
9. 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.
10. 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.
11. 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.
12. 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 réseau**, saisissez le nom de l'utilisateur du périphérique mobile.
13. Pour le type de réseau **L2TP IPSec PSK**, indiquez également le mot de passe pour la clé L2TP dans le champ **Clé L2TP**.
14. Pour le type de réseau **PPTP**, cochez la case **Utiliser une connexion SSL** pour que l'app utilise la méthode de chiffrement MPPE (Microsoft Point-to-Point Encryption) afin d'assurer la sécurité du transfert de données lors de la connexion de l'appareil mobile au serveur VPN.

15. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

    Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Configuration de l'VPN sur les appareils iOS MDM

Afin de connecter l'appareil iOS MDM à un réseau privé virtuel (VPN) 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 VPN.

Pour configurer la connexion VPN sur le périphérique iOS MDM, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.

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

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

4. Dans la fenêtre **Propriétés** de la stratégie qui s'ouvre, sélectionnez la section **VPN**.

5. Dans le groupe **Réseaux VPN**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Réseau VPN** s'ouvre alors.

6. Saisissez le nom du tunnel VPN dans le champ **Nom du réseau**.

7. 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 et 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 versions 6.4 et suivantes avec le paquet Juniper Networks IVE version 7.0 et 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.

8. Dans le champ **Adresse du serveur**, saisissez le nom réseau ou l'adresse IP du serveur VPN.

9. 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**.

10. Configurez les paramètres de sécurité pour la connexion VPN conformément au type de réseau privé virtuel sélectionné.

11. Configurez (si nécessaire) les paramètres de connexion au réseau VPN 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 **OK**.

    Les paramètres de connexion du périphérique au réseau VPN via le serveur proxy seront ainsi configurés sur le périphérique iOS MDM.

12. Cliquez sur **OK**.

    Le nouveau réseau VPN s'affichera dans la liste.

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

La connexion au réseau VPN sera ainsi configurée sur le périphérique iOS MDM de l'utilisateur une fois la stratégie appliquée.

Configuration du Pare-feu sur les appareils Android (Samsung uniquement)

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

Pour configurer le pare-feu sur l'appareil mobile de l'utilisateur, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.

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

3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie active.

4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Administration de Samsung KNOX → Administration d'un appareil Samsung**.

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

   La fenêtre **Pare-feu** s'ouvre alors.

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

   - Pour autoriser toutes les connexions entrantes et sortantes, 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**.

7. 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 pour le Pare-feu** s'ouvre alors.

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

   c. Saisissez le nom système du paquet de l'app mobile (par exemple, `com.mobileapp.example`) dans le champ **Nom du paquet**.

   d. Cliquez sur **OK**.

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

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Protection de Kaspersky Endpoint Security for Android contre la suppression

Pour la protéger l'appareil mobile et respecter les exigences de sécurité de l'entreprise, vous pouvez activer la protection de Kaspersky Endpoint Security for Android contre la suppression. Dans ce cas, l'utilisateur ne peut pas supprimer l'app via l'interface de Kaspersky Endpoint Security for Android. En cas de suppression de l'app via les outils du système d'exploitation Android, une demande de désactivation des autorisations d'administrateur pour Kaspersky Endpoint Security for Android s'affiche. Après que les autorisations ont été désactivées, l'appareil mobile est verrouillé.

Sur certains appareils Samsung tournant sous le système d'exploitation Android 7.0 et version ultérieure, si l'utilisateur tente de configurer des modes de déverrouillage de l'appareil non pris en charge (par exemple, mot de passe graphique), l'appareil peut être verrouillé si les conditions suivantes sont réunies : la protection contre la suppression de Kaspersky Endpoint Security for Android est activée et les exigences de la sécurité du mot de passe de déverrouillage de l'écran sont définies. Pour déverrouiller l'appareil, il faut lui envoyer une commande spéciale.

Pour activer la protection de Kaspersky Endpoint Security for Android contre la suppression, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie.

4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Avancé**.

5. Dans le groupe **Suppression de l'application Kaspersky Endpoint Security for Android**, décochez la case **Autoriser la suppression de l'application Kaspersky Endpoint Security for Android**.

   Sur les appareils tournant sous le système d'exploitation Android version 7.0 et suivantes, Kaspersky Endpoint Security for Android doit être installé en tant que service des Fonctionnalités d'accessibilités pour protéger l'app contre la suppression. Pendant le fonctionnement de l'Assistant de configuration initiale, Kaspersky Endpoint Security for Android propose à l'utilisateur d'accorder les autorisations requises à l'app. L'utilisateur peut ignorer ces étapes ou désactiver les droits ultérieurement dans les paramètres de l'appareil. Dans ce cas, la protection de l'app contre la suppression ne fonctionne pas.

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

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center. En cas de tentative de suppression de l'app, l'appareil mobile est verrouillé.

Détection d'une attaque contre l'appareil (root)

Kaspersky Security for Mobile permet de détecter le piratage de l'appareil (root). Quand un appareil a été débridé, les fichiers système ne sont pas protégés et peuvent être modifiés. Il est également possible dans ce cas d'installer des applications tierces sur l'appareil. Après la détection de l'effraction, il est recommandé de restaurer le travail normal de l'appareil.

Pour la détection de la réception des droits root par l'utilisateur, Kaspersky Endpoint Security for Android utilise les services suivants :

- *Le service intégré Kaspersky Endpoint Security for Android* est un service de Kaspersky qui analyse la réception des droits root par l'utilisateur de l'appareil mobile (Kaspersky Mobile Security SDK).

- *SafetyNet Attestation* est un service de Google qui analyse l'intégrité du système d'exploitation, analyse le logiciel et le matériel de l'appareil, et définit les autres problèmes de sécurité. Pour en savoir plus sur le fonctionnement de SafetyNet Attestation, consultez le site Internet du Support Technique d'Android.

En cas de piratage de l'appareil, vous recevrez une notification. Vous pouvez consulter les notifications relatives à l'effraction dans l'espace de travail du Serveur d'administration sous l'onglet **Surveillance**. Vous pouvez également désactiver la notification relatives à l'effraction dans les paramètres de notifications d'événements.

Sur les appareils tournant sous Android, vous pouvez imposer des limites sur l'utilisation de l'appareil par l'utilisateur (par exemple, verrouiller l'appareil). Vous pouvez définir de telles limites à l'aide du composant Contrôle de conformité (cf. ill. ci-dessous). Pour ce faire, choisissez le critère **Autorisations root reçues sur l'appareil** dans les paramètres de la règle d'analyse.

Configuration du proxy HTTP global sur les appareils iOS MDM

Afin d'assurer la sécurité du trafic Internet de l'utilisateur, configurez 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. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Proxy HTTP global**.
5. Dans le groupe **Paramètres du proxy HTTP global**, cochez la case **Appliquer les paramètres à l'appareil**.
6. Sélectionnez le type de configuration du proxy HTTP global.

   Par défaut, le type de configuration manuel est sélectionné pour le proxy HTTP global et il est interdit à l'utilisateur de se connecter aux réseaux via portail captif sans connexion au serveur proxy. *Réseaux 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 du serveur proxy et port**, indiquez le nom de l'hôte, le domaine ou l'adresse IP du serveur proxy et le numéro de port du serveur proxy.
     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 captifs sans connexion à un 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 **Adresse Internet 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 captifs sans connexion à un serveur proxy**.
7. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

L'utilisateur de l'appareil mobile se connectera ainsi à Internet via le serveur proxy une fois la stratégie appliquée.

Ajout des certificats de sécurité sur les appareils iOS MDM

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 Device Management for iOS prend en charge les normes suivantes de certificats :

- **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. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Certificats**.
5. Dans le groupe **Certificats**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Certificat** s'ouvre.
6. 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.
7. 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.
8. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

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.

Ajout d'un profil SCEP sur les appareils MDM iOS

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. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **SCEP**.
5. Dans le groupe **Profils SCEP**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Profil SCEP** s'ouvre.
6. Dans le champ **Adresse Internet du serveur**, saisissez l'adresse Internet du serveur SCEP sur lequel le Centre de certification est déployé.

   L'URL peut comporter l'adresse IP ou le nom de domaine complet (FQDN). Par exemple, http://10.10.10.10/certserver/companyscep.
7. Dans le champ **Nom**, saisissez le nom du Centre de certification déployé sur le serveur SCEP.
8. 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.
9. 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.
10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. Dans la liste déroulante **Dimension de clé**, sélectionnez la taille en octets de la clé d'enregistrement : 1024 ou 2048.

16. 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**.

17. 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.

18. 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.

19. Cliquez sur **OK**.

    Le nouveau profil SCEP s'affichera dans la liste.

20. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

La réception automatique par Internet du certificat depuis le Centre de certification sera ainsi configurée sur l'appareil mobile de l'utilisateur une fois la stratégie appliquée.

Contrôle

Cette section explique comment contrôler à distance les appareils mobiles dans la Console d'administration Kaspersky Security Center.

Configuration des restrictions

Cette section explique comment configurer l'accès des utilisateurs aux fonctions des appareils mobiles.

Éléments particuliers à prendre en considération pour les appareils tournant sous Android 10 et suivant

Android 10 a introduit de nombreux changements et restrictions visant l'API 29 ou version suivante. Certains de ces changements affectent la disponibilité ou la fonctionnalité de certaines des fonctionnalités de l'application. Ces éléments à prendre en considération s'appliquent uniquement aux appareils tournant sous Android 10 ou plus.

Possibilité d'activer, de désactiver et de configurer le Wi-Fi

- Les réseaux Wi-Fi peuvent être ajoutés, supprimés et configurés dans la Console d'administration de Kaspersky Security Center. Lorsqu'un réseau Wi-Fi est ajouté à une stratégie, Kaspersky Endpoint Security reçoit cette configuration réseau lorsqu'il se connecte pour la première fois à Kaspersky Security Center.

- Lorsqu'un appareil détecte un réseau configuré via Kaspersky Security Center, Kaspersky Endpoint Security invite l'utilisateur à se connecter à ce réseau. Si l'utilisateur choisit de se connecter au réseau, tous les paramètres configurés via Kaspersky Security Center sont automatiquement appliqués. L'appareil se connecte alors automatiquement à ce réseau lorsqu'il est à portée, sans afficher d'autres notifications à l'utilisateur.

- Si l'appareil d'un utilisateur est déjà connecté à un autre réseau Wi-Fi, il arrive que l'utilisateur ne soit pas invité à approuver l'ajout d'un réseau. Dans ce cas, l'utilisateur doit désactiver et réactiver le Wi-Fi pour recevoir la suggestion.

- Lorsque Kaspersky Endpoint Security suggère à un utilisateur de se connecter à un réseau Wi-Fi et que l'utilisateur refuse de le faire, l'autorisation de l'application de changer d'état Wi-Fi est révoquée. Kaspersky Endpoint Security ne peut alors pas suggérer de se connecter à des réseaux Wi-Fi jusqu'à ce que l'utilisateur accorde à nouveau l'autorisation en allant sur **Paramètres** → **Apps et notifications** → **Accès spécial aux applications**→ **Contrôle du Wi-Fi** → **Kaspersky Endpoint Security**.

- Seuls les réseaux ouverts et les réseaux chiffrés avec WPA2-PSK sont pris en charge. Le chiffrement WEP et WPA n'est pas pris en charge.

- Si le mot de passe d'un réseau précédemment suggéré par l'application est modifié, l'utilisateur doit supprimer manuellement ce réseau de la liste des réseaux connus. L'appareil pourra alors recevoir une suggestion de réseau de Kaspersky Endpoint Security et s'y connecter.

- Lorsque le système d'exploitation d'un appareil est mis à jour de la version 9 ou antérieure d'Android à la version 10 ou ultérieure d'Android, et/ou que Kaspersky Endpoint Security installé sur un appareil tournant sous Android version 10 ou ultérieure est mis à jour, les réseaux précédemment ajoutés via Kaspersky Security Center ne peuvent pas être modifiés ou supprimés par les stratégies de Kaspersky Security Center. L'utilisateur peut toutefois modifier ou supprimer ces réseaux manuellement dans les paramètres de l'appareil.

- Sur les appareils tournant sous Android 10, un utilisateur est invité à saisir son mot de passe en cas de tentative de connexion manuelle à un réseau protégé suggéré. La connexion automatique ne nécessite pas la saisie du mot de passe. Si l'appareil d'un utilisateur est connecté à un autre réseau Wi-Fi, l'utilisateur doit d'abord se déconnecter de ce réseau pour se connecter automatiquement à l'un des réseaux suggérés.

- Sur les appareils tournant sous Android 11, un utilisateur peut se connecter manuellement à un réseau protégé suggéré par l'application sans saisir le mot de passe.

- Lorsque Kaspersky Endpoint Security est retiré d'un appareil, les réseaux précédemment suggérés par l'application sont ignorés.

- L'interdiction de l'utilisation des réseaux Wi-Fi n'est pas prise en charge.

Accès à la caméra

- Sur les appareils tournant sous Android 10, l'utilisation de la caméra ne peut pas être totalement interdite. L'interdiction de l'utilisation d'une caméra pour le profil de travail est toujours en vigueur.
- Si une application tierce tente d'accéder à la caméra de l'appareil, cette application sera bloquée et l'utilisateur sera informé du problème. Cependant, les applications qui utilisent la caméra en mode arrière-plan ne peuvent pas être bloquées.
- Lorsqu'une caméra externe est déconnectée d'un appareil, une notification de non disponibilité de la caméra peut s'afficher dans certains cas.

Gestion des méthodes de déverrouillage des écrans

- Kaspersky Endpoint Security résout les exigences de force du mot de passe en une des valeurs du système : moyenne ou élevée.
  - Si la longueur du mot de passe requise est de 1 à 4 symboles, l'application invite l'utilisateur à définir un mot de passe de force moyenne. Elle doit être soit numérique (PIN) sans séquence répétée ou ordonnée (par exemple 1234), soit alphanumérique. Le code PIN ou le mot de passe doit comporter au moins 4 caractères.
  - Si la longueur du mot de passe requise est d'au moins 5 symboles, l'application invite l'utilisateur à définir un mot de passe de force élevée. Elle doit être soit numérique (PIN) sans séquence répétée ou ordonnée, soit alphanumérique (mot de passe). Le code PIN doit comporter au moins 8 chiffres ; le mot de passe doit comporter au moins 6 caractères.
- L'utilisation de l'empreinte digitale pour déverrouiller l'écran peut être administrée pour le profil de travail uniquement.

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. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Gestion de l'appareil**.
5. 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**.

  Sur les appareils tournant sous Android 10.0 ou version ultérieure, l'interdiction d'utiliser les réseaux Wi-Fi n'est pas prise en charge.

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

  Sur les appareils tournant sous Android 10.0 ou version ultérieure, l'utilisation de la caméra ne peut pas être totalement interdite.

  Sur les appareils tournant sous Android 11 et suivantes, Kaspersky Endpoint Security for Android doit être installé en tant que service des fonctionnalités d'accessibilité. Kaspersky Endpoint Security for Android propose à l'utilisateur d'installer l'app comme service des Fonctionnalités d'accessibilité pendant l'exécution de l'Assistant de configuration initiale. L'utilisateur peut ignorer cette étape ou désactiver ultérieurement le service dans les paramètres de l'appareil. Si tel est le cas, vous ne pourrez pas restreindre l'utilisation de l'appareil photo.

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

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

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

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. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Restrictions des fonctionnalités**.
5. Dans le groupe **Paramètres des restrictions de fonctions**, cochez la case **Appliquer les paramètres à l'appareil**.
6. Configurez les restrictions des fonctions du périphérique iOS MDM.
7. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.
8. Sélectionnez la section **Restrictions des applications**.

9. Dans le groupe **Paramètres des restrictions d'applications**, cochez la case **Appliquer les paramètres à l'appareil**.

10. Configurez les restrictions pour les applications sur le périphérique iOS MDM.

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

12. Sélectionnez la section **Restrictions du contenu multimédia**.

13. Dans le groupe **Paramètres de restriction du contenu multimédia**, cochez la case **Appliquer les paramètres à l'appareil**.

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

15. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

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 de la restriction des fonctionnalités pour les appareil EAS

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. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils EAS.

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

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

4. Dans la fenêtre Propriétés de la stratégie, sélectionnez la section **Restrictions des fonctionnalités**.

5. Dans le groupe **Réglages de restriction des fonctionnalités**, 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 l'utilisation de la caméra**.
   - Pour autoriser les connexions Wi-Fi, cochez la case **Autoriser l'utilisation du 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 l'appareil et un poste de travail distant, cochez la case **Autoriser la connexion au Bureau à distance**.

- 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.
  - **Interdire**. L'utilisation de Bluetooth est interdite sur le périphérique mobile.

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

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Configuration de l'accès des utilisateurs aux sites Internet

Cette section explique comment configurer l'accès aux sites Internet sur les appareils Android et iOS.

Configuration de l'accès aux sites Internet sur les appareils Android

Vous pouvez configurer l'accès des utilisateurs des appareils Android aux sites Internet avec l'aide de la Protection Internet. La Protection Internet prend en charge le filtrage des sites Internet par catégorie, selon les catégories définies dans le service cloud du Kaspersky Security Network. Le Filtrage vous permet de limiter l'accès des utilisateurs à certains sites Internet ou catégories de sites Internet (par exemple, aux sites Internet de la catégorie "Jeux de hasard, loterie, tirages au sort" ou "Communication via Internet"). La Protection Internet protège aussi les données personnelles des utilisateurs sur Internet.

Kaspersky Endpoint Security for Android doit être installé en tant que Fonctionnalité d'accessibilité. Kaspersky Endpoint Security for Android propose à l'utilisateur d'installer l'app comme service des Fonctionnalités d'accessibilité pendant l'exécution de l'Assistant de configuration initiale. L'utilisateur peut ignorer cette étape ou désactiver ultérieurement le service dans les paramètres de l'appareil. Dans ce cas, la Protection Internet ne fonctionnera pas.

La Protection Internet sur les appareils Android fonctionne seulement dans les navigateurs Google Chrome (y compris la fonction Onglets personnalisés), Huawei Browser et Samsung Internet Browser. La Protection Internet pour le navigateur Samsung Internet ne bloque pas les sites sur un appareil mobile si un profil de travail est utilisé et que la Protection Internet est activée uniquement pour ce profil de travail.

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. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.

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

3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie.

4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la **Protection Internet**.

5. Cochez la case **Activer la Protection Internet**.

6. Pour utiliser la Protection Internet, vous ou l'utilisateur de l'appareil devez accepter la Déclaration relative au traitement des données aux fins d'utilisation de la Protection Internet (Déclaration sur la Protection Internet) :

   a. Cliquez sur le lien **Déclaration sur la Protection Internet**.

   La fenêtre **Déclaration relative au traitement des données aux fins d'utilisation de la Protection Internet** s'ouvre. Pour accepter la Déclaration sur la Protection Internet, vous devez lire et accepter la Politique de confidentialité.

   b. Cliquez sur le lien Politique de confidentialité. Lisez et acceptez la Politique de confidentialité.

   Si vous n'acceptez pas la Politique de confidentialité, l'utilisateur de l'appareil mobile peut l'accepter dans l'assistant de configuration initiale ou dans l'application (→ **A propos** → **Conditions** → **Politique de confidentialité**).

   c. Sélectionnez le mode d'acceptation de la Déclaration sur la Protection Internet :

   - **J'ai lu et j'accepte la Déclaration sur la Protection Internet**
   - **Demandez l'acceptation de la Déclaration sur la Protection Internet de la part de l'utilisateur de l'appareil**
   - **Je n'accepte pas la Déclaration sur la Protection Internet**

   Si vous sélectionnez **Je n'accepte pas la Déclaration sur la Protection Internet**, la Protection Internet ne bloque pas de site sur un appareil mobile. L'utilisateur de l'appareil mobile ne peut pas activer la Protection Internet dans Kaspersky Endpoint Security.

7. 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 la liste déroulante de la section **Protection Internet**.

   b. Créez une liste de catégories bloquées en cochant les cases en regard des catégories des sites Internet auxquels l'application bloquera l'accès.

8. 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 la liste déroulante de la section **Protection Internet**.

   b. Créez une liste de sites Internet en ajoutant les adresses des sites Internet auxquels l'application ne bloquera pas l'accès. Kaspersky Endpoint Security for Android prend en charge uniquement les expressions rationnelles. Lors de la saisie de l'adresse du site Internet autorisé, utilisez les modèles suivants :

   - `http:\/\/www\.example\.com.*` : autorisation pour toutes les pages enfants de la page Internet (par exemple, `http://www.example.com/about`).

- `https:\/\/.*example\.com` : autorisation pour tous les sous-domaines de la page Internet (par exemple, `https://pictures.example.com`).

Vous pouvez utiliser aussi l'expression `https?` pour choisir les protocoles HTTP et HTTPS. Pour en savoir plus sur les expressions rationnelles, consultez le site du Support Technique Oracle.

9. Si vous souhaitez que l'application bloque l'accès de l'utilisateur à tous les sites Internet, sélectionnez l'option **Tous les sites Internet sont interdits** dans la liste déroulante de la section **Protection Internet**.

10. 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**.

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

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Configuration de l'accès aux sites Internet sur les appareils iOS MDM

Configurez les paramètres de la Protection Internet pour contrôler l'accès aux sites Internet pour les utilisateurs de l'appareil MDM iOS. 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 appareils supervisés.

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

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.

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

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

4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Protection Internet**.

5. Dans le groupe **Paramètres de la Protection Internet**, cochez la case **Appliquer les paramètres à l'appareil**.

6. 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 Device Management for iOS permet l'accès à tous les sites Internet du domaine. Par exemple, si vous avez ajouté http://www.example.com dans la liste des sites Internet autorisés, l'accès à http://pictures.example.com ou http://www.example.com/movies est également autorisé. Si la liste des sites Internet autorisés est vide, l'application autorise l'accès à tous les sites Internet, excepté à ceux apparaissant dans la liste des sites interdits.

c. Dans le groupe **Sites Internet interdits**, créez la liste des sites Internet interdits.

L'adresse du site Internet doit commencer par `"http://"` ou `"https://"`. Kaspersky Device Management for iOS interdit l'accès à tous les sites Internet du domaine.

7. 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 favoris**.

b. Dans le groupe **Favoris**, créez la liste des onglets des sites Internet autorisés.

L'adresse du site Internet doit commencer par `"http://"` ou `"https://"`. Kaspersky Device Management for iOS permet 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 Device Management for iOS ajoute les sites Internet depuis la liste des onglets à la barre d'onglets de Safari sur l'appareil mobile de l'utilisateur.

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

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

Vérification de la conformité des appareils Android aux exigences de la sécurité de l'entreprise

Vous pouvez vérifier si les appareils Android répondent aux exigences de sécurité de l'entreprise. Les exigences de sécurité de l'entreprise régissent l'utilisation de l'appareil par l'utilisateur. Par exemple, la protection en temps réel doit être activée sur l'appareil, les bases antivirus doivent être à jour et le mot de passe de l'appareil doit être suffisamment complexe. La vérification de la conformité s'opère sur la base d'une liste de règles. Une règle de conformité contient les éléments suivants :

- les critères de vérification de l'appareil (par exemple, l'absence d'applications interdites sur l'appareil) ;
- délai octroyé à l'utilisateur de l'appareil pour rendre son appareil conforme (par exemple, 24 heures) ;
- l'action qui sera exécutée sur l'appareil si l'utilisateur ne l'a pas rendu conforme à l'issue du délai octroyé (par exemple, verrouillage de l'appareil).

> Sur Android 12 ou une version ultérieure, l'application peut effectuer cette tâche plus tard que prévu si l'appareil est en mode d'économie de la batterie.

Les actions suivantes sont proposées, si l'utilisateur ne rétablit pas la conformité dans le délai imparti :

- **Verrouillage de toutes les applications, sauf les systèmes**. Le lancement de toutes les applications, à part les apps système, sur l'appareil mobile de l'utilisateur est bloqué.
- **Verrouillage de l'appareil**. L'appareil mobile est verrouillé. Pour accéder aux données, il faut déverrouiller l'appareil. Si la cause du verrouillage n'est pas éliminée après le déverrouillage, l'appareil se verrouille à nouveau après la période indiquée.
- **Suppression des données d'entreprise**. Les données du conteneur, le compte utilisateur d'email d'entreprise, les paramètres de connexion au réseau Wi-Fi de l'entreprise, les réseaux VPN, le point d'accès (APN), le profil de travail Android, le conteneur KNOX, ainsi que la clé KNOX License Manager sont supprimés.

- **Rétablir les paramètres par défaut**. Toutes les données sont supprimées sur l'appareil mobile et les paramètres de configuration sont réinitialisés à leurs valeurs par défaut. Après l'exécution de cette action, l'appareil ne peut plus être administré. Pour connecter l'appareil à Kaspersky Security Center, il faut installe à nouveau Kaspersky Endpoint Security for Android.

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

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.

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

3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie active.

4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Contrôle de conformité**.

5. 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 l'appareil ne correspond pas à la stratégie, Kaspersky Endpoint Security for Android crée l'enregistrement **Non-conformité détectée : <nom du critère de vérification>** dans le journal des événements lors de la synchronisation de l'appareil avec le Serveur d'administration Le journal des événements peut être consulté sous l'onglet **Événements** dans les propriétés du Serveur d'administration ou dans les propriétés locales du programme.

6. 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 l'appareil ne correspond pas à la stratégie, lors de la synchronisation de ce dernier avec le Serveur d'administration, Kaspersky Endpoint Security for Android prévient l'utilisateur dans la section **État**.

7. Dans le groupe **Règles de conformité**, composez la liste des règles de vérification de la conformité des appareils à la stratégie. Pour ce faire, procédez comme suit :

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

      Lance l'Assistant de création des règles d'analyse.

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

      Après la fermeture de l'assistant, la nouvelle règle s'affiche dans le groupe **Règles de conformité** de la liste des règles de vérification.

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

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

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center. 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.

Contrôle du lancement des apps

Cette section explique comment configurer l'accès des utilisateurs aux apps sur l'appareil mobile.

Contrôle du lancement des apps sur les appareils Android

Pour garantir la protection de l'appareil mobile de l'utilisateur, il faut configurer les paramètres de lancement des apps sur l'appareil.

Vous pouvez définir des restrictions pour un utilisateur d'un l'appareil doté d'apps interdites ou privé des apps nécessaires (par exemple, verrouiller l'appareil). Vous pouvez définir de telles limites à l'aide du composant Contrôle de conformité. Pour ce faire, accédez aux paramètres de la règle d'analyse, puis sélectionnez l'option **Des applications interdites sont installées**, **Des applications de catégories bloquées ont été installées** ou **Toutes les applications nécessaires ne sont pas installées**.

Pour que le contrôle des applications fonctionne, Kaspersky Endpoint Security for Android doit être installé en tant que service des Fonctionnalités d'accessibilité. Kaspersky Endpoint Security for Android propose à l'utilisateur d'installer l'app comme service des Fonctionnalités d'accessibilité pendant l'exécution de l'Assistant de configuration initiale. L'utilisateur peut ignorer cette étape ou désactiver ultérieurement le service dans les paramètres de l'appareil. Dans ce cas, le Contrôle des applications ne fonctionne pas.

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

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Contrôle des applications**.
5. Dans le groupe **Mode de fonctionnement**, sélectionnez le mode de lancement des apps sur l'appareil mobile de l'utilisateur :
   - Pour autoriser l'utilisateur de l'appareil 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 interdites**.
   - Pour autoriser l'utilisateur de l'appareil mobile à lancer uniquement les apps reprises dans la liste des catégories et celles marquées comme autorisées, recommandées ou obligatoires, sélectionnez le mode **Applications autorisées**.
6. Pour que Kaspersky Endpoint Security for Android envoie les données relatives aux applications interdites dans le journal des événements sans les bloquer, cochez la case **Ne pas bloquer les apps interdites, consigner uniquement dans le journal des événements**.

   Kaspersky Endpoint Security for Android crée alors l'enregistrement **Une app interdite a été installée** dans le journal des événements lors de la prochaine synchronisation de l'appareil mobile de l'utilisateur avec le Serveur d'administration. Le journal des événements peut être consulté sous l'onglet **Événements** dans les propriétés du Serveur d'administration ou dans les propriétés locales du programme.
7. Pour que Kaspersky Endpoint Security for Android bloque l'exécution des apps système (par exemple, calendrier, appareil photo, paramètres) sur l'appareil mobile de l'utilisateur en mode **Applications autorisées**, cochez la case **Bloquer les apps système**.

   Les experts de Kaspersky ne recommandent pas de bloquer les apps système, puisque cela peut entraîner des défaillances dans le fonctionnement de l'appareil.

8. Composez la liste des catégories et des applications pour configurer le lancement des applications.

   Pour en savoir plus sur les catégories d'applications, consultez les Appendices.

   La liste des applications qui appartiennent à chaque catégorie peut être consultée sur le site de Kaspersky.

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

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Configuration des restrictions des apps sur les appareils EAS

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. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils EAS.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre Propriétés de la stratégie, sélectionnez la section **Restrictions des applications**.
5. 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 email personnels (POP3 ou IMAP4), cochez la case **Autoriser le message**.
   - 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**.
6. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Inventaire des logiciels sur les appareils Android

Vous pouvez exécuter l'inventaire des applications sur les appareils Android connectés à Kaspersky Security Center. Kaspersky Endpoint Security for Android reçoit les informations sur toutes les applications installées sur les appareils mobiles. Les informations acquises à la suite de l'inventaire s'affichent dans les propriétés de l'appareil dans la section **Événements**. Vous pouvez consulter les informations détaillées sur chaque application installée, y compris la version et l'éditeur.

Pour activer l'inventaire des logiciels, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Contrôle des applications**.
5. Dans la section **Inventaire logiciel**, cochez la case **Envoyer les données sur les apps installées**.
6. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center. Kaspersky Endpoint Security for Android envoie les données dans le journal des événements après chaque installation ou suppression d'une app sur l'appareil.

Configuration de l'affichage des appareils Android dans Kaspersky Security Center

Pour simplifier l'utilisation de la liste des appareils mobiles, il faut configurer les paramètres de l'affichage de l'appareil dans Kaspersky Security Center. La liste des appareils mobiles figure par défaut dans l'arborescence de la console **Avancé** → **Administration des appareils mobiles** → **Appareil mobiles**. Les informations sur l'appareil sont mises à jour automatiquement. Il est également possible d'actualiser la liste des appareils mobiles manuellement via le bouton **Mettre à jour** dans le coin supérieur droit.

Une fois connectés à Kaspersky Security Center, les appareils sont automatiquement ajoutés à la liste d'appareils mobiles. Cette liste peut contenir des informations sur l'appareil en question : modèle, système d'exploitation, adresse IP, et autres.

Vous pouvez configurer le format du nom de l'appareil et choisir l'état de l'appareil. L'état de l'appareil vous informe sur le fonctionnement des composants de Kaspersky Endpoint Security for Android sur l'appareil mobile de l'utilisateur.

Les composants de Kaspersky Endpoint Security for Android peuvent ne pas fonctionner pour les raisons suivantes :

- L'utilisateur a désactivé le composant dans les paramètres de l'appareil.
- L'utilisateur n'a pas accordé à l'app les autorisations nécessaires au fonctionnement du composant (par exemple, l'accès aux services de localisation n'a pas été accordé, ce qui empêche Antivol de déterminer la géolocalisation de l'appareil).

Pour afficher l'état de l'appareil, il faut activer la condition **Défini par l'application** dans les propriétés du groupe d'administration (**Propriétés → État de l'appareil → Conditions pour l'état de l'appareil "Critique"** et **Conditions pour l'état de l'appareil "Avertissement"**). Les propriétés du groupe d'administration permettent également de choisir d'autres critères pour la définition de l'état de l'appareil mobile.

Pour configurer l'affichage des appareils Android dans Kaspersky Security Center, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Informations sur l'appareil**.
5. Sélectionnez le format du nom de l'appareil dans la Console d'administration dans la section **Nom de l'appareil dans Kaspersky Security Center** :
   - Modèle d'appareil [email, identifiant de l'appareil] ;
   - Modèle d'appareil [Email (le cas échéant) ou identifiant de l'appareil].

   Identifiant de l'appareil : identifiant unique généré par Kaspersky Endpoint Security for Android à partir des données reçues de l'appareil. Pour les appareils mobiles tournant sous Android 10 et suivants, Kaspersky Endpoint Security for Android utilise le SSAID (identifiant Android) ou la somme de contrôle des autres données reçues de l'appareil. Pour les versions précédentes d'Android, l'application utilise l'IMEI.
6. Fermez le "cadenas" ().
7. Dans le groupe **État de l'appareil dans Kaspersky Security Center** choisissez l'état de l'appareil si le composant de Kaspersky Endpoint Security for Android ne fonctionne pas : (**Critique**), (**Avertissement**) ou (**OK**).

   Dans la liste des appareils mobiles, l'état de l'appareil change de valeur en fonction de l'état choisi.
8. Fermez le "cadenas".
9. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Administration

Cette section explique comment administrer à distance les paramètres des appareils mobiles dans la Console d'administration Kaspersky Security Center.

Configuration de la connexion au réseau Wi-Fi

Cette section explique comment configurer la connexion automatique au réseau Wi-Fi de l'entreprise sur les appareils Android et iOS MDM.

Connexion d'appareils Android au réseau Wi-Fi

Pour connecter un appareil mobile à un réseau Wi-Fi, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie qui s'ouvre, sélectionnez la section **Wi-Fi**.
5. Dans le groupe **Réseaux Wi-Fi**, cliquez sur **Ajouter**.

   La fenêtre **Réseau Wi-Fi** s'ouvre alors.
6. Dans le champ **Identificateur SSID réseau**, indiquez le nom du réseau Wi-Fi contenant le point d'accès (SSID).
7. Dans le groupe **Protection du réseau**, sélectionnez le type de sécurité du réseau Wi-Fi (ouvert ou sécurisé selon les protocoles WEP ou WPA/WPA2 PSK).
8. 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.
9. Saisissez dans le champ **Adresse du serveur proxy et port** l'adresse IP ou le nom DNS du serveur proxy ainsi que son numéro de port, le cas échéant.

   • Sur les appareils fonctionnant sous le système d'exploitation Android version 8.0 ou supérieure, il est impossible de configurer les paramètres du serveur proxy pour le réseau Wi-Fi à l'aide d'une stratégie. Vous pouvez configurer les paramètres du serveur proxy pour le réseau Wi-Fi sur l'appareil mobile manuellement.

   Si vous vous connectez au réseau Wi-Fi via un serveur proxy, vous pouvez configurer les paramètres de la connexion au réseau à l'aide d'une stratégie. La configuration des paramètres du serveur proxy sur les appareils Android 8.0 et suivant est manuelle. Il est impossible de modifier les paramètres de connexion au réseau Wi-Fi à l'aide d'une stratégie sur les appareils 8.0 et suivants, à l'exception du mot de passe d'accès au réseau.

   Si vous ne vous connectez pas au réseau Wi-Fi via un serveur proxy, l'administration de la connexion au réseau Wi-Fi à l'aide de stratégie n'est soumise à aucune restriction.
10. Créez une liste des adresses Internet dont la connexion ne nécessite pas le serveur proxy dans le champ **Ne pas utiliser le serveur proxy pour les adresses**.

    Vous pouvez, par exemple saisir l'adresse `example.com`. Dans ce cas, le serveur proxy ne sera pas utilisé pour les adresses `pictures.example.com`, `example.com/movies`, etc. Le protocole (par exemple, `http://`) peut être omis.

    Sur les appareils fonctionnant sous le système d'exploitation Android version 8.0 ou supérieure, l'exclusion du serveur proxy pour les adresses Internet ne fonctionne pas.
11. Cliquez sur **OK**.

    Le réseau Wi-Fi ajouté s'affichera dans la liste **Réseaux Wi-Fi**.

Vous pouvez modifier ou supprimer les réseaux Wi-Fi mentionnés dans la liste des réseaux en cliquant sur les boutons **Modifier** et **Supprimer** de la partie supérieure de la liste.

12. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center. L'utilisateur pourra ainsi se connecter au réseau Wi-Fi ajouté sans avoir à indiquer les paramètres du réseau après que la stratégie aura été appliquée sur l'appareil mobile de l'utilisateur.

Sur les appareils tournant sous Android version 10.0 ou une version ultérieure, si un utilisateur refuse de se connecter au réseau Wi-Fi suggéré, l'autorisation de l'application de changer d'état Wi-Fi est révoquée. L'utilisateur doit accorder cette autorisation manuellement.

Connexion d'appareils iOS MDM au réseau Wi-Fi

Afin de connecter automatiquement un appareil iOS MDM à un réseau Wi-Fi disponible et de garantir la sécurité des données, il convient de configurer les paramètres de connexion.

Pour configurer la connexion de l'appareil iOS MDM à un réseau Wi-Fi, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie qui s'ouvre, sélectionnez la section **Wi-Fi**.
5. Dans le groupe **Réseaux Wi-Fi**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Réseau Wi-Fi** s'ouvre alors.
6. Dans le champ **Identificateur SSID réseau**, indiquez le nom du réseau Wi-Fi contenant le point d'accès (SSID).
7. Pour que l'appareil MDM iOS se connecte automatiquement au réseau Wi-Fi, cochez la case **Connexion automatique**.
8. Pour empêcher la connexion d'appareils iOS MDM à un réseau Wi-Fi qui requiert une authentification préalable (réseau captif), cochez la case **Interdire la détection de réseau captif**.

   L'utilisation d'un réseau captif requiert la définition d'un abonnement, l'acceptation d'un contrat ou la réalisation d'un paiement. Les réseaux captifs sont déployés, par exemple, dans les cafés ou dans les hôtels.
9. Pour que le réseau Wi-Fi n'apparaisse pas dans la liste des réseaux disponibles sur l'appareil 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.
10. Dans la liste déroulante **Protection du réseau**, sélectionnez le type de protection de la connexion au réseau Wi-Fi :

- **Désactivée**. L'authentification de l'utilisateur n'est pas requise.
- **WEP**. Le réseau est protégé par le protocole de chiffrement WEP (Wireless Encryption Protocol).
- **WPA/WPA2 (personnel)**. Le réseau est protégé par le protocole de chiffrement WPA / WPA2 (Wi-Fi Protected Access).
- **WPA2 (personnel**). Le réseau est protégé par le protocole de chiffrement WPA / WPA2 (Wi-Fi Protected Access 2.0). Le type de protection WPA2 est accessible sur les appareils tournant sous le système d'exploitation iOS version 8 et suivants. WPA2 n'est pas accessible sur les appareils Apple TV.
- **Toutes (personnel)**. Le réseau est protégé par le protocole de chiffrement WEP, WPA ou 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 le protocole 802.1X.
- **WPA2 (d'entreprise)**. Le réseau est protégé par le protocole de chiffrement WPA2 avec une seule clé de chiffrement pour l'ensemble des utilisateurs (802.1X). Le type de protection WPA2 est accessible sur les appareils tournant sous le système d'exploitation iOS version 8 et suivants. WPA2 n'est pas accessible sur les appareils Apple TV.
- **Toutes (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)**, **WPA2 (d'entreprise)** ou **Toutes (d'entreprise)**, vous pouvez sélectionner les types de protocoles EAP (Extensible Authentication Protocol) pour l'identification de l'utilisateur sur le réseau Wi-Fi 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.

11. Configurez le compte utilisateur pour l'authentification de l'utilisateur lors de la connexion de l'appareil iOS MDM au réseau Wi-Fi :

    a. Cliquez sur le bouton **Configurer** 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 Wi-Fi.

    c. Pour imposer à l'utilisateur la saisie manuelle d'un mot de passe à chaque connexion au réseau Wi-Fi, 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 Wi-Fi.

    e. Dans la liste déroulante **Certificat d'authentification**, sélectionnez le certificat pour l'authentification de l'utilisateur sur le réseau Wi-Fi. Si la liste ne contient pas les certificats, **vous pouvez les ajouter dans la section** Certificats.

    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 **OK**.

Les paramètres du compte utilisateur pour l'authentification de l'utilisateur lors de la connexion au réseau Wi-Fi seront ainsi configurés sur l'appareil iOS MDM.

12. Configurez (si nécessaire) les paramètres de connexion au réseau Wi-Fi via le serveur proxy :

    a. Dans le groupe **Serveur proxy**, cliquez sur le bouton **Configurer**.

    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 **OK**.

    Les paramètres de connexion de l'appareil au réseau Wi-Fi via le serveur proxy seront ainsi configurés sur l'appareil iOS MDM.

13. Cliquez sur **OK**.

    Le nouveau réseau Wi-Fi s'affichera dans la liste.

14. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

La connexion au réseau Wi-Fi sera ainsi configurée sur le périphérique iOS MDM de l'utilisateur une fois la stratégie appliquée. L'appareil mobile de l'utilisateur se connectera automatiquement à un réseau Wi-Fi disponible. La protection des données lors de la connexion au réseau Wi-Fi est assurée par la technologie d'authentification.

Configuration de l'email

Cette section explique comment configurer les boîtes aux lettres sur les appareils mobiles.

Configuration d'une boîte aux lettres sur des appareils iOS MDM

Afin de permettre à l'utilisateur de l'appareil iOS MDM d'utiliser sa messagerie électronique, il convient d'ajouter un compte utilisateur de messagerie électronique à la liste des comptes utilisateur sur l'appareil iOS MDM.

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) ;
- 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. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez **Email**.
5. Dans le groupe **Comptes utilisateur de messagerie électronique**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Comptes de messagerie électronique** s'ouvre.
6. Dans le champ **Description**, saisissez la description du compte de messagerie électronique de l'utilisateur.
7. Sélectionnez le protocole de messagerie électronique :
   - **POP**
   - **IMAP**
8. 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.
9. 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.
10. Dans le champ **Adresse email**, saisissez l'adresse électronique de l'utilisateur du périphérique iOS MDM.
11. 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 permettre à l'utilisateur d'utiliser le service Mail Drop pour transmettre des pièces jointes de grande taille, cochez la case **Autoriser Mail Drop**.
    - Pour autoriser l'utilisateur à employer uniquement le client de messagerie iOS standard, cochez la case **Autoriser uniquement l'utilisation de l'application Mail**.
12. Configurez les paramètres d'utilisation du protocole S/MIME dans l'application Mail. *S/MIME* est un protocole pour la transmission des messages chiffrés avec une signature numérique.
    - Pour utiliser le protocole S/MIME pour la signature du courrier sortant, cochez la case **Signer les messages** et choisissez le certificat pour la signature. La signature numérique confirme l'authenticité de l'expéditeur et indique au destinataire que le contenu du message n'a pas changé au cours de la transmission. La signature des messages concerne uniquement les appareils mobiles qui tournent sous le système d'exploitation iOS version 10.3 et suivants.

- Pour utiliser le protocole S/MIME pour le chiffrement du courrier sortant, cochez la case **Chiffrer les messages par défaut** et choisissez le certificat pour le chiffrement (clé publique). Le chiffrement des messages concerne uniquement les appareils mobiles qui tournent sous le système d'exploitation iOS version 10.3 et suivants.

- Pour accorder à l'utilisateur la possibilité d'exécuter le chiffrement des messages séparément, cochez la case **Afficher l'interrupteur de chiffrement des messages**. Pour l'envoi de messages chiffrés, l'utilisateur doit cliquer sur l'icône dans l'application Mail dans le champ **Destinataire**.

13. Dans les groupes **Serveur de messagerie entrante** et **Serveur de messagerie sortante**, cliquez sur **Configuration** et configurez les paramètres de connexion aux serveurs :

    - **Adresse du serveur et port** : noms des hôtes ou adresses IP des serveurs du courrier entrant et sortant et numéros des ports des serveurs.

    - **Nom du compte** : 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 un seul mot de passe pour les serveurs de courrier entrant et sortant** : utilisation d'un seul mot de passe pour l'authentification de l'utilisateur sur les serveurs de courrier entrant et sortant.

    - **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.

14. Cliquez sur **OK**.

    Le nouveau compte utilisateur de messagerie électronique s'affichera dans la liste.

15. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

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.

Configuration d'une boîte aux lettres Exchange sur des appareils iOS MDM

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) ;

- 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. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Exchange ActiveSync**.
5. Dans le groupe **Comptes utilisateur Exchange ActiveSync**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Compte utilisateur Exchange ActiveSync** s'ouvre à l'onglet **Général**.
6. 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**.
7. Dans le champ **Adresse du serveur**, saisissez le nom réseau ou l'adresse IP du serveur Microsoft Exchange.
8. 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**.
9. 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**.
10. Dans le champ **Utilisateur du compte**, saisissez le nom de l'utilisateur du périphérique iOS MDM.

    Si ce champ est laissé vide, Kaspersky Device Management for iOS demandera le nom de l'utilisateur lors de l'application de la stratégie sur l'appareil MDM iOS. Vous pouvez utiliser les macros de la liste déroulante **Macros disponibles**.
11. 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**.
12. Dans le champ **Mot de passe**, saisissez le mot de passe du compte utilisateur Exchange ActiveSync pour l'autorisation sur le serveur Microsoft Exchange.
13. Sélectionnez l'onglet **Avancé** et configurez-y les paramètres avancés du compte utilisateur Exchange ActiveSync :

    - **Synchroniser l'e-mail pour la période <période>** ;
    - **Type d'authentification** ;
    - **Autoriser le déplacement des messages entre les comptes** ;
    - **Autoriser la synchronisation des dernières adresses utilisées** ;
    - **Autoriser uniquement l'utilisation de l'application Mail**.
14. Configurez les paramètres d'utilisation du protocole S/MIME dans l'application Mail. *S/MIME* est un protocole pour la transmission des messages chiffrés avec une signature numérique.

- Pour utiliser le protocole S/MIME pour la signature du courrier sortant, cochez la case **Signer les messages** et choisissez le certificat pour la signature. La signature numérique confirme l'authenticité de l'expéditeur et indique au destinataire que le contenu du message n'a pas changé au cours de la transmission. La signature des messages concerne uniquement les appareils mobiles qui tournent sous le système d'exploitation iOS version 10.3 et suivants.

- Pour utiliser le protocole S/MIME pour le chiffrement du courrier sortant, cochez la case **Chiffrer les messages par défaut** et choisissez le certificat pour le chiffrement (clé publique). Le chiffrement des messages concerne uniquement les appareils mobiles qui tournent sous le système d'exploitation iOS version 10.3 et suivants.

- Pour accorder à l'utilisateur la possibilité d'exécuter le chiffrement des messages séparément, cochez la case **Afficher l'interrupteur de chiffrement des messages**. Pour l'envoi de messages chiffrés, l'utilisateur doit cliquer sur l'icône dans l'application Mail dans le champ **Destinataire**.

15. Cliquez sur **OK**.

    Le nouveau compte utilisateur Exchange ActiveSync s'affichera dans la liste.

16. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

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.

Configuration d'une boîte aux lettres Exchange sur les appareils Android (Samsung uniquement)

Pour pouvoir utiliser l'email, les contacts et le calendrier de l'entreprise sur l'appareil mobile, il convient de configurer les paramètres de la boîte aux lettres Exchange.

La configuration de la boîte aux lettres Exchange est possible uniquement sur les appareils Samsung.

Pour configurer la boîte aux lettres Exchange sur l'appareil mobile, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.

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

3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie active.

4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Administration de Samsung KNOX** → **Administration d'un appareil Samsung**.

5. Dans le groupe **Exchange ActiveSync**, cliquez sur le bouton **Configurer**.

   La fenêtre **Paramètres du serveur de messagerie Exchange** s'ouvre.

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

7. Dans le champ **Domaine**, saisissez le nom du domaine de l'utilisateur de l'appareil mobile sur le réseau de l'entreprise.

8. Dans la liste déroulante **Fréquence de synchronisation**, sélectionnez la fréquence souhaitée pour la synchronisation de l'appareil mobile avec le serveur Microsoft Exchange.

9. Pour utiliser le protocole de transfert de données SSL, cochez la case **Utiliser une connexion (SSL)**.

10. Pour utiliser des certificats numériques afin de protéger l'échange de données entre l'appareil mobile et le serveur Microsoft Exchange, cochez la case **Vérifier le certificat du serveur**.

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

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Administration des applications mobiles tierces

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.

Sur Kaspersky Security for Android Service Pack 3 Maintenance Release 2, la création de conteneurs pour les applications mobiles n'est plus prise en charge. Cependant vous pouvez livrer sur les appareils Android les conteneurs créés dans les versions antérieures de l'application.

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 de l'appareil mobile avec Kaspersky Security Center, la distribution de l'app figurant dans le conteneur est automatiquement copiée sur l'appareil de l'utilisateur.

Pour installer des apps dans des conteneurs sur l'appareil mobile de l'utilisateur, il faut autoriser l'installation d'apps depuis des sources inconnues. Pour assurer la sécurité de l'appareil et protéger les données après l'installation d'apps dans des conteneurs, il est conseillé d'interdire l'installation d'apps depuis des sources inconnues. Pour en savoir plus sur l'installation d'apps qui ne proviennent pas de Google Play, consultez l'*aide d'Android*.

Configuration des notifications de Kaspersky Endpoint Security for Android

Si vous souhaitez que l'utilisateur de l'appareil mobile ne soit pas distrait par les notifications de Kaspersky Endpoint Security for Android, vous pouvez désactiver certaines notifications.

Kaspersky Endpoint Security utilise les outils suivants pour afficher l'état de protection des appareils :

- **Notification de l'état de protection**. Cette notification est épinglée à la barre de notifications. La notification de l'état de protection ne peut pas être supprimée. La notification affiche l'état de protection des appareils (par exemple,) et le nombre de problèmes, le cas échéant. Vous pouvez appuyer sur l'état de protection des appareils et afficher les problèmes de la liste dans l'application.

- **Notifications sur l'application**. Ces notifications informent l'utilisateur de l'appareil sur l'application (par exemple, la détection des menaces).

- **Messages contextuels**. Les messages contextuels nécessitent une action de l'utilisateur de l'appareil (par exemple, une action à effectuer en cas de menace détectée).

Toutes les notifications de Kaspersky Endpoint Security for Android sont activées par défaut.

L'utilisateur de l'appareil Android peut désactiver toutes les notifications de Kaspersky Endpoint Security for Android dans les paramètres du volet de notifications. Si les notifications sont désactivées, l'utilisateur ne contrôle pas le fonctionnement de l'application et peut ignorer des informations importantes (par exemple, sur les défaillances lors la synchronisation de l'appareil avec Kaspersky Security Center). Pour connaître l'état de fonctionnement de l'application, l'utilisateur doit ouvrir Kaspersky Endpoint Security for Android.

Pour configurer l'affichage des notifications relatives au fonctionnement de Kaspersky Endpoint Security for Android, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Avancé**.
5. Dans le groupe **Notification sur l'application**, cliquez sur **Configurer**.

   La fenêtre **Paramètres de notification sur l'appareil** s'ouvre.
6. Choisissez les problèmes de Kaspersky Endpoint Security for Android que vous souhaitez masquer sur l'appareil mobile de l'utilisateur et cliquez sur **OK**.

   Kaspersky Endpoint Security for Android n'affichera pas les problèmes dans la notification de l'état de protection et dans la section **État**. Kaspersky Endpoint Security for Android continuera à afficher les notifications de l'état de protection et les notifications sur l'application.

   Certains problèmes de Kaspersky Endpoint Security for Android sont obligatoires et il est par conséquent impossible de les désactiver (par exemple, les problèmes concernant l'expiration de la durée de la validité de la licence).
7. Pour masquer l'ensemble des notifications et des messages instantanés, sélectionnez **Désactiver les notifications et les messages contextuels lorsque l'application est en mode arrière-plan**.

   Kaspersky Endpoint Security for Android affichera uniquement la notification de l'état de protection. La notification affiche l'état de protection des appareils (par exemple,) et le nombre de problèmes. L'application affiche également des notifications lorsque l'utilisateur travaille avec l'application (l'utilisateur met à jour les bases antivirus manuellement, par exemple).

   Les experts de Kaspersky vous ont recommandé d'activer les notifications et les messages contextuels. Si vous désactivez les notifications et les messages contextuels lorsque l'application est en mode arrière-plan, l'application n'avertira pas les utilisateurs des menaces en temps réel. Les utilisateurs d'appareils mobiles ne peuvent en savoir plus sur l'état de protection de l'appareil que lorsqu'ils ouvrent l'application.
8. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center. Les notifications de Kaspersky Endpoint Security for Android que vous avez désactivées ne s'afficheront pas sur l'appareil mobile de l'utilisateur.

Connexion des appareils iOS MDM à 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. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **AirPlay**.
5. Dans le groupe **Appareil AirPlay**, cochez la case **Appliquer les paramètres à l'appareil**.
6. Dans le groupe **Mots de passe**, cliquez sur le bouton **Ajouter**.

   Une ligne vierge sera ajoutée au tableau des mots de passe.
7. Dans la colonne **Nom de l'appareil**, saisissez le nom du périphérique AirPlay sur le réseau sans fil.
8. Dans la colonne **Mot de passe**, saisissez le mot de passe du périphérique AirPlay.
9. Pour restreindre la connexion du périphérique MDM iOS aux appareil 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 appareils autorisés est laissée vide, Kaspersky Device Management for iOS autorise l'accès à tous les appareil AirPlay.
10. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

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 des appareils iOS MDM à 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. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **AirPrint**.
5. Dans le groupe **Imprimantes AirPrint**, cliquez sur le bouton **Ajouter**.
   La fenêtre **Imprimante** s'ouvre.
6. Saisissez l'adresse IP de l'imprimante AirPrint dans le champ **Adresse IP**.
7. 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 (resource path) du protocole Bonjour. Par exemple :
   - printers/Canon_MG5300_series ;
   - ipp/print ;
   - Epson_IPP_Printer.
8. Cliquez sur **OK**.
   L'imprimante AirPrint ajoutée s'affichera dans la liste.
9. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

L'utilisateur du périphérique mobile pourra ainsi imprimer des documents sur une imprimante AirPrint via une connexion sans fil une fois la stratégie appliquée.

Configuration du point d'accès (APN)

Afin de pouvoir connecter un appareil mobile aux services de transmission de données du réseau mobile, il faut configurer les paramètres APN (Access Point Name).

Configuration de l'APN sur les appareils Android (Samsung uniquement)

La configuration de l'APN n'est possible que pour les appareils Samsung.

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.

Pour configurer les paramètres du point d'accès (APN), procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Administration de Samsung KNOX → APN**.
5. Dans le groupe **APN**, cliquez sur le bouton **Configurer**.

   La fenêtre **Paramètres de l'APN** s'ouvre.
6. Sous l'onglet **Général**, indiquez les paramètres suivants pour le point d'accès :
   a. Dans la liste déroulante **Type de point d'accès**, sélectionnez le type de point d'accès.
   b. Dans le champ **Nom du point d'accès**, indiquez le nom du point d'accès.
   c. Dans le champ **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.
7. Sous l'onglet **Avancé**, configurez les paramètres avancés du point d'accès (APN) :
   a. Dans la liste déroulante **Type d'authentification**, sélectionnez le type d'autorisation de l'utilisateur de l'appareil mobile sur le serveur de l'opérateur mobile fournissant l'accès au réseau.
   b. Dans le champ **Adresse du serveur**, 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.
8. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Configuration de l'APN sur les appareils iOS MDM

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).

La section **APN** est dépassée. Il est conseillé de configurer les paramètres APN dans la section **Communication cellulaire**. Avant de configurer les paramètres de la communication cellulaire, assurez-vous que les paramètres de la section **APN** ne sont pas appliqués sur l'appareil (la case **Appliquer les paramètres à l'appareil** doit être décochée). L'utilisation simultanée des paramètres des sections **APN** et **Communication cellulaire** est impossible.

Pour configurer le point d'accès sur le périphérique iOS MDM de l'utilisateur, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Communication cellulaire**.
5. Dans le groupe **Paramètres de communication cellulaire**, cochez la case **Appliquer les paramètres à l'appareil**.
6. Dans la liste **Type APN**, sélectionnez le type de point d'accès pour la transmission de données sur un réseau mobile GPRS/3G/4G :
   - **APN intégré** : configuration des paramètres de la communication mobile pour le transfert de données via l'opérateur de téléphonie mobile qui prend en charge l'utilisation de la carte Apple SIM intégrée. Pour en savoir plus sur les appareils dotés de la carte Apple SIM intégrée, consultez le site Internet de l'assistance technique d'Apple.
   - **APN** : configuration des paramètres de la communication mobile pour la transmission de données via l'opérateur de téléphonie mobile de la carte SIM installée.
   - **APN intégré et APN** : configuration des paramètres de la communication mobile pour le transfert de données via l'opérateur de téléphonie mobile de la carte SIM insérée et de la carte Apple SIM intégrée. Pour en savoir plus sur les appareils dotés de la carte Apple SIM intégrée, consultez le site Internet de l'assistance technique d'Apple.
7. Dans le champ **Nom du point d'accès**, indiquez le nom du point d'accès.
8. Choisissez le type de l'authentification de l'utilisateur de l'appareil sur le serveur de l'opérateur mobile pour l'accès au réseau (Internet et MMS) dans la liste déroulante **Type d'authentification**.
9. Dans le champ **Nom d'utilisateur**, indiquez le nom de l'utilisateur pour l'autorisation sur le réseau mobile.
10. Dans le champ **Mot de passe**, indiquez le mot de passe pour l'autorisation de l'utilisateur sur le réseau mobile.
11. Dans le champ **Adresse du serveur proxy et port**, indiquez le nom de l'hôte, le domaine ou l'adresse IP du serveur proxy et le numéro de port du serveur proxy.

12. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

    Le point d'accès (APN) sera ainsi configuré sur le périphérique mobile de l'utilisateur une fois la stratégie appliquée.

Configuration du profil de travail Android

Cette section contient des informations sur l'utilisation du profil de travail Android.

A propos du profil de travail Android

Android Enterprise est une plateforme de gestion de l'infrastructure mobile d'entreprise qui fournit aux employés de l'entreprise un environnement professionnel pour appareils mobiles. Pour plus de détails sur l'utilisation d'Android Enterprise, visitez le site d'assistance technique de Google.

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

Configuration du profil de travail

Pour configurer les paramètres du profil de travail Android, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.

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

3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie active.

4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez le **profil de travail Android**.

5. Cochez la case **Créer un profil de travail** dans l'espace de travail **Profil de travail Android**.

6. Spécifiez les paramètres du profil de travail :

   - Pour activer le Contrôle des applications dans le profil de travail Android et le désactiver dans le profil personnel, cochez la case **Activer le Contrôle des applications sous le profil de travail uniquement**.

     Dans la section **Utilisateurs**, vous pouvez sélectionner **Contrôle des applications** et utiliser l'espace de travail pour créer des listes des applications autorisées, bloquées, recommandées et obligatoires, ainsi que des catégories d'applications autorisées et bloquées dans la section.

   - Pour activer la Protection Internet de Google Chrome dans le profil de travail et la désactiver dans le profil personnel, dans l'espace de travail de la section **Profil de travail Android,** cochez la case **Activer la**

Protection Internet sous le profil de travail uniquement.

La Protection Internet pour le navigateur Samsung Internet interdit les sites dans les profils de travail et personnels. Vous ne pouvez pas activer la Protection Internet pour le navigateur Samsung Internet uniquement dans le profil de travail. Pour utiliser la Protection Internet pour le navigateur Samsung, désactivez l'option **Activer la Protection Internet sous le profil de travail uniquement**. Si cette option est activée, la Protection Internet pour le navigateur Samsung Internet ne fonctionne pas. La Protection Internet dans le profil de travail est désactivée par défaut.

> La Protection Internet sur les appareils Android fonctionne seulement dans les navigateurs Google Chrome et Samsung Internet Browser.

Vous pouvez spécifier les paramètres d'accès aux sites Internet (créer une liste de catégories de sites Internet bloqués ou une liste de sites Internet autorisés) dans la section **Protection Internet**.

- Pour empêcher qu'un utilisateur puisse copier des données, au moyen du presse-papiers, des applications du profil de travail aux applications privées, cochez la case **Interdire le transfert de données du profil de travail vers un profil privé**.
- Pour interdire à l'utilisateur d'utiliser le mode dépannage par USB sur l'appareil mobile dans le profil de travail, cochez la case **Interdire d'activer le mode dépannage sur USB**.

  En mode débogage par USB, l'utilisateur peut par exemple télécharger une application à l'aide d'un poste de travail.
- Pour empêcher que l'utilisateur puisse installer des apps dans le profil de travail Android à partir de toutes les sources, sauf Google Play, cochez la case **Interdire l'installation de l'app sur un profil de travail à partir de sources inconnues**.
- Pour empêcher que l'utilisateur puisse supprimer des apps depuis le profil de travail Android, cochez la case **Interdire la suppression de l'app à partir d'un profil de travail**.

7. Pour configurer les paramètres du profil de travail sur le périphérique mobile de l'utilisateur, bloquez la modification des paramètres.
8. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center. L'espace du périphérique mobile de l'utilisateur sera scindé entre le profil de travail et le profil personnel.

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. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.

4. Dans la fenêtre **Propriétés** de la stratégie qui s'ouvre, sélectionnez la section **LDAP**.

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

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

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

7. 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**.

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

9. 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**.

10. Pour utiliser le protocole de transfert de données SSL afin de protéger le transfert de messages, cochez la case **Utiliser une connexion SSL**.

11. 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 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.

12. Cliquez sur **OK**.

    Le nouveau compte utilisateur LDAP s'affichera dans la liste.

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

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. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur la souris pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Calendrier**.
5. Dans le groupe **Comptes CalDAV**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Données du compte CalDAV** s'ouvre.
6. Dans le champ **Description**, saisissez la description du compte CalDAV de l'utilisateur.
7. 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.
8. 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://"`.
9. Dans le champ **Nom du compte**, indiquez le nom du compte utilisateur pour l'autorisation sur le serveur CalDAV.
10. Dans le champ **Mot de passe**, indiquez le mot de passe du compte utilisateur CalDAV pour l'autorisation sur le serveur CalDAV.
11. 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**.
12. Cliquez sur **OK**.

    Le nouveau compte utilisateur CalDAV s'affichera dans la liste.
13. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

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. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.

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

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

4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Contacts**.

5. Dans le groupe **Comptes CardDAV**, cliquez sur le bouton **Ajouter**.

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

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

7. 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.

8. 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://"`.

9. 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**.

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

11. 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**.

12. Cliquez sur **OK**.

    Le nouveau compte utilisateur CardDAV s'affichera dans la liste.

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

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 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 un calendrier, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.

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

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

4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Abonnement au calendrier**.

5. Dans le groupe **Abonnements aux calendriers**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Abonnement au calendrier** s'ouvre.

6. Saisissez une description de l'abonnement au calendrier dans le champ **Description**.

7. Dans le champ **Adresse Internet du serveur**, indiquez l'adresse Internet du calendrier de 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.

8. Dans le champ **Nom d'utilisateur**, saisissez le nom du compte utilisateur pour l'authentification sur le serveur du calendrier de tiers.

9. Dans le champ **Mot de passe**, saisissez le mot de passe de l'abonnement au calendrier pour l'authentification sur le serveur du calendrier de tiers.

10. 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**.

11. Cliquez sur **OK**.

12. Le nouvel abonnement au calendrier s'affichera dans la liste.

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

    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 appareil mobile. En cliquant sur l'icône des clips Internet sur l'écran principal du appareil, l'utilisateur peut rapidement ouvrir des sites Internet (tels que le site de l'entreprise). Vous pouvez ajouter des clips Internet sur les appareils des utilisateurs et configurer l'apparence de l'icône du raccourci affichée sur l'écran.

Par défaut, les restrictions suivantes s'appliquent à l'utilisation des clips Internet :

- L'utilisateur ne peut pas supprimer lui-même les clips Internet du appareil 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 appareil iOS MDM de l'utilisateur, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.

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

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

4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Clips Internet**.

5. Dans le groupe **Clips Internet**, cliquez sur le bouton **Ajouter**.

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

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

7. 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://"`.

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

9. 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 appareil iOS MDM. L'image doit remplir les conditions suivantes :

   - taille de 400 x 400 pixels maximum ;
   - format de fichier GIF, JPEG ou PNG ;
   - taille du fichier de 1 Mo maximum.

   Vous pouvez accéder à un aperçu de l'icône du clip Internet dans le champ **Identification**. Si vous ne sélectionnez pas d'image pour le clip Internet, l'icône apparaîtra sous la forme d'un carré blanc.

   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 effets visuels**.

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

11. Cliquez sur **OK**.

    Le nouveau clip Internet s'affichera dans la liste.

12. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

Les icônes des clips Internet seront ainsi ajoutés à l'écran principal du appareil 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. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils MDM iOS.

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

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

4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Polices**.

5. Dans le groupe **Polices**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Police** s'ouvre.

6. 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.

7. Cliquez sur le bouton **Ouvrir**.

   La nouvelle police s'affichera dans la liste.

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

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.

Gestion de l'application à l'aide de systèmes EMM tiers (Android uniquement)

Vous pouvez utiliser l'application Kaspersky Endpoint Security for Android sans les systèmes d'administration de Kaspersky. Utilisez les solutions d'autres fournisseurs de services EMM (Enterprise Mobility Management) pour déployer et gérer l'application Kaspersky Endpoint Security for Android. Pour garantir le fonctionnement de l'application avec les solutions EMM tierces, Kaspersky participe à AppConfig Community.

L'administration de l'application Kaspersky Endpoint Security for Android via les solutions EMM tierces est accessible seulement sur les appareils fonctionnant sous Android.

Vous pouvez utiliser les solutions EMM tierces pour déployer l'application Kaspersky Endpoint Security for Android uniquement. Connectez l'appareil à Kaspersky Security Center et gérez l'application dans la Console d'administration. Dans ce cas, la gestion de l'application Kaspersky Endpoint Security for Android dans la console EMM ne sera pas disponible.

Si vous avez déployé l'application Kaspersky Endpoint Security for Android en utilisant le système EMM tiers, il est impossible de gérer l'application dans Kaspersky Endpoint Security Cloud. Vous pouvez gérer l'application Kaspersky Endpoint Security for Android dans la console EMM.

Les solutions EMM suivantes prennent en charge l'utilisation de l'application Kaspersky Endpoint Security for Android :

- VMware AirWatch
- MobileIron
- IBM Maas360
- Microsoft Intune
- SOTI MobiControl

Dans la console EMM, vous pouvez exécuter les actions suivantes :

- Déployer l'app dans le profil de travail Android sur les appareils des utilisateurs.
- Activer l'application.
- Configurer les paramètres de l'application :
  - Activer la protection contre les sites Internet malveillants et les sites Internet de phishing ;
  - configurer les paramètres de connexion de l'appareil à Kaspersky Security Center ;
  - configurer les paramètres de l'Antivirus ;
  - configurer le calendrier du lancement de la recherche de virus sur l'appareil ;
  - activer la détection d'applications publicitaires et d'applications que les individus malintentionnés peuvent utiliser pour nuire à l'appareil et aux données de l'utilisateur ;
  - configurer la programmation de la mise à jour des bases de l'app.

Guide de démarrage

Pour le déploiement de l'application sur les appareils mobiles des utilisateurs, Kaspersky Endpoint Security for Android doit être ajouté à la boutique des applications EMM. Vous pouvez ajouter Kaspersky Endpoint Security for Android à la boutique des applications EMM à l'aide du lien vers Google Play. Pour plus de détails sur l'utilisation des applications dans la console EMM, cf. *site du Support Technique du fournisseur de services EMM*.

L'app Kaspersky Endpoint Security for Android se déploie dans le profil de travail Android. L'application est isolée des données personnelles de l'utilisateur et protège seulement les données d'entreprise dans le profil de travail. Il est recommandé d'assurer la protection de Kaspersky Endpoint Security for Android contre la suppression à l'aide de la console EMM.

Comment installer l'application

En fonction de la console EMM, choisissez le moyen d'installation de l'application sur les appareils : installation en mode silencieux, envoi d'un message électronique avec un lien vers l'application dans Google Play ou autre moyen accessible.

Les autorisations suivantes sont nécessaires pour que l'application fonctionne :

- Autorisation "Stockage" pour accéder aux fichiers lorsque l'Antivirus est en cours d'exécution (uniquement pour Android 6.0 et version suivante).
- Autorisation "Téléphone" pour identifier l'appareil, par exemple lors de l'activation d'une application.
- Demande d'ajout de Kaspersky Endpoint Security for Android à la liste des applications lancées au démarrage du système d'exploitation (sur certains appareils Huawei, Meizu et Xiaomi). Si la demande d'ajout ne s'affiche pas, ajoutez manuellement Kaspersky Endpoint Security for Android à la liste des applications de lancement automatique. La demande peut ne pas s'afficher si l'application Sécurité n'est pas installée dans le profil de travail.

Vous pouvez accorder les autorisations requises dans la Console EMM avant de déployer l'application Kaspersky Endpoint Security for Android. Pour plus de détails sur l'octroi des autorisations dans la Console EMM, cf. *site du Support Technique du fournisseur de services EMM*. Vous pouvez également accorder les autorisations tout en exécutant l'Assistant de configuration initiale de Kaspersky Endpoint Security for Android sur l'appareil.

L'app Kaspersky Endpoint Security for Android sera installée dans le profil de travail Android.

Pour le fonctionnement de la protection Internet le serveur proxy doit encore être configuré dans les paramètres de Google Chrome :

- Mode de configuration du serveur proxy : manuel.
- Adresse et port du serveur proxy : 127.0.0.1:3128.
- Prise en charge du protocole SPDY : désactivée.
- Compression des données via le serveur proxy : désactivée.

Comment activer l'application

Les informations sur la licence sont transférées à l'appareil mobile avec les autres paramètres dans le fichier de configuration.

Si l'activation de l'application n'est pas effectuée dans un délai de 30 jours à compter de l'installation sur l'appareil mobile, la durée de validité de la licence d'essai expire. Une fois que la licence d'évaluation de l'app mobile Kaspersky Endpoint Security arrive à échéance, toutes les fonctions de l'app Kaspersky Endpoint Security for Android sont désactivées.

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 for Android n'est pas disponible). Pour pouvoir continuer à bénéficier de toutes les fonctionnalités de l'app, vous devez renouveler la licence commerciale.

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

1. Dans la console EMM, ouvrez les paramètres de l'application Kaspersky Endpoint Security for Android.
2. Dans le champ du paramètre `LicenseActivationCode`, saisissez le code d'activation de l'application.

   L'activation de l'application sur l'appareil nécessite l'accès aux serveurs d'activation de Kaspersky.

Connexion de l'appareil à Kaspersky Security Center

Après avoir installé l'application Kaspersky Endpoint Security for Android sur votre appareil mobile, vous pouvez connecter votre appareil à Kaspersky Security Center. Les données permettant de connecter l'appareil à Kaspersky Security Center sont transférées vers l'appareil mobile avec les autres paramètres répertoriés dans le fichier de configuration. Une fois l'appareil connecté à Kaspersky Security Center, vous pouvez configurer de manière centralisée les paramètres de l'application à l'aide des stratégies de groupe. Vous pouvez également recevoir des rapports et des statistiques sur l'application Kaspersky Endpoint Security for Android.

Avant de connecter des appareils à Kaspersky Security Center, assurez-vous que les conditions suivantes sont remplies :

- Le plug-in d'administration de Kaspersky Endpoint Security for Android est installé sur le poste de travail de l'administrateur.
- Dans les propriétés du Serveur d'administration , le port de connexion des appareils mobiles est ouvert.
- Dans la Console d'administration, l'affichage du dossier **Administration des appareils mobiles** est activé.
- Dans le stockage des certificats de Kaspersky Security Center, un certificat commun a été créé pour identifier l'utilisateur de l'appareil mobile.

Avant de connecter des appareils à Kaspersky Security Center, il est recommandé d'effectuer les actions suivantes :

- Si vous souhaitez créer des tâches et des stratégies pour les appareils mobiles, créez un groupe d'administration séparé pour appareils mobiles.
- Si vous souhaitez déplacer automatiquement des appareils mobiles dans un groupe d'administration séparé, créez une règle de transfert automatique des appareils à partir du dossier **Appareils non définis**.
- Si vous souhaitez configurer les paramètres de l'application Kaspersky Endpoint Security for Android de manière centralisée, créez une stratégie de groupe.

Pour synchroniser l'appareil avec Kaspersky Security Center, procédez comme suit :

1. Dans la console EMM, ouvrez les paramètres de l'application Kaspersky Endpoint Security for Android.
2. Dans le champ du paramètre `KscServer`, saisissez le nom DNS ou l'adresse IP du Serveur d'administration de Kaspersky Security Center. Le port par défaut est 13292.
3. Si vous souhaitez que l'utilisateur de l'appareil mobile ne soit pas distrait par les notifications de Kaspersky Endpoint Security for Android, désactivez les notifications de l'application. Pour ce faire, réglez le paramètre comme suit `DisableNotification = True`.

   Une fois connectée, l'application affiche toutes les notifications. Vous pouvez désactiver certaines notifications de l'application dans les paramètres de la stratégie.

   Ne désactivez pas les notifications sur le fonctionnement des applications si vous n'utilisez pas Kaspersky Security Center. Par exemple, il se peut que l'utilisateur ne soit pas averti lorsque la licence expire. Ainsi, l'application cesse d'exécuter toutes ses fonctions.

Après avoir configuré les paramètres de connexion, l'application Kaspersky Endpoint Security for Android affichera une notification demandant les autorisations et les privilèges supplémentaires suivants :

- Autorisation "Caméra" pour utiliser l'Antivol (commande **Photographier**).
- Autorisation "Localisation" pour utiliser l'Antivol (commande **Géolocaliser l'appareil**).
- Privilèges de l'administrateur de l'appareil (titulaire du profil de travail Android) pour utiliser les fonctions suivantes de l'application :
  - Installation des certificats de sécurité.
  - Configuration Wi-Fi.
  - Configuration Exchange ActiveSync.

- Restriction de l'utilisation de la caméra, Bluetooth, Wi-Fi.

> En raison de la nature du profil de travail Android (absence du service Fonctions d'accessibilité), le Contrôle des applications et l'Antivol ne sont pas disponibles dans l'application.

Lorsque l'utilisateur accorde les autorisations et privilèges nécessaires, l'appareil se connecte à Kaspersky Security Center. Si la règle de transfert automatique des appareils dans le groupe d'administration n'est pas créée, l'appareil est automatiquement ajouté dans le dossier **Appareils non définis**. Si la règle de transfert automatique des appareils dans le groupe d'administration est créée, l'appareil est automatiquement ajouté dans le dossier indiqué.

Kaspersky Endpoint Security fournit le format suivant pour le nom de l'appareil :

- Modèle d'appareil [email, identifiant de l'appareil] ;
- Modèle d'appareil [Email (le cas échéant) ou identifiant de l'appareil].

Un identifiant de l'appareil est un identifiant unique généré par Kaspersky Endpoint Security for Android à partir des données reçues de l'appareil. Pour les appareils mobiles tournant sous Android 10 et suivants, Kaspersky Endpoint Security for Android utilise le SSAID (identifiant Android) ou la somme de contrôle des autres données reçues de l'appareil. Pour les versions précédentes d'Android, l'application utilise l'IMEI. Vous pouvez configurer le format du nom de l'appareil dans la stratégie de groupe. Vous pouvez également ajouter un tag au nom de l'appareil. Cela facilite la recherche et le tri des appareils dans Kaspersky Security Center. Ce tag est disponible uniquement pour VMware AirWatch.

Pour ajouter le tag au nom de l'appareil :

1. Dans la console EMM, ouvrez les paramètres de l'application Kaspersky Endpoint Security for Android.
2. Dans le champ `KscDeviceNameTag`, sélectionnez les valeurs :
   - `{DeviceSerialNumber}` : numéro de série de l'appareil.
   - `{DeviceUid}` : identifiant unique de l'appareil (UDID).
   - `{DeviceAssetNumber}` : numéro de ressource de l'appareil. Ce numéro est créé en interne au sein de votre organisation.

> Nous vous recommandons d'utiliser uniquement ces valeurs. VMware AirWatch prend en charge les autres valeurs, mais Kaspersky Endpoint Security ne peut pas garantir leur compatibilité.

Vous pouvez ajouter des valeurs (par exemple, `{DeviceSerialNumber} {DeviceUid}`). Le tag sera ajouté au nom d'appareil dans Kaspersky Security Center. Un espace sépare le tag et le nom d'appareil. Par exemple, si l'appareil a pour nom `Google Pixel 2 a10c6b75f7b31de9 22:7D:78:9E:C5:1E`, alors le tag d'UDID est `22:7D:78:9E:C5:1E`. Si vous utilisez Kaspersky Security Center et VMwareAirWatch, le tag vous permet d'identifier des appareils dans les deux consoles. Pour mettre l'appareil en correspondance, sélectionnez les mêmes valeurs pour son nom (par exemple, son numéro de série).

Une fois l'appareil connecté à Kaspersky Security Center, les paramètres de l'application seront modifiés en fonction de la stratégie du groupe. Kaspersky Endpoint Security for Android ignore les paramètres de l'application du fichier de configuration configuré dans la console EMM. Toutes les sections de la stratégies peuvent être configurées sauf les sections suivantes :

- **Antivol** (Verrouillage de l'appareil) ;

- **Conteneurs ;**
- **Contrôle de l'appareil** (Verrouillage de l'écran) ;
- **Contrôle des applications** (Verrouillage des applications interdites) ;
- **Profil de travail Android ;**
- **Administration de Samsung KNOX.**

En raison de la façon dont le profil de travail est déployé, il n'est pas possible d'appliquer les paramètres de la stratégie de groupe à partir du **Profil de travail Android**. Ces paramètres ne peuvent être appliqués que si le profil de travail est créé à l'aide de Kaspersky Security Center.

Fichier AppConfig

Pour la configuration de l'application dans une console EMM, un fichier de configuration est constitué. Les paramètres de l'application dans le fichier de configuration sont présentés dans le tableau ci-après.

Paramètres du fichier de configuration

Clé de configuration	Description	Type	Valeur
`LicenseActivationCode`	Code d'activation de l'application	String	Code d'activation de l'application constitué de 20 caractères alphanumériques (alphabet latin). Pour activer l'application à l'aide de ce code d'activation, il faut un accès Internet pour se connecter aux serveurs d'activation de Kaspersky. Si vous laissez le champ vide, l'application sera activée selon la licence essai. La licence d'essai a une durée de validité de 30 jours. Une fois que la licence d'essai de l'app mobile Kaspersky Endpoint Security arrive à échéance, toutes les fonctions de l'app Kaspersky Endpoint Security for Android sont désactivées. Pour continuer à utiliser l'app, vous devez acheter une licence commerciale.
`EulaAcceptanceConfirmationV1`	<Lien vers le contrat de licence>	Choice	Ce paramètre est disponible uniquement pour VMware AirWatch. `Accepted` - Je confirme que j'ai lu, que je comprends et que j'accepte l'ensemble des conditions de ce Contrat de licence utilisateur final

			`Declined` - Je n'accepte pas les termes et conditions de ce Contrat de licence utilisateur final (CLUF). L'acceptation des termes et conditions du Contrat de licence utilisateur final (CLUF) pour tous les appareils mobiles nécessite un accès Internet pour la connexion aux serveurs Kaspersky. Si vous choisissez `Declined`, l'app demande à l'utilisateur d'accepter les termes et conditions du Contrat de licence utilisateur final (CLUF). Les utilisateur d'appareils mobiles peuvent accepter les termes et conditions dans l'Assistant de configuration initiale.
`EulaAcceptanceCodeV1`	Code de contrat de licence	String	Ces paramètres sont disponibles uniquement pour VMware AirWatch. Utilisez `EulaAcceptanceCodeV1` si vous souhaitez accepter un seul contrat de licence utilisateur final (CLUF). Utilisez `EulaAcceptanceCodesV2` si vous souhaitez accepter plusieurs CLUF en même temps. Le champ `EulaAcceptanceCodesV2` doit contenir une liste de codes CLUF séparés par des points-virgules : `"<EULAid1>;<EULAid2>;<EULAid3>;..."`. Le code de contrat de licence est contenu dans le Contrat de licence utilisateur final. *Pour connaître le code de contrat de licence :* 1. Copiez le lien de contrat de licence (`EulaAcceptanceConfirmationV1`) depuis la console EMM. 2. Collez le lien dans le navigateur. Le Contrat de licence utilisateur final (CLUF) s'ouvre. 3. Lisez les conditions de ce Contrat de licence utilisateur final (CLUF) et trouvez le code de contrat de licence. L'acceptation des termes et conditions des Contrats de licence utilisateur final (CLUF) pour tous les appareils mobiles nécessite un accès Internet pour la connexion aux serveurs Kaspersky.
`EulaAcceptanceCodesV2`	Codes du Contrat de licence	String	

			Si vous laissez ces champs vides, l'application demande à l'utilisateur d'accepter les termes et conditions des Contrats de licence utilisateur final (CLUF). L'utilisateur de l'appareil mobile peut accepter les conditions dans l'assistant de configuration initiale. Si vous spécifiez les valeurs des deux champs, les conditions générales de tou les CLUF qui y sont spécifiés seront acceptées.
`KscServer`	Adresse et port du Serveur d'administration de Kaspersky Security Center	String	Nom DNS ou adresse IP du Serveur d'administration de Kaspersky Security Center et numéro de port. Saisissez l'adresse comme suit : `<adresse du serveur>:<port>`. Si vous avez saisi l'adresse de serveur sans préciser le port, l'application utilise le port par défaut 13292.
`DisableNotification`	Désactiver les notifications de l'application avant la connexion à Kaspersky Security Center	Boolean	`True` : Kaspersky Endpoint Security for Android masque toutes les notifications concernant le fonctionnement de l'application. L'application Kaspersky Endpoint Security for Android masque les notifications avant de connecter l'appareil à Kaspersky Security Center. Une fois connectée, l'application affiche toutes les notifications. Vous pouvez désactiver certaines notifications de l'application dans les paramètres de la stratégie. Ne désactivez pas les notifications sur le fonctionnement des applications si vous n'utilisez pas Kaspersky Security Center. Par exemple, il se peut que l'utilisateur ne reçoive pas de notifications sur une expiration de la licence. Dans ce cas, l'application arrête d'effectuer ses fonctions. `False` : l'application Kaspersky Endpoint Security for Android affiche toutes les notifications concernant le fonctionnement de l'application.
`ScanScheduleType`	Mode de lancement de l'analyse	Choice	`AfterUpdate` : lancement d'une recherche de virus après une mise à jour des bases de données. L'application met à jour les bases antivirus de manière programmée `(UpdateScheduleType)`.

			`Daily` : lancement d'une recherche de virus une fois par jour. Configurez l'heure de lancement de l'analyse (`ScanScheduleTime`). `Weekly` : lancement d'une recherche de virus une fois par semaine. Choisissez le jour de la semaine du lancement de la recherche de virus (`ScanScheduleDay`) et configurez l'heure (`ScanScheduleTime`). `Off` : le lancement automatique d'une recherche de virus est désactivé. Quelle que soit la valeur du paramètre, l'utilisateur de l'appareil peut lancer la recherche de virus à la main.
`ScanScheduleDay`	Jour du lancement de l'analyse	Choice	`Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday` Vous pouvez choisir une seule valeur de paramètre.
`ScanScheduleTime`	Heure du lancement de l'analyse	String	Heure au format 24 heures (par exemple 13:00) ou 12 heures (par exemple, 10:30 pm).
`ScanScheduleLock`	Interdire la configuration du mode d'exécution de l'analyse	Boolean	`True` : les paramètres du mode de lancement de la recherche de virus sont inaccessibles pour l'utilisateur dans les paramètres de l'application. `False` : l'utilisateur peut configurer le mode de lancement de la recherche de virus et, par exemple, désactiver le lancement automatique de la recherche de virus.
`ScanOnlyExecutableFiles`	Types des fichiers pour l'analyse (recherche de virus)	Choice	`AllFiles` : analyse de tous les fichiers. `OnlyExecutables` : analyse des fichiers exécutables uniquement. Les fichiers avec l'extension .apk (.zip), .dex ou .so sont des fichiers exécutables. Dans Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 1, il est impossible d'activer uniquement l'analyse des fichiers exécutables.
`ScanArchives`	Analyser les archives avec dépaquetage	Boolean	`True` : l'application décompresse les archives et analyse leur contenu. `False` : l'application analyse seulement les fichiers d'archives. L'application analyse seulement les archives avec l'extension .zip (.apk). Dans Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 1, il est impossible de désactiver l'analyse du contenu des archives.

`ScanActionOnThreatFound`	Action lors de la détection d'une menace (recherche de virus)	Choice	`Quarantine` : l'application place les objets détectés en quarantaine. 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. `Delete` : l'application supprime les objets détectés. `Skip` : l'application laisse les objets détectés sans modifications. Si des objets détectés ont été ignorés, Kaspersky Endpoint Security for Androi avertit l'utilisateur de la présence de problèmes dans la protection de l'appareil. Les requêtes envoyées à l'obje sur l'appareil (par exemple, tentative de copie ou d'ouverture) seront bloquées par l'application. `AskUser` : l'application propose à l'utilisateur de choisir l'action pour chaque objet détecté : ignorer, placer en quarantaine ou supprimer. En cas de détection de plusieurs objets, l'utilisateu peut appliquer l'action choisie à tous les objets. L'application inscrit des informations sur les menaces détectées et les actions exécutées dans les rapports de l'application.
`ScanLock`	Interdire la configuration des paramètres d'analyse	Boolean	`True` : les paramètres d'analyse sont inaccessibles pour l'utilisateur dans les paramètres de l'application : type des fichiers pour l'analyse, analyse des archives, action à effectuer en cas de détection d'une menace. `False` : l'utilisateur peut configurer les paramètres d'analyse et, par exemple, choisir l'action `Skip` en cas de détectio de menaces.
`ScanAndProtectionAdwareRiskware`	Bloquez les applications publicitaires, les numéroteurs automatiques et les applications susceptibles d'être utilisés par des criminels pour nuire à l'appareil et aux données de l'utilisateur	Boolean	`True` : l'application détecte les applications publicitaires et les applications que des individus malintentionnés peuvent utiliser pour nuire à l'appareil ou aux données personnelles de l'utilisateur. `False` : l'application ignore les applications publicitaires et d'applications que des individus malintentionnés peuvent utiliser pour nuire à l'appareil ou aux données personnelles de l'utilisateur.
`ProtectionMode`	Mode de	Choice	`Recommended` : l'application analyse

	protection en temps réel.		seulement les nouvelles applications une fois, juste après leur installation, ainsi que les fichiers du dossier Téléchargements. `Extended` (Étendu) : l'application analyse tous les fichiers, que l'utilisateur ouvre, modifie, copie, lance et enregistre sur l'appareil. En outre, l'application analyse les nouvelles applications et les nouveaux fichiers du dossier Téléchargements. `Disabled` : la protection en temps réel est désactivée.
`UseKsnMode`	Mode de Kaspersky Security Network	Choice	`Recommended` : l'application échange des données avec Kaspersky Security Network (KSN). Kaspersky Endpoint Security for Android utilise KSN pour la protection en temps réel de l'appareil contre les menaces (protection cloud) e pour le fonctionnement de la protection Internet dans Internet. `Extended` : l'application échange des données avec Kaspersky Security Network et envoie en plus au laboratoire de recherche sur les virus des statistiques définies sur les performances de Kaspersky Endpoint Security for Android. Ces informations permet de suivre les menaces en temps réel. Les services KSN ne collectent, ne traitent et ne conservent aucune donnée personnelle de l'utilisateur. `Disabled` (Désactivé) : l'application n'utilise pas les données de Kaspersky Security Network. Il est impossible d'activer la protection Internet (`EnableWebFilter`). Le composant Protection cloud est inaccessible pour l'Antivirus.
`ProtectScanOnlyExecutableFiles`	Types des fichiers pour l'analyse (protection en temps réel)	Boolean	`AllFiles` : analyse de tous les fichiers. `OnlyExecutables` : analyse des fichiers exécutables uniquement. Les fichiers avec l'extension .apk (.zip), .dex ou .so sont des fichiers exécutables. Dans Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 1, il est impossible d'activer uniquement l'analyse des fichiers exécutables.
`ProtectionActionOnThreatFound`	Action en cas de détection d'une menace (protection en temps réel)	Choice	`Quarantine` : l'application place les objets détectés en quarantaine. 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. `Delete` : l'application supprime les objets détectés. `Skip` : l'application laisse les objets détectés sans modifications. Si des objets détectés ont été ignorés, Kaspersky Endpoint Security for Androi avertit l'utilisateur de la présence de problèmes dans la protection de l'appareil. Les requêtes envoyées à l'obje sur l'appareil (par exemple, tentative de copie ou d'ouverture) sont bloquées par l'application. L'application inscrit des informations sur les menaces détectées et les actions exécutées dans les rapports de l'application.
`ProtectionLock`	Interdire la configuration des paramètres de protection en temps réel	Boolean	`True` : les paramètres de protection en temps réel sont inaccessibles pour l'utilisateur dans les paramètres de l'application : mode de protection en temps réel, type des fichiers pour l'analyse et action à effectuer en cas de détection d'une menace. `False` : l'utilisateur peut configurer les paramètres de protection en temps réel et, par exemple, choisir l'action `Skip` en cas de détection de menaces.
`UpdateScheduleType`	Mode d'exécution de la mise à jour des bases de données	Choice	`Daily` : vérification de la présence de nouvelles bases antivirus et téléchargement de celles-ci sur les appareils une fois par jour. Configurez l'heure de lancement de la mise à jour des bases de données (`UpdateScheduleTime`). `Weekly` : vérification de la présence de nouvelles bases antivirus et téléchargement de celles-ci sur les appareils une fois par semaine. Choisissez le jour de la semaine du lancement de la mise à jour des bases de données (`UpdateScheduleDay`) et configurez l'heure (`UpdateScheduleTime`). `Off` : la mise à jour automatique des bases antivirus est désactivée. L'utilisateur de l'appareil peut lancer manuellement la mise à jour des bases antivirus quelle que soit la valeur du paramètre.
`UpdateScheduleDay`	Jour du lancement de la mise à jour des	Choice	`Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday`

	bases de données		Vous pouvez choisir une seule valeur de paramètre.
`UpdateScheduleTime`	Heure du lancement de la mise à jour des bases de données	String	Heure au format 24 heures (par exemple 13:00) ou 12 heures (par exemple, 10:30 pm).
`UpdateScheduleLock`	Interdire la configuration du mode de lancement de la mise à jour des bases de données	Boolean	`True` : les paramètres du mode d'exécution de la mise à jour des bases de données sont inaccessibles pour l'utilisateur dans les paramètres de l'application. `False` : l'utilisateur peut configurer le mode de lancement de la mise à jour des bases de données et, par exemple, désactiver le lancement automatique de la mise à jour des bases antivirus.
`AllowUpdateInRoaming`	Mettre à jour les bases dans le roaming	Boolean	`True` : l'application télécharge les bases antivirus si l'appareil se trouve dans la zone d'itinérance. L'application charge le bases antivirus selon le programme établi `(UpdateScheduleType)`. `False` : l'application télécharge les bases antivirus seulement si l'appareil se trouve chez un particulier.
`EnableWebFilter`	Protection Internet	Boolean	`True` : l'application bloque les sites Internet malveillants et les sites Internet de phishing dans Internet à l'aide du composant Protection Internet. La Protection Internet fonctionne seulement dans Google Chrome. Les sites Internet malveillants et les sites Internet de phishing qui utilisent le protocole HTTPS peuvent rester déverrouillés si le domaine est un domaine de confiance. Si le domaine n'est pas un domaine de confiance, la Protection Internet bloque les sites Internet malveillants et de phishing. `False` : la protection contre les sites Internet malveillants et les sites Internet de phishing est désactivée. Pour le fonctionnement de la protection Internet, les conditions suivantes doiven être remplies : • Les utilisateurs de l'appareil acceptent la Politique de confidentialité et la déclaration de Protection Internet dans l'Assistant

			de configuration initiale ou dans les paramètres de l'application. • Dans les paramètres du navigateur, le serveur proxy est configuré : `ProxyMode = "fixed_servers" ProxyServer = "127.0.0.1:3128" DisableSpdy = true DataCompressionProxyEnabled = false` La configuration du serveur proxy peut varié en fonction de la version de Google Chrome. Pour plus de détails sur la configuration de Google Chrome, consultez le site Internet du projet Chromium. Après la suppression de l'application Kaspersky Endpoint Security for Android de l'appareil mobile, supprimez les paramètres du serveur proxy. • L'utilisation de KSN est activée dans les paramètres de l'application : `UseKsnMode = Recommended` ou `UseKsnMode = Extended`. • Dans les paramètres du système d'exploitation il est recommandé de choisir Google Chrome comme navigateur par défaut.
`EnableWebFilterLock`	Interdire la configuration de la Protection Internet	Boolean	`True` : les paramètres de la Protection Internet sont inaccessibles pour l'utilisateur dans les paramètres de l'application. `False` : l'utilisateur peut configurer les paramètres de la Protection Internet et, par exemple, désactiver la protection contre les sites Internet malveillants et les sites Internet de phishing dans Internet.
`UpdateServer`	Adresse du serveur source de mise à jour des bases de données	String	Adresse du serveur source de mise à jour des bases de données, par exemple, `http://update.server.com`. Si le champ reste vide, Kaspersky Endpoint Security for Android utilise les serveurs de mise à jour des bases de données de Kaspersky.
`AllowGoogleAnalytics`	Envoyer des données aux services Google Analytics pour Firebase,	Boolean	`True` : l'application transfère automatiquement les données sur le fonctionnement de Kaspersky Endpoint Security for Android aux services Google Analytics pour Firebase, SafetyNet Attestation, Firebase

	SafetyNet Attestation, Firebase Performance Monitoring et Crashlytics		Performance Monitoring et Crashlytics. Les données sont nécessaires à l'amélioration de la qualité du fonctionnement de l'application et à l'analyse de la satisfaction des utilisateurs. Les données sont transmises aux services Google Analytics pour Firebase, SafetyNet Attestation, Firebase Performance Monitoring et Crashlytics via une connexion sécurisée. L'accès aux données et la protection de celles-ci sont réglementés par les conditions d'utilisation des services Google Analytics pour Firebase, SafetyNet Attestation, Firebase Performance Monitoring et Crashlytics. `False` : la soumission des données aux services Google Analytics pour Firebase SafetyNet Attestation, Firebase Performance Monitoring et Crashlytics est désactivée.
`KscDeviceNameTag`	Tag de nom d'appareil pour Kaspersky Security Center	String	Ce paramètre est disponible uniquement pour VMware AirWatch. Le tag sera ajouté au nom d'appareil dans Kaspersky Security Center. Un espace sépare le tag et le nom d'appareil. Cela facilite la recherche et le tri des appareils dans Kaspersky Security Center. • `{DeviceSerialNumber}` : numéro de série de l'appareil. • `{DeviceUid}` : identifiant unique de l'appareil (UDID). • `{DeviceAssetNumber}` : numéro de ressource de l'appareil. Ce numéro est créé en interne au sein de votre organisation. Vous pouvez ajouter des valeurs (par exemple, `{DeviceSerialNumber}` `{DeviceUid}`). Nous vous recommandons d'utiliser uniquement ces valeurs. VMware AirWatch prend en charge les autres valeurs, mais Kaspersky Endpoint Security ne peut pas garantir leur compatibilité.

`KscGroup`	Nom du groupe d'appareils	String	Vous pouvez spécifier des groupes d'appareils dans une console EMM. Lorsqu'un appareil est connecté à Kaspersky Security Center, il est automatiquement ajouté à un sous-dossier du dossier Appareils non définis. Le nom du sous-dossier correspondra au nom du groupe spécifié dans ce paramètre. Vous pouvez ensuite créer des règles pour déplacer automatiquement les appareils des sous-dossiers du dossier Appareils non définis vers les groupes d'administration du dossier Appareils administrés. Si vous laissez le champ vide, l'appareil sera automatiquement ajouté à la racine du dossier Appareils non définis.
`KscCorporateEmail`	Messagerie professionnelle de l'utilisateur	String	Vous pouvez spécifier les adresses emai des utilisateurs dans une console EMM. Ces emails s'afficheront dans Kaspersky Security Center. La chaîne doit être une adresse email valide. Les autres valeurs sont ignorées.

Charge sur le réseau

Cette section contient des informations sur le volume du trafic réseau qu'échangent entre eux-mêmes les appareils mobiles et Kaspersky Security Center lors du fonctionnement.

Débit du trafic

Tâche	Trafic sortant	Trafic entrant	Trafic général
Déploiement initial de l'application, Mo	0.08	17.76	17.84
Mise à jour initiale des bases antivirus (le volume du trafic peut varier à cause de la taille des bases antivirus), Mo	0.04	2.21	2.25
Synchronisation de l'appareil mobile avec Kaspersky Security Center, Mo	0.03	0.02	0.05
Mise à jour régulière des bases antivirus (le volume du trafic peut varier à cause de la taille des bases antivirus), Mo	0.08	3.06	3.14
Exécution des commandes d'Antivol. Géolocaliser (le volume du trafic peut varier à cause des caractéristiques de l'appareil-photo intégré et de la qualité des images), Mo	0.09	0.8	0.17
Exécution des commandes d'Antivol. Prise de photos, Mo	1.0	0.02	1.02
Exécution des commandes d'Antivol. Verrouillage de l'appareil, Mo	0.06	0.05	0.11
Volume moyen par jour, Mo	0.22	6.96	7.18

Participation au Kaspersky Security Network

Pour renforcer l'efficacité de la protection des périphériques mobiles, Kaspersky Endpoint Security for Android utilise des données acquises 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 sur la réputation des fichiers, des ressources Internet et du logiciel. L'utilisation des données de Kaspersky Security Network permet aux applications de Kaspersky 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 d'acquérir 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. 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 sont obtenues lors du fonctionnement de Kaspersky Endpoint Security for Android sur l'ordinateur de l'utilisateur sont envoyées automatiquement à Kaspersky. 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 pour une analyse complémentaire.

Pour le fonctionnement de Kaspersky Endpoint Security for Android, l'utilisation de Kaspersky Security Network est obligatoire. KSN est utilisé pour le fonctionnement des composants fondamentaux de l'application : Antivirus, Protection Internet et Contrôle des applications. Le refus de la participation à KSN réduit le niveau de protection du périphérique, ce qui peut amener à l'infection du périphérique et à la perte des informations. Afin de pouvoir utiliser Kaspersky Security Network, vous devez accepter les conditions du Contrat de licence utilisateur final lors de l'utilisation de l'application. Le Contrat de licence utilisateur final présente les types de données que Kaspersky Endpoint Security for Android transmet à Kaspersky Security Network.

Pour améliorer le fonctionnement de l'application, vous pouvez en plus expédier à Kaspersky Security Network les données statistiques. La participation à Kaspersky Security Network pour le traitement des données statistiques 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 suspendre votre participation à Kaspersky Security Network à tout moment. La Déclaration de Kaspersky Security Network présente les types de données que Kaspersky Endpoint Security for Android transmet au Kaspersky Security Network.

Échange d'informations avec Kaspersky Security Network

Pour augmenter le niveau de protection rapide, Kaspersky Security for Mobile utilise le service cloud du Kaspersky Security Network pour les composants suivants :

- **Anti-Virus.** L'application a accès à la base opérationnelle de connaissances de Kaspersky sur la réputation des fichiers et des applications. L'analyse est effectuée sur les menaces dont les informations ne figurent pas encore dans les bases antivirus mais se trouvent déjà dans KSN. Le service cloud de Kaspersky Security Network assure le bon fonctionnement de l'Antivirus et réduit la probabilité de faux positifs.

- **Protection Internet.** L'application exécute une analyse des sites Internet avant leur ouverture en tenant compte des données reçues de la part de KSN. L'application définit aussi la catégorie du site Internet pour le contrôle de l'accès des utilisateurs au réseau Internet sur la base des listes de catégories autorisées et interdites (par exemple, la catégorie "Communication via Internet").

- **Contrôle des applications.** L'application définit la catégorie de l'application pour la restriction du lancement de l'application qui ne satisfait pas aux exigences de sécurité de l'entreprise, à partir des listes de catégories

autorisées et interdites (par exemple, catégorie "Jeux").

Le Contrat de licence utilisateur final détaille la nature des données transmises à Kaspersky lorsque le KSN est utilisé parallèlement Anti-Virus et Contrôle des applications. En acceptant les termes du Contrat de licence, vous consentez à transmettre les informations suivantes.

Les informations sur le type de données soumises à Kaspersky lors de l'utilisation de KSN pendant le fonctionnement de la Protection Internet sont disponibles dans la Déclaration concernant le traitement des données pour la Protection Internet. En acceptant les termes de la Déclaration, vous consentez à transmettre les informations suivantes.

Afin de détecter les menaces nouvelles et difficiles à détecter pour la sécurité de l'information et leurs sources, les menaces d'intrusion, ainsi que pour augmenter le niveau de protection des informations conservées et traitées sur l'appareil, vous pouvez étendre la participation au KSN.

Afin de pouvoir échanger les données avec le KSN pour améliorer la qualité d'exécution de l'application, les conditions suivantes doivent être remplies :

- Vous ou l'utilisateur de l'appareil devez accepter les conditions de la Déclaration de Kaspersky Security Network. Si vous optez pour que la Déclaration soit acceptée par les utilisateurs, ils seront invités par une notification affichée sur l'écran principal de l'application à accepter les conditions de la Déclaration. Les utilisateurs peuvent également accepter les Déclarations dans la section **Infos sur l'application** dans les paramètres de Kaspersky Endpoint Security for Android.

  Si vous optez pour l'acceptation globale des déclarations, les versions des déclarations acceptées via Kaspersky Security Center doivent correspondre aux versions déjà acceptées par les utilisateurs. Dans le cas contraire, les utilisateurs seront informés du problème et invités à accepter la version d'une déclaration qui correspond à la version acceptée globalement par l'administrateur. L'état de l'appareil dans le Plug-in d'administration de Kaspersky Endpoint Security for Android passera également à *Avertissement*.

- Vous devez autoriser la transmission des données statistiques à KSN dans les paramètres de la stratégie de groupe (voir ci-dessous).

Vous pouvez à tout moment refuser l'envoi des données statistiques à KSN. La Déclaration de Kaspersky Security Network détaille la nature des données statistiques transmises à Kaspersky lorsque le KSN est utilisé parallèlement à l'application mobile Kaspersky Endpoint Security for Android sur les appareils des utilisateurs.

Pour en savoir plus à propos de la collecte des données dans KSN, reportez-vous à la section "Collecte des données".

La fourniture de données à KSN est volontaire. Si vous le souhaitez, vous pouvez désactiver l'échange de données avec KSN.

Activation et désactivation de l'utilisation de Kaspersky Security Network

Pour le fonctionnement des composants de Kaspersky Endpoint Security for Android utilisant Kaspersky Security Network, l'application envoie les demandes aux services cloud. Les demandes contiennent les données telles que décrites dans la section "Collecte des données".

Si l'utilisation de Kaspersky Security Network est désactivée sur l'appareil, les modules 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 est installé.

2. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Avancé**.

3. Dans le groupe **Paramètres de Kaspersky Security Network (KSN)**, configurez les paramètres d'utilisation de Kaspersky Security Network :

   - Cochez la case **Utiliser Kaspersky Security Network** pour le fonctionnant des composants suivants : Antivirus (protection cloud), Protection Internet, Contrôle de l'application (catégories d'applications).

   - Cochez la case **Autoriser le transfert des données statistiques dans KSN** pour le transfert des données à Kaspersky. Les données permettront d'augmenter la vitesse de la réaction de l'application Kaspersky Endpoint Security for Android face aux menaces, d'améliorer les performances des composants de protection et de réduire la probabilité des faux positifs.

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

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center. Une fois la stratégie appliquée, les modules qui utilisent Kaspersky Security Network sont désactivés et la configuration des modules est indisponible.

Utilisation du Kaspersky Private Security Network

Kaspersky Private Security Network (ci-après également dénommé *KSN privé* ou *KPSN)* est une solution qui permet d'accéder aux bases de données de réputation de Kaspersky Security Network, sans envoyer les données des appareils des utilisateurs au Kaspersky Security Network.

Une base de données des réputations des objets (fichiers ou adresses Internet) est stockée sur le serveur de Kaspersky Private Security Network, mais pas sur les serveurs de Kaspersky Security Network. Les bases de données de réputation KPSN sont stockées dans le réseau de l'entreprise et sont gérées par l'administrateur de l'entreprise.

Lorsque KPSN est activé, Kaspersky Endpoint Security n'envoie aucune statistique des appareils des utilisateurs à KSN.

Pour activer l'utilisation du KSN privé via Kaspersky Security Center :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console ou Cloud Console, cliquez sur **Paramètres** ( ).

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

2. Dans l'onglet **Général**, sélectionnez la section **Paramètres du proxy KSN.**

3. Basculez le bouton bascule sur la position **Utiliser Kaspersky Private Security Network ENABLED**.

4. Cliquez sur le bouton **Sélectionner le fichier avec les paramètres du proxy KSN** , puis recherchez le fichier de configuration portant l'extension pkcs7 ou pem (fourni par Kaspersky).

5. Cliquez sur le bouton **Ouvrir**.

6. Si les paramètres du serveur proxy sont configurés dans les propriétés du Serveur d'administration, mais que votre architecture réseau nécessite que vous utilisiez directement le KSN privé, activez l'option **Ignorer les paramètres du serveur proxy KSC lors de la connexion au KSN privé.** Sinon, les demandes des applications administrées ne peuvent pas atteindre le KSN privé.

7. Cliquez sur le bouton **Enregistrer**.

Une fois les paramètres téléchargés, l'interface affiche le nom et les contacts du fournisseur, ainsi que la date de création du fichier avec les paramètres du KSN privé. Les paramètres KPSN sont appliqués aux appareils mobiles.

Lorsque vous passez au KSN privé, le Contrôle des application ne prend pas en charge les catégories d'applications disponibles lors de l'utilisation du KSN global. La catégorisation des applications est disponible si vous décidez de revenir à KSN.

Collecte de données par des services tiers

Kaspersky Endpoint Security for Android utilise les services Google™ : Firebase Cloud Messaging, Google Analytics pour Firebase™, SafetyNet Attestation, Firebase Performance Monitoring et Crashlytics. Kaspersky Endpoint Security for Android utilise le service Firebase Cloud Messaging (FCM) pour un envoi opportun des commandes aux appareils mobiles et une synchronisation forcée en cas de modification des paramètres de la stratégie. Kaspersky Endpoint Security for Android utilise les services Google Analytics pour Firebase, SafetyNet Attestation, Firebase Performance Monitoring et Crashlytics pour améliorer la qualité de fonctionnement de l'application et créer du contenu marketing Kaspersky efficace.

Échange d'informations avec Firebase Cloud Messaging

Kaspersky Endpoint Security for Android utilise le service Firebase Cloud Messaging (FCM) pour un envoi opportun des commandes aux appareils mobiles et une synchronisation forcée en cas de modification des paramètres de la stratégie. De plus, l'application utilise le mécanisme des notifications push.

Pour utiliser le service Firebase Cloud Messaging, il faut configurer les paramètres du service dans Kaspersky Security Center. Pour en savoir plus sur la configuration de Firebase Cloud Messaging dans Kaspersky Security Center, consultez *l'Aide de Kaspersky Security Center*. Si les paramètres de Firebase Cloud Messaging ne sont pas configurés, les commandes sur l'appareil seront exécutées et les paramètres de la stratégie seront envoyés aux appareils pendant la synchronisation de l'appareil avec Kaspersky Security Center d'après la programmation définie dans stratégie (par exemple, toutes les 24 h.). Ainsi, les commandes et les paramètres de la stratégie seront envoyés avec du retard.

Pour garantir le fonctionnement général du produit, vous acceptez automatiquement d'accorder au service Firebase Cloud Messaging l'identifiant unique d'instance de l'application (Instance ID) ainsi que les données suivantes :

- les informations sur le logiciel installé : la version de l'application, l'identifiant de l'application, la version de l'application, le nom du paquet de l'application ;
- les informations sur l'ordinateur sur lequel est installé le logiciel : la version du système d'exploitation, l'identifiant de l'appareil, la version des services Google ;
- les informations sur FCM : l'identifiant de l'application dans FCM, l'identifiant de l'utilisateur FCM, la version du protocole.

Les données sont transmises aux services Firebase via un canal sécurisé. L'accès aux informations et la protection de celles-ci sont réglementés par les conditions d'utilisation des services Firebase : https://firebase.google.com/terms/data-processing-terms/, https://firebase.google.com/support/privacy/.

Pour interdire l'échange d'informations avec le service Firebase Cloud Messaging, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez **Administration des appareils mobiles → Appareils mobiles**.
2. Dans le menu contextuel du dossier **Appareils mobiles**, choisissez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du dossier **Appareils mobiles**, choisissez la section **Paramètres de Google Firebase Cloud Messaging**.
4. Cliquez sur le bouton **Annuler les paramètres**.

Échange d'informations avec les services Google Analytics pour Firebase, SafetyNet Attestation, Firebase Performance Monitoring et Crashlytics

Si vous utilisez le Plug-in d'administration d'une version antérieure et que vous avez activé l'échange de données avec le service Google Analytics, Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 3 effectuera un échange de données avec le service Google Analytics pour Firebase. La prise en charge de Google Analytics a été interrompue.

Kaspersky Security for Mobile exécute l'échange de données avec les services Google Analytics pour Firebase, SafetyNet Attestation, Firebase Performance Monitoring et Crashlytics pour les raisons suivantes :

- Pour améliorer la qualité d'exécution de l'application.

  Afin de pouvoir échanger les données avec les services Google Analytics pour Firebase, SafetyNet Attestation, Firebase Performance Monitoring et Crashlytics pour améliorer la qualité d'exécution de l'application, les conditions suivantes doivent être remplies :

  - L'administrateur ou l'utilisateur de l'appareil doit accepter les conditions de la Déclaration de Kaspersky Security Network. Si vous optez pour que la Déclaration soit acceptée par les utilisateurs, ils seront invités par une notification affichée sur l'écran principal de l'application à accepter les conditions de la Déclaration. Les utilisateurs peuvent également accepter les Déclarations dans la section **Infos sur l'application** dans les paramètres de Kaspersky Endpoint Security for Android.

    Si vous optez pour l'acceptation globale des déclarations, les versions des déclarations acceptées via Kaspersky Security Center doivent correspondre aux versions déjà acceptées par les utilisateurs. Dans le cas contraire, les utilisateurs seront informés du problème et invités à accepter la version d'une déclaration qui correspond à la version acceptée globalement par l'administrateur. L'état de l'appareil dans le Plug-in d'administration de Kaspersky Endpoint Security for Android passera également à *Avertissement*.

  - L'administrateur doit autoriser la transmission des données statistiques à KSN dans les paramètres de la stratégie de groupe (voir ci-dessous).

- Pour faciliter la création de contenus publicitaires efficaces par Kaspersky.

  Afin de pouvoir échanger les données avec les services Google Analytics pour Firebase, SafetyNet Attestation, Firebase Performance Monitoring et Crashlytics pour faciliter la création de contenus publicitaires efficaces par Kaspersky, les conditions suivantes doivent être remplies :

  - L'administrateur ou l'utilisateur de l'appareil doit lire et accepter les conditions de la Déclaration sur le traitement des données à des fins marketing. Si vous optez pour une acceptation de la Déclaration par les

utilisateurs, ils peuvent en accepter les conditions lors de l'installation de l'application ou dans la section **Infos sur l'application** dans les paramètres de Kaspersky Endpoint Security for Android.

- L'administrateur doit autoriser la transmission de données aux services Google Analytics pour Firebase, SafetyNet Attestation, Firebase Performance Monitoring et Crashlytics dans les paramètres de la stratégie de groupe (voir ci-dessous).

La divulgation des données aux services Google Analytics pour Firebase, SafetyNet Attestation, Firebase Performance Monitoring et Crashlytics dans le cadre de la Déclaration sur le traitement des données à des fins marketing

Le Titulaire des droits utilise des systèmes d'information tiers pour traiter les données. Son processus de traitement des données est régi par les déclarations de confidentialité desdits systèmes d'information tiers. Le titulaire des droits utilise les services suivants pour le traitement des données énumérées :

Google Analytics pour Firebase

Durant l'utilisation du Logiciel, les données suivantes seront envoyées à Google Analytics pour Firebase automatiquement et à intervalles réguliers afin de remplir l'objectif déclaré :

- Les informations sur l'app (la version et l'identifiant de l'app, ainsi que l'identifiant de l'app dans le service Firebase, l'identifiant de l'instance dans le service Firebase, le nom de la boutique où l'application a été achetée, l'horodatage du premier lancement du Logiciel)
- L'identifiant d'installation de l'app sur l'appareil et la méthode d'installation sur l'appareil
- La région et la localisation
- La résolution de l'écran de l'appareil
- Les informations sur l'utilisateur bénéficiant de privilèges de root
- Les informations de diagnostic sur l'appareil du service SafetyNet Attestation
- Les informations sur la configuration de Kaspersky Endpoint Security for Android en tant que fonctionnalité d'accessibilité
- Les informations sur les transitions entre les écrans de l'application, la durée de la session, le début et la fin d'une session d'écran, le nom de l'écran
- Le protocole utilisé pour envoyer des données au service Firebase, sa version, et l'identifiant de la méthode de soumission des données utilisée
- Les informations sur le type et les paramètres de l'événement pour lequel les données sont envoyées
- La licence de l'application, sa disponibilité, le nombre d'appareils
- Les informations sur la fréquence des mises à jour de la base antivirus et la synchronisation avec le Serveur d'administration
- La Console d'administration (Kaspersky Security Center ou systèmes EMM tiers)
- Identifiant Android
- Identifiant de publicité
- Informations relatives à l'Utilisateur : catégorie d'âge et sexe, identifiant du pays de résidence et liste d'intérêts
- Informations relatives à l'Ordinateur de l'Utilisateur sur lequel le Logiciel est installé : Informations sur l'ordinateur de l'Utilisateur sur lequel le Logiciel est installé : nom du fabricant de l'ordinateur, type d'ordinateur, modèle, version et langue (locale) du système d'exploitation, informations sur l'application ouverte pour la première fois au cours des 7 derniers jours et l'application ouverte pour la première fois il y a plus de 7 jours

  Les données sont transmises à Firebase via un canal sécurisé. Les informations relatives au traitement des données dans Firebase sont publiées à l'adresse suivante : https://firebase.google.com/support/privacy.

SafetyNet Attestation.

Durant l'utilisation du Logiciel, les données suivantes seront envoyées à l'API d'attestation SafetyNet automatiquement et à intervalles réguliers afin de remplir l'objectif déclaré :

- L'heure de vérification de l'appareil
- Les informations sur le Logiciel, le nom et les données relatives aux certificats logiciels
- Les résultats de la vérification de l'appareil
- Les vérifications d'identifiant aléatoires pour consulter les résultats de la vérification de l'appareil

  Les données sont transmises à l'API d'attestation SafetyNet via un canal sécurisé. Les informations relatives au traitement des données dans l'API d'attestation SafetyNet sont publiées à l'adresse suivante : https://policies.google.com/privacy.

Firebase Performance Monitoring

Durant l'utilisation du Logiciel, les données suivantes seront envoyées à l'API d'attestation SafetyNet automatiquement et à intervalles réguliers afin de remplir l'objectif déclaré :

- identifiant unique d'installation ;
- nom du paquet de l'application ;
- version du logiciel installé ;
- niveau de batterie et état de charge de la batterie ;
- opérateur ;
- état de premier plan ou d'arrière-plan de l'application ;
- géographie ;
- adresse IP ;
- code de langue de l'appareil ;
- informations relatives à la connexion radio/réseau ;
- identifiant pseudonyme de l'instance du Logiciel ;
- taille de la mémoire vive et du disque ;
- indicateur précisant si l'appareil est débridé ou associé à une racine ;
- puissance du signal ;
- durée des traces automatisées.
- réseau et les informations correspondantes suivantes : code de réponse, taille de la charge utile en octets, temps de réponse
- description de l'appareil

Les données sont transmises à Firebase via un canal sécurisé. Les informations relatives au traitement des données dans Firebase Performance Monitoring sont publiées à l'adresse suivante : https://firebase.google.com/support/privacy.

Crashlytics

Durant l'utilisation du Logiciel, les données suivantes seront envoyées à SafetyNet automatiquement et à intervalles réguliers afin de remplir l'objectif déclaré :

- identifiant du Logiciel ;
- version du logiciel installé ;
- indicateur précisant si le Logiciel fonctionnait en arrière-plan ;
- architecture du processeur ;
- identifiant unique de l'événement ;
- date et heure de l'événement ;
- modèle de l'appareil ;
- espace disque total et quantité actuellement utilisée ;
- nom et version du SE ;
- mémoire vive totale et quantité actuellement utilisée ;
- indicateur précisant si l'appareil est associé à une racine ;
- orientation de l'écran au moment de l'événement ;
- fabricant de produits/matériels ;
- identifiant unique d'installation ;
- version des statistiques en cours d'envoi ;
- le type d'exception du Logiciel ;
- texte du message d'erreur ;
- un indicateur précisant que l'exception du Logiciel a été causée par une exception imbriquée ;
- identifiant du flux de travail ;
- un indicateur précisant si l'image est la cause de l'erreur du Logiciel ;
- un indicateur précisant que le flux de travail a provoqué l'arrêt inattendu du Logiciel.
- informations à propos du signal qui a provoqué l'arrêt inattendu du Logiciel : nom du signal, code du signal, adresse du signal
- pour chaque image associée à un flux de travail, à une exception ou à une erreur : le nom du fichier de l'image, le numéro de ligne du fichier de l'image, les symboles de débogage, l'adresse et le décalage dans

l'image binaire, le nom d'affichage de la bibliothèque avec l'image, le type d'image, l'indicateur précisant si l'image est la cause de l'erreur

- identifiant du SE
- identifiant de la question associée à l'événement
- informations à propos des événements qui se sont produits avant que le Logiciel ne s'arrête de manière inattendue : identifiant de l'événement, date et heure de l'événement, type et valeur de l'événement
- valeurs du processeur enregistrées
- type et valeur d'événement

  Les données sont transmises à Facebook via un canal sécurisé. Les informations relatives au traitement des données dans Crashlytics sont publiées à l'adresse suivante : https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

La transmission des informations susmentionnées pour le traitement à des fins marketing s'effectue sur une base volontaire.

Pour désactiver l'échange de données avec les services Google Analytics pour Firebase, SafetyNet Attestation, Firebase Performance Monitoring et Crashlytics, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de la stratégie d'administration des appareils mobiles sur lesquels l'application Kaspersky Endpoint Security for Android est installée.
2. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Avancé**.
3. Dans la section **Transfert de données**, décochez la case **Autoriser le transfert de données afin d'améliorer la qualité, l'apparence et les performances de l'application**.
4. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Acceptation globale des Dispositions supplémentaires

Pour activer la protection fournie par Kaspersky Endpoint Security for Android, les conditions du Contrat de licence utilisateur final, ainsi que les Dispositions supplémentaires (voir ci-dessous) doivent être acceptées. Vous configurez une stratégie pour accepter globalement les Déclarations répertoriées ci-dessous, pour tous les utilisateurs. Les utilisateurs ne seront pas invités à lire et à accepter les conditions des Contrats et Déclarations suivants qui ont déjà été acceptés globalement :

- Déclaration de Kaspersky Security Network
- Déclaration sur le traitement des données pour la Protection Internet
- Déclaration sur le traitement des données à des fins marketing

Si vous optez pour l'acceptation globale des déclarations, les versions des déclarations acceptées via Kaspersky Security Center doivent correspondre aux versions déjà acceptées par les utilisateurs. Dans le cas contraire, les utilisateurs seront informés du problème et invités à accepter la version d'une déclaration qui correspond à la version acceptée globalement par l'administrateur. L'état de l'appareil dans le Plug-in d'administration de Kaspersky Endpoint Security for Android passera également à *Avertissement*.

Pour choisir si les conditions doivent être acceptées globalement ou par les utilisateurs en appliquant une stratégie de groupe :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Avancé**.
5. Dans la section **Transfert de données**, choisissez si la Déclaration sur le traitement des données à des fins marketing sera acceptée globalement ou par les utilisateurs.
6. Dans la section des **Paramètres de Kaspersky Security Network (KSN)** , choisissez si la Déclaration de Kaspersky Security Network sera acceptée globalement ou par les utilisateurs.
7. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

L'utilisateur peut à n'importe quel moment accepter les conditions de l'application ou les refuser dans la section **Infos sur l'application** des paramètres de Kaspersky Endpoint Security for Android.

Samsung KNOX

Samsung KNOX est une solution mobile pour la configuration et la protection des périphériques mobiles Samsung tournant sous Android. Pour en savoir plus sur Samsung KNOX, consultez le *site de l'assistance technique de Samsung*.

Installation de l'application Kaspersky Endpoint Security for Android via KNOX Mobile Enrollment

KNOX Mobile Enrollment (KME) est une partie de la solution mobile Samsung KNOX. Il est utilisé pour l'installation massive et la configuration initiale des applications sur les nouveaux appareils Samsung acquis auprès des fournisseurs officiels.

L'installation de l'application Kaspersky Endpoint Security for Android via KNOX Mobile Enrollment comprend les étapes suivantes :

1. Création du profil MDM KNOX avec l'application Kaspersky Endpoint Security for Android.
2. Ajout d'appareils à KNOX Mobile Enrollment.
3. Installation de l'application Kaspersky Endpoint Security for Android sur les appareils mobiles de l'utilisateur.

Pour en savoir plus sur l'utilisation de KNOX Mobile Enrollment, consultez le *Manuel de l'utilisateur KNOX Mobile Enrollment*.

Le déploiement via KNOX Mobile Enrollment est possible uniquement pour les appareils Samsung. La liste des appareils pris en charge se trouve sur le *site du Support Technique de Samsung*.

Création du profil MDM KNOX

Le profil MDM KNOX est un profil qui contient les liens vers les applications pour leur déploiement rapide et la configuration initiale sur les appareils mobiles.

Pour créer un profil MDM KNOX, procédez comme suit :

1. Connectez-vous à la console Samsung KNOX → **KNOX Mobile Enrollment**.
2. Choisissez la section **Profils MDM**.
3. Cliquez sur le bouton **Ajouter**.

   L'assistant de la création du profil MDM KNOX est lancé.
4. A l'étape **Connexion du serveur MDM** choisissez **L'URI du serveur n'est pas obligatoire pour mon service MDM** et cliquez sur **Suivant**.
5. A l'étape **Informations sur le profil MDM** procédez comme suit :
   a. Saisissez les informations générales sur le profil MDM KNOX : **Nom du profil** et **Description**.
   b. Saisissez le chemin vers le fichier d'installation APK à l'aide du bouton **Ajouter les applications MDM**.

      Le fichier d'installation de Kaspersky Endpoint Security for Android fait partie du kit de distribution de Kaspersky Security for Mobile. Installez préalablement le fichier d'installation APK sur le Serveur Web de Kaspersky Security Center ou sur un autre serveur accessible pour le chargement à partir de l'appareil.
   c. Saisissez les paramètres de connexion de l'appareil à Kaspersky Security Center dans le champ **Données utilisateur JSON** au format :
      `{"serverAddress":"ksc.server.com","serverPort":"12345","groupName":"MOBILE GROUP"}`.

      La connexion de l'appareil à Kaspersky Security Center est demandée pour l'activation de l'application, la configuration de l'appareil et l'envoi des commandes.
   d. Cochez la case **Ajout des accords liés à Knox**.

      Pour l'installation de Kaspersky Endpoint Security for Android via KNOX Mobile Enrollment, l'utilisateur de l'appareil mobile doit accepter les conditions du Contrat de licence utilisateur final Samsung. Vous pouvez prendre connaissance des conditions du Contrat de licence utilisateur final Samsung dans le bloc **Contrats de licence utilisateur final, conditions du service et les accords utilisateur**. Vous pouvez également ajouter d'autres documents juridiques de votre entreprises, documents nécessaires au déploiement du profil KNOX MDM, à l'aide du bouton **Ajouter l'accord utilisateur**.
   e. Décochez la case **Associez la licence Knox à ce profil**.

      Les informations sur la licence Samsung KNOX sont transmises à l'appareil mobile avec la stratégie lors de la synchronisation de l'appareil avec Kaspersky Security Center.
6. Cliquez sur le bouton **Enregistrer**.

En conséquence, un nouveau profil MDM KNOX avec l'application Kaspersky Endpoint Security for Android est ajouté à la liste dans la console KME.

Ajout d'appareils à KNOX Mobile Enrollment

L'ajout d'appareils à la console KNOX Mobile Enrollment (KME) peut s'effectuer par les moyens suivants :

- Le fournisseur ajoute automatiquement les appareils à la console KME après leur acquisition.

  Choisissez ce moyen si votre organisation coopère avec un fournisseur officiel d'appareils Samsung.

- L'administrateur installe l'application KNOX Deployment de Google Play sur l'appareil mobile et transfère le profil MDM KNOX sur les appareils des utilisateurs à l'aide de Bluetooth ou NFC (Near Field Communication). Après le déploiement du profil MDM KNOX, l'appareil sera automatiquement ajouté dans la console KME.

  Choisissez ce moyen si les appareils Samsung ne sont pas acquis auprès d'un fournisseur officiel.

Ajout d'un appareil par le fournisseur

Le fournisseur officiel d'appareils Samsung est enregistré dans Samsung KNOX. Vous pouvez consulter la liste des fournisseurs officiels sur le site du *Support Technique de Samsung*. Le fournisseur ajoute automatiquement les appareils à la console KME pour votre compte utilisateur Samsung immédiatement après l'acquisition des appareils. Pour l'ajout d'appareils par le fournisseur, vous devez enregistrer ce dernier dans la console KME pour votre compte utilisateur Samsung. Pour l'ajout du fournisseur d'appareils Samsung à la console KME, vous aurez besoin de l'identificateur de l'intermédiaire. Pour la réception de l'identificateur de l'intermédiaire, il vous est nécessaire d'envoyer la demande au fournisseur. Dans la demande indiquez votre identificateur de client KNOX.

Pour consulter votre identificateur de client KNOX, procédez comme suit :

1. Connectez-vous à la console Samsung KNOX → **KNOX Mobile Enrollment**.
2. Choisissez la section **Intermédiaires**.
3. Le champ **Identificateur du client KNOX** affiche votre identificateur.

Après la réception de la réponse du fournisseur avec l'identificateur de l'intermédiaire, enregistrez le fournisseur dans la console KME. Avant l'enregistrement du fournisseur, vous pouvez créer un profil MDM KNOX pour le déploiement automatique du profil à l'ajout des nouveaux appareils.

Pour enregistrer le fournisseur officiel dans la console KME, procédez comme suit :

1. Connectez-vous à la console Samsung KNOX → **KNOX Mobile Enrollment**.
2. Choisissez la section **Intermédiaires**.
3. Cliquez sur le bouton **Enregistrer l'intermédiaire commercial**.

   La fenêtre d'enregistrement du fournisseur d'appareils s'ouvre.
4. Dans le champ **Identificateur de l'intermédiaire**, saisissez l'identificateur reçu du fournisseur officiel d'appareils Samsung.
5. Si vous avez créé un profil MDM KNOX, choisissez-le dans la fenêtre de l'enregistrement du fournisseur.

   Lors de l'ajout des nouveaux appareils, le profil MDM KNOX est installé automatiquement.

6. Dans la liste **Moyen préféré de confirmation des téléchargements**, choisissez le moyen de confirmation de l'ajout de l'appareil pour le fournisseur.

   - **Tous les téléchargements doivent être confirmés**. Lors de l'ajout de l'appareil par le fournisseur, vous devrez confirmer l'opération.

   - **Confirmer automatiquement tous les téléchargements de cet intermédiaire**. Les appareils du fournisseur seront automatiquement ajoutés à la console KME.

7. Cliquez sur **OK**.

Le fournisseur d'appareils Samsung sera ajouté à la liste des fournisseurs dans la console KME.

Après l'acquisition de nouveaux appareils auprès du fournisseur officiel, l'application Kaspersky Endpoint Security for Android est automatiquement ajoutée aux appareils après leur connexion au réseau Internet. Pour plus de détails sur l'utilisation de KNOX Mobile Enrollment, consultez le *Manuel de l'utilisateur KNOX Mobile Enrollment*. Si vous avez déjà constitué une liste d'appareils dans la console KME, ajoutez sur l'appareil le profil MDM KNOX avec l'application MDM KNOX.

Pour installer un profil MDM KNOX sur des appareils, procédez comme suit :

1. Connectez-vous à la console Samsung KNOX → **KNOX Mobile Enrollment**.

2. Choisissez la section **Appareils** → **tous les appareils**.

3. Choisissez les appareils sur lesquels vous voulez installer le profil MDM KNOX.

4. Cliquez sur le bouton **Configurer**.

   La fenêtre **Informations sur l'appareil** s'ouvre.

5. Dans la liste **Profil MDM**, choisissez le profil MDM KNOX avec l'application Kaspersky Endpoint Security for Android.

6. Dans le champ **Tags**, indiquez les tags pour le groupement et le marquage des appareils, ainsi que pour l'optimisation de la recherche dans la console KME.

7. Saisissez les identifiants du compte utilisateur de l'appareil dans les champs **Identifiant utilisateur** et **Mot de passe**.

   Les identifiants de l'utilisateur sont demandés pour la réception du certificat commun. L'identifiant utilisateur et le mot de passe doivent coïncider avec les identifiants de l'utilisateur dans Kaspersky Security Center (nom complet et mot de passe dans les propriétés du compte utilisateur).

8. Choisissez le profil MDM KNOX pour les autres appareils.

9. Cliquez sur le bouton **Enregistrer**.

Suite à la connexion de l'appareil au réseau Internet, l'application propose à l'utilisateur d'installer le profil MDM KNOX.

Ajout d'un appareil à l'aide de l'application KNOX Deployment

Si vous n'avez pas acquis l'appareil Samsung auprès d'un fournisseur officiel, vous pouvez l'ajouter à KNOX Mobile Enrollment à l'aide de Bluetooth ou NFC. Pour cela, vous aurez besoin du périphérique mobile de l'administrateur à l'aide duquel les profils MDM KNOX sont installés sur les appareils mobiles des utilisateurs.

Pour l'ajout d'appareils à l'aide de l'application KNOX Deployment, les conditions suivantes doivent être remplies :

- Sur les appareils mobiles, les modules Bluetooth ou NFC doivent être activés, en fonction du mode d'installation choisi.
- Les appareils mobiles doivent être connectés au réseau Internet.

Pour installer un profil MDM KNOX à l'aide de l'application KNOX Deployment, procédez comme suit :

1. Installez sur l'appareil mobile de l'administrateur l'app KNOX Deployment depuis Google Play.
2. Lancez l'application KNOX Deployment.
3. Saisissez les identifiants de votre compte utilisateur Samsung.
4. Dans la fenêtre **KNOX Deployment**, configurez les paramètres de déploiement du profil MDM KNOX :
   - Choisissez le profil MDM KNOX.
   - Choisissez le mode de déploiement : **Bluetooth** ou **NFC**.

     Lors de l'utilisation de Bluetooth, vous pouvez ajouter le profil MDM KNOX sur plusieurs appareils à la fois.
5. Cliquez sur **Commencer le déploiement** :
   - **Bluetooth**. Sur l'appareil mobile de l'utilisateur ouvrez le site Internet https://configure.samsungknox.com.

     L'assistant d'enregistrement de l'appareil Samsung KNOX se lance. Suivez les indications de l'écran.

     Suite à l'installation du profil MDM KNOX, un nouvel appareil est ajouté dans la console KME avec le tag **Bluetooth**.
   - **NFC**. Approchez l'appareil mobile de l'administrateur de l'appareil mobile de l'utilisateur et transmettez le profil MDM KNOX.

     En conséquence, l'application propose d'installer le profil MDM KNOX sur l'appareil mobile de l'utilisateur. Dans la console KME, un nouvel appareil est ajouté avec le tag **NFC**.

Installation de l'application

Avant l'installation de l'application Kaspersky Endpoint Security for Android, copiez dans la Console d'administration de Kaspersky Security Center le certificat commun pour les utilisateurs des appareils mobiles. Le certificat commun est demandé pour l'identification de l'utilisateur de l'appareil mobile dans la Console d'administration de Kaspersky Security Center.

Après le début du déploiement du profil MDM KNOX sur l'appareil mobile, le fichier d'installation APK sera chargé automatiquement. L'installation de l'application Kaspersky Endpoint Security for Android sera lancée automatiquement. L'utilisateur doit accepter le Contrat de Licence Utilisateur Final de Samsung KNOX et le Contrat de Licence Utilisateur Final de Kaspersky Endpoint Security for Android. Aucune configuration supplémentaire de l'application n'est nécessaire. Après l'installation de l'application, la synchronisation avec Kaspersky Security Center sera automatiquement exécutée. En conséquence, l'appareil mobile sera ajouté à la Console d'administration de Kaspersky Security Center dans le groupe d'administration indiqué dans les paramètres du profil MDM KNOX (`groupName`).

Configuration des conteneurs KNOX

Cette section fournit des informations sur l'utilisation de conteneurs KNOX sur les appareils Samsung tournant sous le système d'exploitation Android.

L'utilisation de conteneur KNOX est disponible uniquement sur les appareils Samsung qui tournent sous Android version 6.0 ou suivantes.

A propos du conteneur KNOX

Le *conteneur KNOX* est un environnement sécurisé sur l'appareil de l'utilisateur. Ce conteneur comprend son propre écran d'accueil, son propre dispositif de lancement, ainsi que ses propres apps et widgets. Le conteneur KNOX permet de séparer les données et les applications d'entreprise des données et apps personnelles. Le conteneur KNOX est un élément de la solution mobile Samsung KNOX.

Samsung KNOX est une solution mobile pour la configuration et la protection des périphériques mobiles Samsung tournant sous Android. Pour en savoir plus sur Samsung KNOX, consultez le *site de l'assistance technique de Samsung*.

Les conteneurs KNOX permettent de séparer les données personnelles des données d'entreprise sur l'appareil mobile. Il est par exemple impossible d'envoyer un fichier du conteneur KNOX via la boîte aux lettres personnelles. Il est conseillé d'utiliser un conteneur KNOX si les données d'entreprise sont exploitées à l'aide des appareils mobiles personnels des employés.

L'utilisation d'un conteneur KNOX requiert l'activation de Samsung KNOX. Une fois que l'appareil a été synchronisé avec Kaspersky Security Center, l'utilisateur de cet appareil mobile est invité à installer un conteneur KNOX. Avant d'installer un conteneur KNOX, l'utilisateur doit accepter les dispositions du Contrat de licence utilisateur final de la société Samsung.

L'icône KNOX  apparaît sur le bureau de l'appareil mobile après l'installation d'un conteneur KNOX. Ou l'espace de travail sera ajouté à la liste des applications sur l'appareil mobile. Pour manipuler les données d'entreprise, l'utilisateur doit lancer l'application depuis le conteneur KNOX.

Kaspersky Endpoint Security for Android n'est pas installé sur le conteneur KNOX et ne protège pas les données d'entreprise. Kaspersky Endpoint Security for Android ne détecte pas le téléchargement de fichiers malveillants et ne bloque pas les sites malveillants dans le conteneur KNOX. Vous ne pouvez pas contrôler le lancement des applications ni interdire l'utilisation de la caméra dans le conteneur KNOX. Kaspersky Endpoint Security for Android protège uniquement les données privées. Vous pouvez protéger les données d'entreprise avec les outils de Samsung KNOX. Pour en savoir plus sur Samsung KNOX, consultez le *site de l'assistance technique de Samsung*.

Activation de Samsung KNOX

Pour utiliser un conteneur KNOX sur l'appareil mobile de l'utilisateur, vous devez activer Samsung KNOX. La procédure d'activation de Samsung KNOX dépend de la version de Kaspersky Endpoint Security for Android installée sur les appareils de vos utilisateurs :

- Si la version actuelle de Kaspersky Endpoint Security for Android est installée sur les appareils, vous n'avez besoin d'aucune clé pour activer Samsung KNOX.
- Si une ancienne version de Kaspersky Endpoint Security for Android (10.8.3.174 ou antérieure) est installée sur les appareils, vous devez obtenir une clé KNOX License Manager (ci-après la clé KLM) auprès de Samsung. Une *clé KNOX License Manager* est un code unique utilisé par le système de licence Samsung KNOX. Pour des informations détaillées sur la clé KLM, reportez-vous au site Internet du Support Technique de Samsung KNOX.

La configuration de conteneurs KNOX n'est possible que sur les appareils Samsung.

Pour activer Samsung KNOX :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés** de la stratégie, sélectionnez la section **Administration de Samsung KNOX → Conteneurs KNOX**.
5. Dans le champ **Clé KNOX License Manager**, définissez les éléments suivants :
   - Si la version actuelle de Kaspersky Endpoint Security for Android est installée sur les appareils, saisissez n'importe quel caractère.
   - Si une ancienne version de Kaspersky Endpoint Security for Android (10.8.3.174 ou antérieure) est installée sur les appareils, saisissez la clé KLM envoyée par Samsung.
6. Placez l'attribut Verrouiller en position Verrouillée.
7. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

Samsung KNOX sera activé après la prochaine synchronisation de l'appareil avec Kaspersky Security Center. L'utilisateur devra, sur invite, accepter les dispositions de Contrat de licence utilisateur final de Samsung et installer le conteneur KNOX.

Pour désactiver Samsung KNOX :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés de la stratégie**, sélectionnez la section **Administration de Samsung KNOX → Conteneurs KNOX**.

5. Effacez la valeur du champ **Clé KNOX License Manager**.

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

Samsung KNOX sera désactivé après la prochaine synchronisation de l'appareil avec Kaspersky Security Center. L'accès au conteneur KNOX est bloqué.

Restrictions de Samsung KNOX

- L'utilisation de conteneurs KNOX n'est possible que sur les appareils Samsung.
- Sur les appareils Samsung avec la prise en charge de KNOX 2.6, 2.7 et 2.7.1 dans le conteneur KNOX, la protection Internet et le contrôle des applications ne fonctionnent pas. Le problème est lié à l'absence des privilèges requis dans le conteneur KNOX (service des fonctions d'accessibilité). Sur les appareils compatibles avec KNOX 2.8 et suivants, tous les composants de l'application fonctionnent sans restrictions.
- Les versions de Kaspersky Endpoint Security for Android antérieure à Service Pack 4 Maintenance Release 3 mise à jour 2 risquent de fonctionner de manière instable sur les appareils Samsung Android 10 en raison des mises à jour de Samsung KNOX. Il est recommandé de mettre à jour Kaspersky Endpoint Security for Android vers la version Service Pack 4 Maintenance Release 3 mise à jour 2.

Configuration du pare-feu dans KNOX

Pour pouvoir contrôler les connexions réseau dans le conteneur KNOX, il faut configurer les paramètres du Pare-feu.

Pour configurer le Pare-feu dans le conteneur KNOX, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.

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

3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie active.

4. Dans la fenêtre **Propriétés de la stratégie**, sélectionnez la section **Administration de Samsung KNOX → Conteneurs KNOX**.

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

   La fenêtre **Pare-feu** s'ouvre alors.

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

   - Pour autoriser toutes les connexions entrantes et sortantes, 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**.

7. 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 pour le Pare-feu** s'ouvre alors.

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

c. Saisissez le nom système du paquet de l'app mobile (par exemple, `com.mobileapp.example`) dans le champ **Nom du paquet**.

d. Cliquez sur **OK**.

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

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Configuration de la boîte aux lettres Exchange dans KNOX

Pour utiliser l'email, les contacts et le calendrier d'entreprise dans le conteneur KNOX, il faut configurer les paramètres de la boîte aux lettres Exchange.

Pour configurer la boîte aux lettres Exchange dans le conteneur KNOX, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Appareils administrés**, choisissez le groupe d'administration dont font partie les appareils Android.
2. Dans l'espace de travail du groupe, choisissez l'onglet **Stratégies**.
3. Double-cliquez sur une colonne pour ouvrir la fenêtre des propriétés de la stratégie active.
4. Dans la fenêtre **Propriétés**, sélectionnez la section **Administration de Samsung KNOX → Conteneurs KNOX**.
5. Dans le groupe **Exchange ActiveSync**, cliquez sur le bouton **Configurer**.

   La fenêtre **Paramètres du serveur de messagerie Exchange** s'ouvre.
6. Dans le champ **Adresse du serveur**, saisissez l'adresse IP ou le nom DNS du serveur sur lequel se trouve le serveur de messagerie.
7. Dans le champ **Domaine**, saisissez le nom du domaine de l'utilisateur de l'appareil mobile sur le réseau de l'entreprise.
8. Dans la liste déroulante **Fréquence de synchronisation**, sélectionnez la fréquence souhaitée pour la synchronisation de l'appareil mobile avec le serveur Microsoft Exchange.
9. Pour utiliser le protocole de transfert de données SSL, cochez la case **Utiliser une connexion (SSL)**.
10. Pour utiliser des certificats numériques afin de protéger l'échange de données entre l'appareil mobile et le serveur Microsoft Exchange, cochez la case **Vérifier le certificat du serveur**.
11. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications effectuées.

Les paramètres sur l'appareil mobile sont configurés après la prochaine synchronisation de l'appareil avec Kaspersky Security Center.

Annexes

Cette section contient des informations qui enrichissent le texte du document.

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 :

- **Autoriser la modification**. L'utilisateur de la Console d'administration peut modifier les paramètres de la stratégie dans la fenêtre des propriétés.
- **Interdire 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.

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

Zone opérationnelle	Section Stratégies
Android Enterprise	Profil de travail Android
Antivol	Antivol
Contrôle des applications installées	Contrôle des applications installées
Protection	Protection, Analyse, Mise à jour
Contrôle de conformité	Contrôle de conformité
Conteneurs ;	Conteneurs ;
Paramètres du périphérique	Gestion de l'appareil, Synchronisation
Administration des périphériques Samsung	APN, Administration des unités Samsung, conteneurs KNOX
Administration du système	Avancé, Wi-Fi
Protection Internet	Protection Internet

Droits d'accès aux sections du plug-in d'administration de Kaspersky Device Management for iOS

Zone opérationnelle	Section Stratégies
Avancé	Clips Internet, Polices, AirPlay, AirPrint
Exchange ActiveSync	Généraux, Mot de passe, Synchronisation, Restrictions des fonctions, Restrictions des fonctionnalités
Général	Généraux, Compte unique, Protection Internet, 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 fonctionnalités, Restrictions des applications, Restrictions du contenu multimédia, Mot de passe, VPN, Proxy HTTP global, Certificats, SCEP

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.

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.
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.
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 appareils.
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'utilisation des stockages de fichiers, de notes et de fichiers multimédias en ligne.
Applications d'aide	Applications destinées à la lecture de livres, d'ouvrages de référence, de manuels, de dictionnaires, de thésaurus, de pages wiki.
Applications de messagerie	Applications d'envoi et de réception de messages électroniques.

Utilisation de l'application Kaspersky Endpoint Security for Android

Cette section d'aide décrit les fonctionnalités et les opérations accessibles aux utilisateurs de l'app Kaspersky Endpoint Security for Android.

Les articles de cette section comprennent toutes les options éventuellement disponibles ou visibles sur un appareil mobile. La disposition et le comportement réels de l'application dépendent du système d'administration à distance exploité et de la manière dont l'administrateur configure votre appareil conformément aux exigences de sécurité de l'entreprise. Certaines fonctions et options décrites dans cette section ne concerneront sans doute pas votre expérience avec l'application. Pour toute question concernant l'application sur votre appareil spécifique, contactez votre administrateur.

Fonctions de l'application

Kaspersky Endpoint Security offre les fonctions principales suivantes.

Protection contre les virus et les autres applications malveillantes

Le module Anti-Virus est utilisé pour la protection contre les virus et les autres applications malveillantes.

L'Anti-Virus exécute les fonctions suivantes :

- analyse à la recherche d'éventuelles menaces sur tous les appareils, les applications installées ou les dossiers sélectionnés ;
- protection de l'appareil en temps réel ;
- analyse des nouvelles applications installées avant leur premier lancement ;
- mise à jour des bases antivirus.

Si l'appareil mobile est doté d'une application de collecte et d'envoi d'informations à traiter, Kaspersky Endpoint Security for Android peut considérer une telle application comme malveillante.

Contrôle des applications installées

Conformément aux exigences de la stratégie de sécurité d'entreprise, l'*administrateur du système d'administration à distance* (ci-après, l'administrateur) établit des listes d'apps conseillées, interdites et requises. Le module Contrôle des applications est utilisé pour l'installation et la mise à jour des applications conseillées et obligatoires, ainsi que pour la suppression des applications interdites.

Le Contrôle des applications vous permet d'installer les apps conseillées et requises sur votre appareil à l'aide d'un lien direct vers la distribution ou vers Google Play. Grâce au Contrôle des applications, vous pouvez supprimer les applications interdites, non conformes aux exigences à la sécurité corporative.

Pour que le contrôle des applications fonctionne correctement, Kaspersky Endpoint Security doit être installé en tant que service des Fonctionnalités d'accessibilité. Vous pouviez activer le service pendant le fonctionnement de l'Assistant de configuration initiale de l'app. Si vous avez ignoré cette étape, activez Kaspersky Endpoint Security en tant que service des Fonctionnalités d'accessibilité dans la section **État** en choisissant la notification correspondante ou dans les paramètres de l'appareil (**Paramètres Android** → **Fonctionnalité d'accessibilité** → **Services**).

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

Le module Antivol sert à éviter que les informations soient consultées par une personne tierce et à faciliter la recherche de l'appareil en cas de perte ou de vol.

L'Antivol permet d'exécuter les actions suivantes à distance :

- Verrouiller l'appareil.

  Pour que l'individu malintentionné ne puisse pas déverrouiller l'appareil, Kaspersky Endpoint Security doit être activé en tant que service des Fonctionnalités d'accessibilité sur les appareils mobiles tournant sous le système d'exploitation Android 7.0 et suivants.

- activer sur l'appareil une alarme retentissante, même si le son est désactivé ;
- recevoir les coordonnées de l'emplacement de l'appareil sur la carte ;
- supprimer les données enregistrées sur l'appareil ;
- rétablir les valeurs d'usine des paramètres ;
- Prendre une photographie discrète de la personne qui utilise votre appareil.

Pour garantir le fonctionnement de l'Antivol, Kaspersky Endpoint Security doit être installé en tant qu'administrateur de l'appareil. Vous pouviez octroyer les privilèges d'administrateur sur l'appareil pendant la configuration initiale de l'app. Si vous avez ignoré cette étape, octroyez les privilèges d'administrateur à Kaspersky Endpoint Security dans la section **État** en choisissant la notification correspondante ou dans les paramètres de l'appareil (**Paramètres d'Android** → **Sécurité** → **Administrateurs de l'appareil**).

Protection contre les menaces Internet

Le module Protection Internet sert à la protection contre les menaces Internet.

La Protection Internet bloque les sites Internet malveillants qui distribuent un code malveillant et des sites Internet de phishing servant à voler vos données confidentielles afin d'obtenir un accès à vos comptes bancaires. La Protection Internet analyse les sites Internet avant leur ouverture à l'aide du service cloud de Kaspersky Security Network.

Pour activer la Protection Internet :

- Kaspersky Endpoint Security doit être activé en tant que service des Fonctionnalités d'accessibilité.

- Vous devez accepter la Déclaration relative au traitement des données aux fins d'utilisation de la Protection Internet (Déclaration sur la Protection Internet). Kaspersky Endpoint Security utilise Kaspersky Security Network (KSN) pour analyser les sites Internet. La Déclaration sur la Protection Internet contient les conditions générales de l'échange de données avec KSN.

  Votre administrateur peut accepter la Déclaration sur la Protection Internet pour vous dans Kaspersky Security Center. Dans ce cas, vous n'avez rien à faire.

  Si votre administrateur n'a pas accepté la Déclaration sur la Protection Internet et qu'il vous a envoyé la demande, vous devez lire et accepter la Déclaration sur la Protection Internet dans les paramètres de l'application.

  Si votre administrateur n'a pas accepté la Déclaration sur la Protection Internet, la Protection Internet n'est pas disponible.

La Protection Internet sur les appareils Android fonctionne seulement dans les navigateurs Google Chrome (y compris la fonction Onglets personnalisés), Huawei Browser et Samsung Internet Browser. La Protection Internet pour le navigateur Samsung Internet ne bloque pas les sites sur un appareil mobile si un profil de travail est utilisé et que la Protection Internet est activée uniquement pour ce profil de travail.

Navigation dans la fenêtre principale

L'apparence de la fenêtre principale diffère légèrement selon la résolution de l'écran.

L'aspect de l'écran principal change en cas de problèmes qui peuvent réduire le niveau de protection ou entraîner une infection de l'appareil ou une perte d'informations.

La section **État** affiche les informations suivantes :

- Problèmes de protection de l'appareil ;
- Informations sur l'adéquation de l'appareil aux exigences de sécurité de l'entreprise ;
- Informations sur l'état de la protection de votre appareil.

Vous pouvez ouvrir la section **État** en appuyant sur la partie supérieure de la fenêtre principale de Kaspersky Endpoint Security.

Problèmes dans la protection de l'appareil

Les problèmes de protection sont regroupés par catégories. Des actions que vous pouvez exécuter sont proposées pour résoudre chaque problème.

La section **État** reprend également la liste des objets ignorés détectés par l'app. Le contenu de la liste des objets ignorés peut changer, par exemple si un fichier malveillant est supprimé ou déplacé. Pour obtenir la liste actuelle des menaces, lancez une analyse complète de l'appareil. Afin de vraiment garantir la protection des données, il est conseillé de supprimer tous les objets détectés.

Les problèmes de protection peuvent être de deux types différents :

- *Notificatifs*. Surlignés en jaune. Les problèmes notificatifs avertissent sur les événements importants pour la sécurité de l'appareil (par exemple, la dernière analyse a été effectuée il y a plus de 14 jours ou une nouvelle

application a été installée sans analyse). Il est possible de dissimuler le problème signalé. Suite à cette action, les informations sur le problème demeureront accessibles dans le menu **Problèmes masqués**.

- *Critiques*. Surlignés en rouge. Les problèmes critiques vous informent sur les événements de première gravité à propos de la sécurité de l'appareil (par exemple, la mise à jour des bases antivirus n'a pas été exécutée depuis longtemps, une application interdite est installée sur votre appareil). Il est impossible de masquer un problème critique.

Contrôle de conformité

L'application analyse automatiquement la conformité de l'appareil aux exigences à la sécurité corporative. La section **État** affiche les informations suivantes relatives à la compatibilité de votre appareil avec les exigences de sécurité de l'entreprise :

- contenu de la non-conformité de l'appareil aux exigences de sécurité de l'entreprise (par exemple, des applications interdites sont installées sur l'appareil) ;
- le délai imparti pour supprimer le problème (par exemple, 24 heures) ;
- Action qui va être exécutée sur l'appareil si vous ne le rendez pas conforme aux exigences à l'issue du délai octroyé (par exemple, verrouillage de l'appareil) ;
- option de l'action pour l'élimination de la non-conformité de l'appareil aux exigences de la stratégie d'entreprise.

Icône sur la ligne d'état

Une fois l'assistant de première exécution de l'application terminé, l'icône Kaspersky Endpoint Security apparaît sur la ligne d'état.

L'icône sert d'indicateur concernant le fonctionnement de l'application et assure l'accès à la fenêtre principale de Kaspersky Endpoint Security.

L'icône sert d'indicateur de fonctionnement de Kaspersky Endpoint Security et reflète l'état de la protection de votre appareil :

: l'appareil est protégé.

: il existe des problèmes au niveau de la protection (par exemple, les bases antivirus sont dépassées ou une nouvelle app non vérifiée a été installée).

Analyse de l'appareil

L'Antivirus possède une série de restrictions :

- Lors du fonctionnement de l'Antivirus dans le profil de travail, il est impossible d'éliminer automatiquement la menace détectée dans la mémoire externe de l'appareil (par exemple, sur la carte SD) (Applications avec "portefeuille", Configuration du profil de travail Android). Kaspersky Endpoint Security for Android n'a pas dans le profil de travail accès à la mémoire externe. Les informations sur les objets détectés s'affichent dans la section **État** de l'app. Pour éliminer les objets détectés dans la mémoire externe, il faut supprimer le fichier à la main et lancer à nouveau l'analyse de l'appareil.
- En raison de restrictions techniques, Kaspersky Endpoint Security for Android n'est pas capable d'analyser les fichiers de 2 Go ou plus. Dans le cadre de l'analyse, l'app ignore ces fichiers et ne les signale pas.

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

1. Dans la fenêtre principale de Kaspersky Endpoint Security, ouvrez le volet de lancement rapide et cliquez sur **Analyse**.

2. Sélectionnez la zone d'analyse de l'appareil :

   - **Analyser tout l'appareil**. L'application analyse l'ensemble du système de fichiers de l'appareil.
   - **Analyser les apps installées**. L'app analyse uniquement les apps installées.
   - **Analyse personnalisée**. L'app analyse le dossier sélectionné ou un fichier séparé. Vous pouvez choisir un objet séparé (dossier ou fichier) ou une des sections suivantes de la mémoire de l'appareil :
     - **Mémoire de l'appareil**. La mémoire de tout l'appareil est accessible en lecture. La section système de la mémoire sur laquelle se trouvent les fichiers du système d'exploitation fait aussi partie de cette zone.
     - **Mémoire interne**. Section de la mémoire de l'appareil destinée à l'installation des app, à la conservation du contenu média, des documents et d'autres fichiers.
     - **Mémoire externe**. Mémoire de la carte SD externe. Si la carte SD externe n'est pas installée, l'option est cachée.

L'accès aux paramètres de la recherche de virus peut être limité par votre administrateur.

Pour configurer la recherche de virus :

1. Dans la fenêtre principale de Kaspersky Endpoint Security ouvrez le volet de lancement rapide et cliquez sur → **Paramètres** → **Anti-Virus** → **Analyse**.

2. Si vous souhaitez que lors de l'analyse, l'application ne détecte les applications publicitaires et les programmes pouvant être exploités par des individus malintentionnés pour nuire au appareil ou à vos données, cochez la case **Publicité, numéroteurs et autres**.

3. Cliquez sur **Action en cas de détection d'une menace**, et sélectionnez l'action de l'application par défaut :

   - **Quarantaine**

     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.

   - **Confirmer l'action**

     L'application vous propose de choisir l'action pour chaque objet détecté : ignorer, placer en quarantaine ou supprimer. En cas de détection de plusieurs objets, vous pouvez appliquer l'action choisie à tous les objets.

   - **Supprimer**

     Les objets détectés sont automatiquement supprimés. Aucune action supplémentaire n'est requise. Avant la suppression, Kaspersky Endpoint Security affiche une notification temporaire sur la détection de l'objet.

   - **Ignorer**

Si des objets détectés ont été ignorés, Kaspersky Endpoint Security vous avertit de la présence de problèmes dans la protection de l'appareil. Les informations sur les objets ignorés s'affichent dans la section **État** de l'app. Pour chaque menace ignorée, vous avez le choix entre plusieurs actions pour l'éliminer. Le contenu de la liste des objets ignorés peut changer, par exemple si un fichier malveillant est supprimé ou déplacé. Pour obtenir la liste actuelle des menaces, lancez une analyse complète de l'appareil. Afin de vraiment garantir la protection des données, il est conseillé de supprimer tous les objets détectés.

L'application inscrit les informations sur les menaces détectées et les actions exécutées dans les rapports de l'application (→ **Rapports**). Vous pouvez sélectionner l'affichage des rapports via l'Antivirus.

Exécution d'une analyse programmée

L'Antivirus possède une série de restrictions :

- Lors du fonctionnement de l'Antivirus dans le profil de travail, il est impossible d'éliminer automatiquement la menace détectée dans la mémoire externe de l'appareil (par exemple, sur la carte SD) (Applications avec "portefeuille", Configuration du profil de travail Android). Kaspersky Endpoint Security for Android n'a pas dans le profil de travail accès à la mémoire externe. Les informations sur les objets détectés s'affichent dans la section **État** de l'app. Pour éliminer les objets détectés dans la mémoire externe, il faut supprimer le fichier à la main et lancer à nouveau l'analyse de l'appareil.

- En raison de restrictions techniques, Kaspersky Endpoint Security for Android n'est pas capable d'analyser les fichiers de 2 Go ou plus. Dans le cadre de l'analyse, l'app ignore ces fichiers et ne les signale pas.

Pour configurer la programmation de l'analyse complète de l'appareil, procédez comme suit :

1. Dans la fenêtre principale de Kaspersky Endpoint Security ouvrez le volet de lancement rapide et cliquez sur → **Paramètres** → **Anti-Virus** → **Analyse**.

2. Appuyez sur **Planification** et sélectionnez la fréquence de lancement de l'analyse complète :

   - **Une fois par semaine**
   - **Daily**
   - **Désactivé**
   - **Après la mise à jour des bases**

3. Cliquez sur **Jour du lancement** et sélectionnez le jour de la semaine où l'analyse complète sera lancée.

4. Cliquez sur **Heure du lancement** et indiquez l'heure du lancement de l'analyse complète.

L'analyse complète de l'appareil est lancée selon une programmation.

Sur Android 12 ou une version ultérieure, l'application peut effectuer cette tâche plus tard que prévu si l'appareil est en mode d'économie de la batterie.

Modification du mode de protection

La Protection en temps réel permet de détecter les menaces dans les fichiers ouverts, d'analyser les applications en temps réel lors de leur installation sur l'appareil. Pour assurer la protection automatiquement, les bases antivirus et le service cloud Kaspersky Security Network (Protection cloud) sont utilisés.

Pour configurer le mode de protection de l'appareil, procédez comme suit :

1. Dans la fenêtre principale de Kaspersky Endpoint Security, dans le volet de lancement rapide, appuyez sur → **Paramètres** → **Antivirus** → **Protection en temps réel**.

2. Sélectionnez le mode de protection de l'appareil :

   - **Désactivée**. La protection est désactivée.

   - **Recommandé**. Anti-Virus analyse uniquement les apps installées et les fichiers du dossier "Téléchargements". L'Anti-Virus analyse les nouvelles applications une fois, directement après l'installation.

   - **Avancé**. L'Anti-Virus recherche la présence éventuelle d'objets malveillants dans tous les fichiers de l'appareil pour toute action les concernant (par exemple, enregistrement, déplacement ou modification). L'Anti-Virus analyse également les nouvelles applications directement après leur installation.

Les informations relatives au de mode de protection en vigueur apparaissent sous la description du composant.

L'accès aux paramètres de la protection en temps réel peut être limité par votre administrateur.

Pour activer la Protection cloud (KSN), procédez comme suit :

1. Dans la fenêtre principale de Kaspersky Endpoint Security ouvrez le volet de lancement rapide et cliquez sur → **Paramètres** → **Antivirus**.

2. Activez le commutateur **Protection cloud (KSN)**.

   Le commutateur **Protection cloud (KSN)** administre l'utilisation de Kaspersky Security Network seulement pour la protection en temps réel de l'appareil. Si la case est désactivée, Kaspersky Endpoint Security continue d'utiliser KSN pour faire fonctionner les autres composants de l'application.

Ainsi, l'application a accès à la base opérationnelle de connaissances de Kaspersky sur la réputation des fichiers et des applications. L'analyse est effectuée sur les menaces dont les informations ne figurent pas encore dans les bases antivirus mais se trouvent déjà dans KSN. Le service cloud de Kaspersky Security Network assure le bon fonctionnement de l'Antivirus et réduit la probabilité de faux positifs. Seul votre administrateur peut entièrement désactiver l'utilisation de Kaspersky Security Network.

Pour configurer la protection en temps réel, procédez comme suit :

1. Dans la fenêtre principale de Kaspersky Endpoint Security, dans le volet de lancement rapide, appuyez sur → **Paramètres** → **Antivirus** →**Protection en temps réel**.

2. Si vous souhaitez que lors de l'analyse, l'application ne détecte les applications publicitaires et les programmes pouvant être exploités par des individus malintentionnés pour nuire au appareil ou à vos données, cochez la case **Publicité, numéroteurs et autres**.

3. Cliquez sur **Action en cas de détection d'une menace**, et sélectionnez l'action de l'application par défaut :

   - **Quarantaine**

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.

- **Supprimer**

  Les objets détectés sont automatiquement supprimés. Aucune action supplémentaire n'est requise. Avant la suppression, Kaspersky Endpoint Security affiche une notification temporaire sur la détection de l'objet.

- **Ignorer**

  Si des objets détectés ont été ignorés, Kaspersky Endpoint Security vous avertit de la présence de problèmes dans la protection de l'appareil. Les informations sur les objets ignorés s'affichent dans la section **État** de l'app. Pour chaque menace ignorée, vous avez le choix entre plusieurs actions pour l'éliminer. Le contenu de la liste des objets ignorés peut changer, par exemple si un fichier malveillant est supprimé ou déplacé. Pour obtenir la liste actuelle des menaces, lancez une analyse complète de l'appareil. Afin de vraiment garantir la protection des données, il est conseillé de supprimer tous les objets détectés.

L'application inscrit des informations sur les menaces détectées et les actions exécutées dans les rapports de l'application (→ **Paramètres** → **Rapports**). Vous pouvez sélectionner l'affichage des rapports via l'Antivirus.

Mise à jour des bases antivirus

Pour mettre à jour les bases antivirus de l'application,

dans la fenêtre principale de Kaspersky Endpoint Security, ouvrez le volet de lancement rapide et touchez **Mise à jour des bases de données**.

Mise à jour des bases selon la planification

L'application peut mettre à jour automatiquement les bases antivirus en fonction de la programmation définie.

Pour planifier une mise à jour, procédez comme suit :

1. Dans la fenêtre principale de Kaspersky Endpoint Security, ouvrez le volet de lancement rapide et cliquez sur → **Paramètres** → **Antivirus** → **Mise à jour des bases de données**.
2. Cliquez sur **Planification** et sélectionnez la fréquence du lancement de la mise à jour :
   - **Une fois par semaine**
   - **Daily**
   - **Désactivé**
3. Cliquez sur **Jour du lancement** et sélectionnez le jour de la semaine où il est nécessaire de lancer la mise à jour.
4. Cliquez sur **Heure du lancement** et indiquez l'heure du lancement de la mise à jour.

La mise à jour des bases antivirus est lancée selon une programmation.

Sur Android 12 ou une version ultérieure, l'application peut effectuer cette tâche plus tard que prévu si l'appareil est en mode d'économie de la batterie.

Actions en cas de perte ou de vol de l'appareil

En cas de vol ou de perte de votre appareil, contactez votre administrateur système. L'administrateur lance à distance sur le périphérique les fonctions d'Antivol conformément aux exigences de la sécurité d'entreprise.

Si une commande de rétablissement des paramètres par défaut est envoyée à l'appareil, le contrôle de l'appareil sera perdu et les autres commandes Antivol ne fonctionneront pas.

Protection Internet

Pour activer la Protection Internet :

- Kaspersky Endpoint Security doit être activé en tant que service des Fonctionnalités d'accessibilité.
- Vous devez accepter la Déclaration relative au traitement des données aux fins d'utilisation de la Protection Internet (Déclaration sur la Protection Internet). Kaspersky Endpoint Security utilise Kaspersky Security Network (KSN) pour analyser les sites Internet. La Déclaration sur la Protection Internet contient les conditions générales de l'échange de données avec KSN.

  Votre administrateur peut accepter la Déclaration sur la Protection Internet pour vous dans Kaspersky Security Center. Dans ce cas, vous n'avez rien à faire.

  Si votre administrateur n'a pas accepté la Déclaration sur la Protection Internet et qu'il vous a envoyé la demande, vous devez lire et accepter la Déclaration sur la Protection Internet dans les paramètres de l'application.

  Si votre administrateur n'a pas accepté la Déclaration sur la Protection Internet, la Protection Internet n'est pas disponible.

La Protection Internet sur les appareils Android fonctionne seulement dans les navigateurs Google Chrome (y compris la fonction Onglets personnalisés), Huawei Browser et Samsung Internet Browser. La Protection Internet pour le navigateur Samsung Internet ne bloque pas les sites sur un appareil mobile si un profil de travail est utilisé et que la Protection Internet est activée uniquement pour ce profil de travail.

Si vous voulez que la Protection Internet analyse constamment les sites Internet pendant la navigation, faites de Google Chrome ou de Samsung Internet Browser le navigateur par défaut.

Pour définir le navigateur pris en charge comme navigateur par défaut et utiliser la Protection Internet pour l'analyse permanente des sites Internet, procédez comme suit :

1. Dans la fenêtre principale de Kaspersky Endpoint Security, ouvrez le volet de lancement rapide et cliquez sur → **Paramètres** → **Protection Internet**.
2. Activez la **Protection Internet** via l'interrupteur.
3. Appuyez sur **Définir le navigateur par défaut** .

   Ce bouton s'affiche si la Protection Internet est activée, mais que le navigateur pris en charge n'est pas défini en tant que navigateur par défaut.

   L'Assistant de sélection du navigateur par défaut est lancé.

4. Suivez les indications de l'assistant.

   Après l'exécution de l'assistant, Google Chrome, Huawei Browser ou Samsung Internet Browser est défini comme navigateur par défaut. La Protection Internet analysera constamment les sites Internet pendant la navigation.

Contrôle des applications installées

Le *Contrôle des applications* vérifie si les apps installées sur l'appareil mobile répondent aux exigences de sécurité de l'entreprise. L'administrateur dresse dans Kaspersky Security Center les listes des applications autorisées, interdites, nécessaires et recommandées conformément aux exigences de sécurité de l'entreprise. Pendant son utilisation, le Contrôle des applications de Kaspersky Endpoint Security propose d'installer les applications nécessaires et recommandées et de supprimer les applications interdites. Le lancement d'une applications interdite sur l'appareil mobile est alors impossible.

Pour installer les applications nécessaires et recommandées ou supprimer des applications interdites, procédez comme suit :

1. Passez à la section **État** de Kaspersky Endpoint Security.
2. Choisissez les tâches du Contrôle des applications.
3. Exécutez les options d'action proposées.

Obtention du certificat

Pour obtenir un certificat permettant d'accéder au réseau d'entreprise, procédez comme suit :

1. Dans la fenêtre principale de Kaspersky Endpoint Security, ouvrez le volet de lancement rapide et cliquez sur → **Paramètres** → **Avancé** → **Obtention du certificat**.
2. Indiquez vos identifiants dans le réseau de l'organisation.
3. Si vous avez reçu un mot de passe à usage unique de l'administrateur, cochez la case **Mot de passe à usage unique** et entrez le mot de passe reçu.

   L'assistant d'installation du certificat s'ouvre.
4. Suivez les indications de l'assistant.

Synchronisation avec Kaspersky Security Center

La synchronisation de l'appareil mobile avec le système d'administration à distance Kaspersky Security Center est indispensable pour la protection et la configuration de votre appareil conformément aux exigences de sécurité de l'entreprise. La synchronisation de l'appareil avec Kaspersky Security Center est exécutée automatiquement. Vous pouvez également lancer la synchronisation à la main. Après la première synchronisation, votre appareil est ajouté à la liste des appareils mobiles administrés via Kaspersky Security Center. Ensuite, l'administrateur peut configurer votre appareil conformément aux exigences de sécurité de l'entreprise.

Vous pouvez définir les valeurs des paramètres de synchronisation pendant l'exécution de l'assistant de configuration initiale ou dans les paramètres de Kaspersky Endpoint Security. Les paramètres de synchronisation doivent être configurés si vous avez installé Kaspersky Endpoint Security à l'aide de Google Play. Pour obtenir les valeurs des paramètres de synchronisation, contactez l'administrateur.

Modifiez les paramètres de synchronisation du périphérique avec le système d'administration à distance Kaspersky Security Center uniquement sur instruction de l'administrateur.

Pour synchroniser le périphérique avec Kaspersky Security Center, procédez comme suit :

1. Dans la fenêtre principale de Kaspersky Endpoint Security, ouvrez le volet de lancement rapide et cliquez sur → **Paramètres** → **Synchronisation**.
2. Dans la section **Paramètres de synchronisation** indiquez la valeur des paramètres suivants :
   - **Serveur**
   - **Port**
   - **Groupe**
   - **Adresse email professionnelle**

   Les paramètres de synchronisation peuvent être masqués par l'administrateur.
3. Cliquez sur **Synchroniser**.

Activation de l'application Kaspersky Endpoint Security for Android sans Kaspersky Security Center

Dans la plupart des cas, l'application Kaspersky Endpoint Security for Android installée sur votre appareil est activée par l'administrateur de manière centralisée dans le système d'administration à distance de Kaspersky Security Center. Si votre appareil n'est pas connecté à Kaspersky Security Center, vous pouvez saisir le code d'activation manuellement. Pour obtenir le code d'activation, contactez l'administrateur.

Activez l'application manuellement uniquement lorsque l'administrateur vous le demande.

Pour saisir le code d'activation :

1. Dans le message d'erreur indiquant que votre licence va bientôt expirer ou a expiré et que votre appareil n'est pas connecté au Serveur d'administration, appuyez sur **Activer**.
2. Dans la fenêtre d'activation, saisissez le code d'activation que l'administrateur vous a donné, puis appuyez sur **Activer**.
3. Si le code d'activation est correct, une notification reprenant la date d'expiration de la licence s'affiche pour signaler que l'application a été activée.

L'application Kaspersky Endpoint Security for Android sur votre appareil est activée.

Mise à jour de l'application

Kaspersky Endpoint Security peut être mis à jour par les moyens suivants :

- Par vous-même à l'aide de Google Play. Vous téléchargez de Google Play une nouvelle version de l'application et l'installez sur votre périphérique.
- Avec l'aide de l'administrateur. L'administrateur met à jour à distance la version de l'application sur votre appareil à l'aide du système d'administration à distance Kaspersky Security Center.

Mise à jour à l'aide de Google Play

L'administrateur peut vous empêcher de mettre l'app à jour via Google Play.

La mise à jour à l'aide de Google Play s'effectue par un moyen classique compatible avec la plateforme Android. Pour la mise à jour de l'application, les conditions suivantes doivent être remplies :

- Vous devez avoir un compte Google.
- Le périphérique doit être associé au compte Google.
- L'appareil doit disposer d'une connexion à Internet.

Pour en savoir plus sur la création d'un compte Google, sur l'association de l'appareil au compte ou sur l'utilisation de l'app Google Play Store, consultez le site d'assistance technique de Google.

Mise à jour à l'aide de Kaspersky Security Center

La mise à jour de l'app à l'aide de Kaspersky Security Center comprend les étapes suivantes :

1. L'administrateur envoie sur votre appareil mobile la distribution de l'app dont la version répond aux exigences de sécurité de l'entreprise.

   Une invite d'installation de Kaspersky Endpoint Security sur votre appareil s'affiche.

2. Acceptez les conditions de la mise à jour.

   La nouvelle version de l'app est installée sur l'appareil. Il n'est pas nécessaire de configurer l'app après la mise à jour.

Suppression de l'application

L'administrateur peut vous interdire de supprimer vous-même l'app. Dans ce cas, la suppression de Kaspersky Endpoint Security est impossible.

Kaspersky Endpoint Security peut être supprimé en suivant une de ces méthodes :

- par l'utilisateur dans les paramètres de l'app.
- par l'utilisateur dans les paramètres de l'appareil.
- Avec l'aide de l'administrateur. L'administrateur supprime l'application à distance de votre appareil à l'aide du système d'administration à distance de Kaspersky Security Center.

Suppression dans les paramètres de l'app.

Pour supprimer Kaspersky Endpoint Security de votre appareil, procédez comme suit :

1. Dans la fenêtre principale de Kaspersky Endpoint Security, ouvrez le volet de lancement rapide et cliquez sur → **Supprimer l'app**.

   L'Assistant de suppression de l'app. s'ouvre.

2. Suivez les indications de l'assistant.

Suppression dans les paramètres de l'appareil.

La suppression de l'app s'effectue selon la méthode classique pour la plate-forme Android. Pour supprimer l'app, il faut désactiver les privilèges d'administrateur pour Kaspersky Endpoint Security dans les paramètres de sécurité de l'appareil.

Sur les appareils tournant sous le système d'exploitation Android version 7.0 et suivants, si l'administrateur a interdit la suppression, l'appareil sera bloqué en cas de tentative de suppression de l'app dans les paramètres d'Android. Pour débloquer l'appareil, contactez votre administrateur.

Suppression à l'aide de Kaspersky Security Center

La suppression de l'application à l'aide de Kaspersky Security Center comprend les étapes suivantes :

1. L'administrateur envoie à votre appareil mobile la commande de suppression de l'app.

   Votre appareil mobile affiche une invite pour confirmer la suppression de Kaspersky Endpoint Security.

2. Confirmez la suppression de l'app.

   L'app sera supprimée de votre appareil.

Application avec "portefeuille"

Icône de l'app dans le profil de travail Android

Les apps signalées par l'icône de portefeuille (apps d'entreprise) se trouvent sur votre appareil dans le profil de travail Android (ci-après, "profil de travail"). Le *profil de travail Android* est un environnement sécurisé sur votre appareil dans lequel l'administrateur peut gérer les apps et les comptes utilisateur sans limiter vos possibilités d'utilisation de données personnelles.

Le profil de travail permet de séparer les données d'entreprise des données personnelles. Cela garantit la confidentialité des données d'entreprise et leur protection contre les applications malveillantes. Lors de la création d'un profil professionnel sur votre périphérique, les applications d'entreprise suivantes sont installées automatiquement : Google Play Store, Google Chrome, Téléchargements, Kaspersky Endpoint Security for Android, etc.

App KNOX

Identification KNOX

L'app KNOX ouvre le conteneur KNOX sur l'appareil. Le *conteneur KNOX* est un environnement sécurisé sur votre appareil. Ce conteneur comprend son propre écran d'accueil, son propre dispositif de lancement, ainsi que ses propres apps et widgets. L'administrateur peut administrer les apps et les compte utilisateur dans le conteneur KNOX sans limiter vos possibilités d'utiliser vos données personnelles.

Le conteneur KNOX permet d'enregistrer les donnés d'entreprise à l'écart des données personnelles. Cela garantit la confidentialité des données d'entreprise et leur protection contre les applications malveillantes.

Le conteneur KNOX permet d'accéder à la boîte aux lettres d'entreprise, aux coordonnées des employés de l'organisation, aux stockages de fichiers et à d'autres apps.

Pour en savoir plus sur l'utilisation de KNOX, consultez le *site de l'assistance technique de Samsung*.

Licence de l'application

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

A propos du Contrat de licence

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

Lisez attentivement les Conditions générales du CLUF avant de commencer à utiliser Kaspersky Security for Mobile.

Vous pouvez consulter les Conditions générales du CLUF de la manière suivante :

- 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.
- Dans l'application Kaspersky Endpoint Security for Android dans la section **Infos sur l'application**.
- Dans la section **Avancé** → **Contrats de licence acceptés** des propriétés du Serveur d'administration. Cette fonction est disponible dans Kaspersky Security Center version 12.1.

Vous acceptez les Conditions générales du Contrat de licence utilisateur final (CLUF), 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 annuler 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 :

- *Essai*.

  Une licence gratuite conçue pour découvrir Kaspersky Security for Mobile.

La licence d'essai a une durée de validité de 30 jours. A l'expiration du délai de validité de la licence d'essai, l'application mobile Kaspersky Endpoint Security for Android cesse d'assurer la plupart des fonctions, excepté la synchronisation avec le Serveur d'administration. Pour continuer à utiliser l'app, vous devez acheter une licence commerciale.

- *Commerciale*.

  Une licence fournie lors de l'achat de Kaspersky Security for Mobile.

  A l'expiration du délai de validité de la licence commerciale, l'application mobile continue à fonctionner mais en mode limité. Dans le mode limité, les composants suivants sont accessibles dans l'application Kaspersky Endpoint Security for Android :

  - **Antivirus**.

    La Protection en temps réel et la Recherche de virus dans l'appareil sont disponibles, mais la mise à jour des bases antivirus est inaccessible.

  - **Antivol**.

    Seul l'envoi de commandes vers un appareil mobile est disponible.

  - **Synchronisation à l'aide du Serveur d'administration**.

  Les autres composants de l'application Kaspersky Endpoint Security for Android sont inaccessibles à l'utilisateur de l'appareil. L'administrateur peut administrer ces composants en mode limité à l'aide de stratégies de groupe. Il est impossible de configurer les autres composants de l'application à l'aide de stratégies de groupe.

L'application Kaspersky Endpoint Security for Android cesse l'échange d'informations avec Kaspersky Security Network, Google Analytics pour Firebase, SafetyNet Attestation, Firebase Performance Monitoring et Crashlytics en cas de blocage de la clé de Kaspersky à l'expiration du délai de validité de la licence essai et en l'absence de la licence (le code d'activation est supprimé de la stratégie de groupe).

Pour poursuivre l'utilisation de l'application en mode de fonctionnement complet, vous devez proroger 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'app continue à fonctionner. Le fournisseur de services détermine l'existence et la durée de la période de renouvellement à tarif préférentiel.

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'app continue à fonctionner après la date d'expiration.

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

A propos de la clé

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

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 par exemple en cas de non-respect des conditions du Contrat de licence utilisateur final. Si une clé est bloquée, l'application mobile Kaspersky Endpoint Security for Android désactive toutes les fonctions, excepté la synchronisation avec le Serveur d'administration. Pour continuer à utiliser l'application, vous devez ajouter une autre clé.

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.

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 le restaurer, vous devrez contacter le Support Technique de Kaspersky.

A propos du fichier clé

Le *fichier clé* est un fichier doté d'une extension key qui vous est fourni par Kaspersky. 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.

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 distributeur de la licence ;
- Obtenir le fichier clé sur le site Internet de Kaspersky à partir du code d'activation que vous possédez.

Collecte des données

Kaspersky Security for Mobile correspond aux normes générales de protection des données (GDPR).

Pour installer l'application, vous ou l'utilisateur de l'application doit lire et accepter les conditions du Contrat de licence utilisateur final. De plus, vous pouvez configurer une stratégie pour accepter globalement les Déclarations répertoriées ci-dessous, pour tous les utilisateurs. Dans le cas contraire, les utilisateurs seront invités par une notification sur l'écran principal de l'application à accepter les Déclarations suivantes concernant le traitement des données personnelles de l'utilisateur :

- Déclaration de Kaspersky Security Network
- Déclaration sur le traitement des données pour la Protection Internet
- Déclaration sur le traitement des données à des fins marketing

Si vous optez pour l'acceptation globale des déclarations, les versions des déclarations acceptées via Kaspersky Security Center doivent correspondre aux versions déjà acceptées par les utilisateurs. Dans le cas contraire, les utilisateurs seront informés du problème et invités à accepter la version d'une déclaration qui correspond à la version acceptée globalement par l'administrateur. L'état de l'appareil dans le Plug-in d'administration de Kaspersky Endpoint Security for Android passera également à *Avertissement*.

L'utilisateur peut à n'importe quel moment accepter les conditions de l'application ou les refuser dans la section **Infos sur l'application** des paramètres de Kaspersky Endpoint Security for Android.

Échange d'informations avec Kaspersky Security Network

Pour améliorer la protection en temps réel, Kaspersky Security for Mobile utilise le service cloud de Kaspersky Security Network pour les composants suivants :

- **Antivirus.** L'application a accès à la base opérationnelle de connaissances de Kaspersky sur la réputation des fichiers et des applications. L'analyse est effectuée sur les menaces dont les informations ne figurent pas encore dans les bases antivirus mais se trouvent déjà dans KSN. Le service cloud de Kaspersky Security Network assure le bon fonctionnement de l'Antivirus et réduit la probabilité de faux positifs.
- **Protection Internet.** L'application utilise les données reçues de la part de KSN pour analyser les sites Internet avant leur ouverture. L'application définit aussi la catégorie du site Internet pour contrôler l'accès des

utilisateurs au réseau Internet sur la base des listes de catégories autorisées et interdites (par exemple, la catégorie "Communication via Internet").

- **Contrôle des applications.** L'application définit la catégorie de l'application pour la restriction du lancement de l'application qui ne satisfait pas aux exigences de sécurité de l'entreprise, à partir des listes de catégories autorisées et interdites (par exemple, catégorie "Jeux").

Le Contrat de licence utilisateur final détaille la nature des données transmises à Kaspersky lorsque le KSN est utilisé parallèlement Anti-Virus et Contrôle des applications. En acceptant les termes du Contrat de licence, vous consentez à transmettre les informations suivantes.

Les informations sur le type de données soumises à Kaspersky lors de l'utilisation de KSN pendant le fonctionnement de la Protection Internet sont disponibles dans la Déclaration concernant le traitement des données pour la Protection Internet. En acceptant les termes de la Déclaration, vous consentez à transmettre les informations suivantes.

La Déclaration de Kaspersky Security Network détaille la nature des données statistiques transmises à Kaspersky lorsque le KSN est utilisé parallèlement à l'application mobile Kaspersky Endpoint Security for Android sur les appareils des utilisateurs. En acceptant les termes de la Déclaration, vous consentez à transmettre les informations suivantes.

Divulgation des données dans le cadre du Contrat de licence utilisateur final

Si un Code d'activation est utilisé pour activer le Logiciel, l'Utilisateur final accepte de fournir périodiquement les informations suivantes au Détenteur des droits afin de vérifier son utilisation légitime :

- format des données dans la requête adressée à l'infrastructure du Détenteur des droits ; l'adresse IPv4 du service Web à laquelle l'utilisateur a accédé ; taille du contenu de la requête à l'infrastructure du Détenteur des droits ; identifiant du protocole ; code d'activation du Logiciel ; type de compression de données ; identifiant du Logiciel ; ensemble d'identifiants du Logiciel qui peuvent être activés sur l'appareil de l'utilisateur ; localisation du Logiciel ; version complète du Logiciel ; identifiant unique de l'appareil ; date et heure sur l'appareil de l'utilisateur ; identifiant de l'installation du Logiciel (PCID) ; version du système d'exploitation, numéro de version du système d'exploitation, numéro de mise à jour du système d'exploitation, édition du système d'exploitation, informations détaillées relatives à l'édition du système d'exploitation. modèle de l'appareil ; famille du système d'exploitation ; format des données dans la requête adressée à l'infrastructure du Détenteur des droits ; type de somme de contrôle de l'objet en cours de traitement ; en-tête de licence du Logiciel ; identifiant d'un centre d'activation régional ; date et heure de création de la clé de licence du Logiciel ; l'identifiant de licence ; identifiant du modèle d'information utilisé pour fournir la licence du Logiciel ; date et heure d'expiration de la licence du Logiciel ; état actuel de la clé de licence du Logiciel ; type de licence utilisée pour le Logiciel ; type de licence utilisée pour activer le Logiciel ; identifiant du Logiciel dérivé de la licence ;

Afin de protéger l'Ordinateur contre les menaces de sécurité de l'information, l'Utilisateur final accepte de fournir périodiquement les informations suivantes :

- type de somme de contrôle de l'objet en cours de traitement ; somme de contrôle de l'objet en cours de traitement ; l'identifiant du composant du Logiciel ;

- identifiant de la signature déclenchée dans les bases de données antivirus du Logiciel ; date et heure de la signature déclenchée dans les bases de données antivirus du Logiciel ; type de signature déclenchée dans les bases de données antivirus du Logiciel ; nom de l'application malveillante ou du logiciel légitime détecté qui peuvent être utilisés pour endommager l'appareil ou les données de l'utilisateur ;

- nom de la boutique à partir de laquelle l'application a été installée ; nom du paquet de l'application ; clé publique utilisée pour signer le fichier APK ; somme de contrôle du certificat utilisé pour signer le fichier APK ; date et heure du certificat numérique;

- version complète du Logiciel ; identifiant de la mise à jour du Logiciel ; type de Logiciel installé ; identifiant de la configuration ; le résultat de l'action du Logiciel ; code d'erreur ;

- nombres qui sont dérivés du fichier APK de l'application Android selon certaines règles mathématiques et qui ne permettent pas de restaurer le contenu du fichier original ; ces données ne contiennent pas de noms de fichiers, de chemins d'accès, d'adresses, de numéros de téléphone ni d'autres informations personnelles des utilisateurs.

Si Vous utilisez les serveurs de mise à jour du Titulaire des droits pour télécharger les Mises à jour, l'Utilisateur final, dans le but d'augmenter l'efficacité de la procédure de mise à jour, accepte de fournir périodiquement au Titulaire des droits les informations suivantes :

- identifiant du Logiciel dérivé de la licence ; version complète du Logiciel ; l'identifiant de licence ; type de licence utilisée pour le Logiciel ; identifiant de l'installation du Logiciel (PCID) ; identifiant du début de la mise à jour du Logiciel ; adresse Internet en cours de traitement.

Le Titulaire des droits peut également utiliser ces informations pour recueillir des données statistiques concernant la distribution et l'utilisation du Logiciel.

Les informations obtenues sont protégées par Kaspersky conformément aux exigences établies par la loi. 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) ou à la demande de l'utilisateur. Les données des statistiques générales sont conservées de manière illimitée.

Divulgation de données dans le cadre de la Déclaration de Kaspersky Security Network

Toute utilisation de KSN pourrait accroître l'efficacité de la protection fournie par le Logiciel, notamment contre les menaces de sécurité du réseau et des informations.

Si vous utilisez une licence pour 5 nœuds ou plus, le titulaire des droits recevra et traitera automatiquement les données suivantes lors de l'utilisation du KSN :

- identifiant de la signature déclenchée dans les bases de données antivirus du Logiciel ; date et heure de la signature déclenchée dans les bases de données antivirus du Logiciel ; type de signature déclenchée dans les bases de données antivirus du Logiciel ; date et heure de publication des bases de données du Logiciel ; version du système d'exploitation, numéro de version du système d'exploitation, numéro de mise à jour du système d'exploitation, édition du système d'exploitation, informations détaillées relatives à l'édition du système d'exploitation. version du Service Pack du système d'exploitation ; caractéristiques de détection ; somme de contrôle (MD5) de l'objet en cours de traitement ; nom de l'objet en cours de traitement ; indicateur précisant si l'objet en cours de traitement est un fichier PE ; somme de contrôle (MD5) du masque qui a bloqué le service Web ; somme de contrôle (SHA256) de l'objet en cours de traitement ; taille de l'objet en cours de traitement ; code du type d'objet ; décision du Logiciel sur l'objet en cours de traitement ; chemin d'accès vers l'objet en cours de traitement ; code de répertoire ; version du composant du Logiciel ; version des statistiques en cours d'envoi ; adresse d'accès du service Web (URL, IP) ; type de client utilisé pour accéder au service Internet ; l'adresse IPv4 du service Web à laquelle l'utilisateur a accédé ; l'adresse IPv6 du service Web à laquelle l'utilisateur a accédé ; adresse Internet de la source de la requête du service Web (référant) ; adresse Internet en cours de traitement.

- informations concernant les objets analysés (version de l'application dans le fichier AndroidManifest.xml ; la décision du Logiciel sur l'application ; méthode utilisée pour obtenir la décision du Logiciel sur l'application ; nom du paquet d'installation de la boutique ; nom du paquet (ou de l'offre groupée) dans le fichier AndroidManifest.xml ; catégorie Google SafetyNet ; indicateur précisant si la fonctionnalité SafetyNet est activée sur l'appareil ; valeur SHA256 de la réponse Google SafetyNet ; schéma de signature APK pour le certificat APK ; code de version du Logiciel installé ; numéro de série du certificat utilisé pour signer le fichier APK ; nom du fichier APK installé ; chemin d'accès au fichier APK installé ; émetteur du certificat utilisé pour signer le fichier APK ; clé publique utilisée pour signer le fichier APK ; somme de contrôle du certificat utilisé pour signer le fichier APK ; date et heure d'expiration du certificat ; date et heure d'émission du certificat ;

version des statistiques en cours d'envoi ; algorithme de calcul de l'empreinte du certificat numérique ; hachage MD5 du fichier APK installé ; hachage MD5 du fichier DEX situé dans le fichier APK ; autorisations octroyées à l'application de façon dynamique ; version du logiciel tiers ; indicateur précisant si l'application est la messagerie SMS par défaut ; indicateur précisant si l'application possède des droits d'administration sur l'appareil ; indicateur précisant si l'application se trouve dans le catalogue système ; indicateur précisant si l'application utilise des services d'accessibilité.

- informations concernant tous les objets et activités potentiellement malveillants (contenu en fragments de l'objet en cours de traitement ; date et heure d'expiration du certificat ; date et heure d'émission du certificat ; identifiant de la clé à partir de la boutique de clés utilisé pour le chiffrement ; protocole utilisé pour l'échange de données avec KSN ; ordre des fragments dans l'objet en cours de traitement ; données du journal interne généré par le module antivirus du Logiciel pour un objet en cours de traitement ; nom de l'émetteur du certificat ; clé publique du certificat ; algorithme de calcul de la clé publique du certificat ; numéro de série du certificat ; date et heure de la signature de l'objet ; nom et paramètres du propriétaire du certificat ; empreinte du certificat numérique de l'objet analysé et de l'algorithme de hachage ; date et heure de la dernière modification de l'objet en cours de traitement ; date et heure de création d'un objet en cours de traitement ; objets ou ses parties en cours de traitement ; description d'un objet en cours de traitement comme défini dans les propriétés de l'objet ; format de l'objet en cours de traitement ; type de somme de contrôle de l'objet en cours de traitement ; somme de contrôle (MD5) de l'objet en cours de traitement ; nom de l'objet en cours de traitement ; somme de contrôle (SHA256) de l'objet en cours de traitement ; taille de l'objet en cours de traitement ; nom du fournisseur du Logiciel ; décision du Logiciel sur l'objet en cours de traitement ; version de l'objet en cours de traitement ; source de la décision prise pour l'objet en cours de traitement ; somme de contrôle de l'objet en cours de traitement ; nom de l'application parente ; chemin d'accès vers l'objet en cours de traitement ; informations relatives aux résultats de la vérification de la signature des fichiers ; clé de session de connexion ; algorithme de chiffrement pour la clé de session de connexion ; temps de stockage de l'objet en cours de traitement ; algorithme de calcul de l'empreinte du certificat numérique).

- type de version, par exemple "utilisateur" ou "ing" ; nom complet du produit ; fabricant de produits/matériels ; si les applications peuvent être installées à partir d'une autre source que Google Play ; statut du service cloud pour vérifier les applications Google ; statut du service cloud pour vérifier les applications Google installées via ADB ; nom de code actuel du développement ou chaîne "REL" pour les versions de production ; numéro de version incrémentiel ; chaîne de version visible par l'utilisateur ; nom de l'appareil de l'utilisateur ; identifiant de version du Logiciel visible par l'utilisateur ; empreinte du micrologiciel ; identifiant du micrologiciel ; indicateur précisant si l'appareil est associé à une racine ; système d'exploitation ; nom du Logiciel ; type de licence utilisée pour le Logiciel.

- informations concernant la qualité des services KSN (protocole utilisé pour l'échange de données avec KSN ; identifiant du service KSN auquel le Logiciel a accédé ; date et heure auxquelles les statistiques ont cessé d'être reçues ; nombre de connexions KSN prélevées à partir du cache ; nombre de requêtes pour lesquelles une réponse a été trouvée dans la base de données des requête locales ; nombre de connexions KSN ayant échoué ; nombre de transactions KSN ayant échoué ; répartition de temps des requête adressées à KSN annulées ; répartition de temps des connexions KSN ayant échoué ; répartition de temps des transactions KSN ayant échoué ; répartition de temps des connexions KSN réussies ; répartition de temps des transactions KSN réussies ; répartition de temps des requêtes adressées à KSN réussies ; répartition de temps des requêtes adressées à KSN ayant expiré ; nombre de nouvelles connexions KSN ; nombre de requêtes non abouties adressées à KSN en raison d'erreurs de routage ; nombre de requêtes non abouties causées par la désactivation de KSN dans les paramètres du Logiciel ; nombre de requêtes non abouties adressées à KSN en raison de problèmes de réseau ; nombre de connexions KSN ayant réussi ; nombre de transactions KSN ayant réussi ; nombre total de requêtes adressées à KSN ; date et heure auxquelles les statistiques ont commencé à être reçues).

- identifiant du périphérique ; version complète du Logiciel ; identifiant de la mise à jour du Logiciel ; identifiant de l'installation du Logiciel (PCID) ; type de Logiciel installé.

- hauteur de l'écran de l'appareil ; largeur de l'écran de l'appareil ; informations sur le chevauchement de l'application : hachage MD5 du fichier APK ; informations sur le chevauchement de l'application : hachage MD5 du fichier classes.dex ; informations sur le chevauchement de l'application : nom du fichier APK ; informations sur le chevauchement de l'application : chemin d'accès au fichier APK sans le nom du fichier ; hauteur de chevauchement ; informations sur les Logiciels qui se chevauchent : hachage MD5 du fichier APK ;

chevauchement des informations sur les applications : hachage MD5 du fichier classes.dex ; chevauchement des informations sur les applications : nom du fichier APK ; chevauchement des informations sur les applications : chemin d'accès au fichier APK sans le nom du fichier ; chevauchement des informations sur les applications : nom du paquet de l'application (pour l'application qui se chevauche : si la publicité est affichée sur un bureau vide, la valeur doit être "launcher") ; date et heure du chevauchement ; informations sur le chevauchement de l'application : nom du paquet de l'application ; largeur du chevauchement.

- Paramètres du point d'accès Wi-Fi utilisé (type d'appareil détecté ; paramètres DHCP (sommes de contrôle du protocole IPv6 passerelle local, DHCP IPv6, DNS1 IPv6, DNS2 IPv6 ; somme de contrôle de la longueur du préfixe réseau ; somme de contrôle de l'adresse locale IPv6) ; paramètres DHCP (sommes de contrôle de l'adresse IP locale de la passerelle, DHCP IP, DNS1 IP, DNS2 IP et masque de sous-réseau) ; indicateur précisant si le domaine DNS existe ou non ; somme de contrôle de l'adresse IPv6 locale affectée ; somme de contrôle de l'adresse IPv4 locale affectée ; indicateur précisant si l'appareil est branché ; type d'authentification du réseau Wi-Fi ; liste des réseaux Wi-Fi disponibles et leurs paramètres ; somme de contrôle (MD5 avec sel) de l'adresse MAC du point d'accès ; somme de contrôle (SHA256 avec sel) de l'adresse MAC du point d'accès ; types de connexion pris en charge par le point d'accès ; type de chiffrement du réseau Wi-Fi ; heure locale du début et de la fin de la connexion réseau Wi-Fi ; identifiant du réseau Wi-Fi basé sur l'adresse MAC du point d'accès ; identifiant du réseau Wi-Fi basé sur le nom du réseau Wi-Fi ; identifiant du réseau Wi-Fi basé sur le nom du réseau Wi-Fi et sur l'adresse MAC du point d'accès ; puissance du signal Wi-Fi ; Le nom du réseau Wi-Fi ; ensemble de protocoles d'authentification pris en charge par cette configuration ; protocole d'authentification utilisé pour une connexion WPA-EAP ; protocole d'authentification interne ; ensemble de chiffrements de groupe pris en charge par cette configuration ; ensemble de protocoles de gestion des clés pris en charge par cette configuration ; la catégorie de confidentialité finale du réseau dans le Logiciel ; la catégorie de sécurité finale du réseau dans le Logiciel ; ensemble de chiffrement de blocs pour le WPA qui sont pris en charge par cette configuration ; ensemble de protocoles de sécurité pris en charge par cette configuration).

- date et heure d'installation du Logiciel ; date d'activation du Logiciel ; identifiant de l'organisation partenaire à travers laquelle la licence du Logiciel a été achetée ; identifiant du Logiciel dérivé de la licence ; numéro de série de la clé de licence du Logiciel ; localisation du Logiciel ; indicateur précisant si la participation à KSN est activée ; identifiant du Logiciel sous licence ; l'identifiant de licence ; identifiant du SE ; version en bits du système d'exploitation.

En outre, afin d'atteindre l'objectif déclaré visant à améliorer l'efficacité de la protection fournie par le Logiciel, le Détenteur des droits peut recevoir des objets (fichier ou partie d'un fichier, informations sur le service) susceptibles d'être exploités par des intrus pour nuire à l'Ordinateur et créer des menaces de sécurité des informations.

La participation à Kaspersky Security Network pour le traitement des données statistiques est volontaire. Vous pouvez suspendre votre participation à Kaspersky Security Network à tout moment.

Collecte de données dans le cadre de la Déclaration sur le traitement des données pour la Protection Internet

Selon la Déclaration sur la Protection Internet, le Détenteur des droits traite les données dans l'ordre pour la fonctionnalité Protection Internet. L'objectif déclaré inclut la détection des menaces Internet et la détermination des catégories des sites Internet visités à l'aide du service cloud Kaspersky Security Network (KSN).

Avec votre consentement, les données suivantes seront envoyées automatiquement à intervalles réguliers au titulaire des droits conformément à la Déclaration sur la Protection Internet :

- Version du produit ; identifiant unique de l'appareil ; ID d'installation ; type de produit.

- L'adresse URL de la page, le numéro de port, le protocole URL, l'URL qui fait référence aux informations demandées.

La divulgation des données dans le cadre de la Déclaration sur le traitement des données à des fins marketing.

Le Titulaire des droits utilise des systèmes d'information tiers pour traiter les données. Son processus de traitement des données est régi par les déclarations de confidentialité desdits systèmes d'information tiers. Le titulaire des droits utilise les services suivants pour le traitement des données énumérées :

Google Analytics pour Firebase

Durant l'utilisation du Logiciel, les données suivantes seront envoyées à Google Analytics pour Firebase automatiquement et à intervalles réguliers afin de remplir l'objectif déclaré :

- Les informations sur l'app (la version et l'identifiant de l'app, ainsi que l'identifiant de l'app dans le service Firebase, l'identifiant de l'instance dans le service Firebase, le nom de la boutique où l'application a été achetée, l'horodatage du premier lancement du Logiciel)
- L'identifiant d'installation de l'app sur l'appareil et la méthode d'installation sur l'appareil
- La région et la localisation
- La résolution de l'écran de l'appareil
- Les informations sur l'utilisateur bénéficiant de privilèges de root
- Les informations de diagnostic sur l'appareil du service SafetyNet Attestation
- Les informations sur la configuration de Kaspersky Endpoint Security for Android en tant que fonctionnalité d'accessibilité
- Les informations sur les transitions entre les écrans de l'application, la durée de la session, le début et la fin d'une session d'écran, le nom de l'écran
- Le protocole utilisé pour envoyer des données au service Firebase, sa version, et l'identifiant de la méthode de soumission des données utilisée
- Les informations sur le type et les paramètres de l'événement pour lequel les données sont envoyées
- La licence de l'application, sa disponibilité, le nombre d'appareils
- Les informations sur la fréquence des mises à jour de la base antivirus et la synchronisation avec le Serveur d'administration
- La Console d'administration (Kaspersky Security Center ou systèmes EMM tiers)
- Identifiant Android
- Identifiant de publicité
- Informations relatives à l'Utilisateur : catégorie d'âge et sexe, identifiant du pays de résidence et liste d'intérêts
- Informations relatives à l'Ordinateur de l'Utilisateur sur lequel le Logiciel est installé : Informations sur l'ordinateur de l'Utilisateur sur lequel le Logiciel est installé : nom du fabricant de l'ordinateur, type d'ordinateur, modèle, version et langue (locale) du système d'exploitation, informations sur l'application ouverte pour la première fois au cours des 7 derniers jours et l'application ouverte pour la première fois il y a plus de 7 jours

  Les données sont transmises à Firebase via un canal sécurisé. Les informations relatives au traitement des données dans Firebase sont publiées à l'adresse suivante : https://firebase.google.com/support/privacy.

SafetyNet Attestation.

Durant l'utilisation du Logiciel, les données suivantes seront envoyées à l'API d'attestation SafetyNet automatiquement et à intervalles réguliers afin de remplir l'objectif déclaré :

- L'heure de vérification de l'appareil
- Les informations sur le Logiciel, le nom et les données relatives aux certificats logiciels
- Les résultats de la vérification de l'appareil
- Les vérifications d'identifiant aléatoires pour consulter les résultats de la vérification de l'appareil

  Les données sont transmises à l'API d'attestation SafetyNet via un canal sécurisé. Les informations relatives au traitement des données dans l'API d'attestation SafetyNet sont publiées à l'adresse suivante : https://policies.google.com/privacy.

Firebase Performance Monitoring

Durant l'utilisation du Logiciel, les données suivantes seront envoyées à l'API d'attestation SafetyNet automatiquement et à intervalles réguliers afin de remplir l'objectif déclaré :

- identifiant unique d'installation ;
- nom du paquet de l'application ;
- version du logiciel installé ;
- niveau de batterie et état de charge de la batterie ;
- opérateur ;
- état de premier plan ou d'arrière-plan de l'application ;
- géographie ;
- adresse IP ;
- code de langue de l'appareil ;
- informations relatives à la connexion radio/réseau ;
- identifiant pseudonyme de l'instance du Logiciel ;
- taille de la mémoire vive et du disque ;
- indicateur précisant si l'appareil est débridé ou associé à une racine ;
- puissance du signal ;
- durée des traces automatisées.
- réseau et les informations correspondantes suivantes : code de réponse, taille de la charge utile en octets, temps de réponse
- description de l'appareil

Les données sont transmises à Firebase via un canal sécurisé. Les informations relatives au traitement des données dans Firebase Performance Monitoring sont publiées à l'adresse suivante : https://firebase.google.com/support/privacy.

Crashlytics

Durant l'utilisation du Logiciel, les données suivantes seront envoyées à SafetyNet automatiquement et à intervalles réguliers afin de remplir l'objectif déclaré :

- identifiant du Logiciel ;
- version du logiciel installé ;
- indicateur précisant si le Logiciel fonctionnait en arrière-plan ;
- architecture du processeur ;
- identifiant unique de l'événement ;
- date et heure de l'événement ;
- modèle de l'appareil ;
- espace disque total et quantité actuellement utilisée ;
- nom et version du SE ;
- mémoire vive totale et quantité actuellement utilisée ;
- indicateur précisant si l'appareil est associé à une racine ;
- orientation de l'écran au moment de l'événement ;
- fabricant de produits/matériels ;
- identifiant unique d'installation ;
- version des statistiques en cours d'envoi ;
- le type d'exception du Logiciel ;
- texte du message d'erreur ;
- un indicateur précisant que l'exception du Logiciel a été causée par une exception imbriquée ;
- identifiant du flux de travail ;
- un indicateur précisant si l'image est la cause de l'erreur du Logiciel ;
- un indicateur précisant que le flux de travail a provoqué l'arrêt inattendu du Logiciel.
- informations à propos du signal qui a provoqué l'arrêt inattendu du Logiciel : nom du signal, code du signal, adresse du signal
- pour chaque image associée à un flux de travail, à une exception ou à une erreur : le nom du fichier de l'image, le numéro de ligne du fichier de l'image, les symboles de débogage, l'adresse et le décalage dans l'image binaire, le

nom d'affichage de la bibliothèque avec l'image, le type d'image, l'indicateur précisant si l'image est la cause de l'erreur

- identifiant du SE
- identifiant de la question associée à l'événement
- informations à propos des événements qui se sont produits avant que le Logiciel ne s'arrête de manière inattendue : identifiant de l'événement, date et heure de l'événement, type et valeur de l'événement
- valeurs du processeur enregistrées
- type et valeur d'événement

  Les données sont transmises à Facebook via un canal sécurisé. Les informations relatives au traitement des données dans Crashlytics sont publiées à l'adresse suivante : https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

La transmission des informations susmentionnées pour le traitement à des fins marketing s'effectue sur une base volontaire.

Contacter le Support Technique

Cette section contient des informations sur le mode et les conditions d'obtention de l'assistance technique.

Moyens de bénéficier du support technique

Si vous ne trouvez pas de solution à votre problème dans la documentation de Kaspersky Endpoint Security ni dans aucune des sources d'information sur l'application, contactez le Support Technique. Les experts du Support Technique répondront à toutes vos questions sur l'installation et l'utilisation de Kaspersky Endpoint Security.

Kaspersky prend en charge Kaspersky Endpoint Security pendant son cycle de vie (voir la page du cycle de vie du support produit). Avant de contacter le Support Technique, il est recommandé de lire les règles d'octroi du Support Technique.

Vous pouvez contacter les experts du Service de Support Technique d'une des manières suivantes:

- En visitant le site du Support Technique
- En envoyant une demande au Support Technique via le portail Kaspersky CompanyAccount

Assistance technique via Kaspersky CompanyAccount

Kaspersky CompanyAccount est un portail dédié aux entreprises utilisant les applications Kaspersky. Le portail Kaspersky CompanyAccount vise à faciliter l'interaction entre les utilisateurs et les spécialistes de Kaspersky via des requêtes électroniques. Vous pouvez utiliser Kaspersky CompanyAccount pour suivre l'état de vos requêtes électroniques et pour en stocker un historique également.

Vous pouvez inscrire tous les collaborateurs de votre société sous un même compte utilisateur Kaspersky CompanyAccount. Un compte utilisateur vous permet de gérer de manière centralisée les requêtes électroniques envoyées à Kaspersky par les collaborateurs inscrits et d'administrer les privilèges de ces collaborateurs dans Kaspersky CompanyAccount.

Le portail Kaspersky CompanyAccount est disponible dans les langues suivantes :

- anglais ;
- espagnol ;
- italien ;
- allemand ;
- polonais ;
- portugais ;
- russe ;
- français ;

- japonais.

Pour en savoir plus sur le Kaspersky CompanyAccount, veuillez consulter le site Internet du Service de Support Technique.

Autres sources d'informations sur l'application

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

La page Kaspersky Security for Mobile 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 Internet de Kaspersky Endpoint Security dans la base de connaissances

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

La page de Kaspersky Security for Mobile dans la Base de connaissances 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. 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 de l'application Kaspersky Endpoint Security permet de trouver des informations sur la configuration et l'utilisation de l'application mobile.

Discussion sur les applications Kaspersky dans notre communauté d'utilisateurs

Si votre question n'est pas urgente, vous pouvez la soumettre aux experts de Kaspersky et aux autres utilisateurs de nos applications dans notre communauté.

Dans la communauté, vous pouvez consulter les sujets de discussion, envoyer vos commentaires et créer de nouveaux sujets de discussion.

Glossaire

Abonnement

Permet l'utilisation de l'application selon des paramètres choisis (date d'expiration et nombre d'appareils). Vous pouvez suspendre ou reprendre l'abonnement, le renouveler automatiquement ou l'annuler.

Activation de l'application

Activation de toutes les fonctions de l'application. L'utilisateur effectue l'activation pendant ou après l'installation de l'application. Le code d'activation ou le fichier clé est nécessaire pour activer l'application.

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.

Administrateur de Kaspersky Security Center

Personne gérant les opérations de l'application via le système d'administration centralisée à distance de Kaspersky Security Center.

Appareil contrôlé

Appareil iOS dont les paramètres sont surveillés par Apple Configurator, application de configuration de groupe des appareils iOS. Les appareils supervisés possèdent l'état *supervised* dans Apple Configurator. Chaque fois qu'un appareil supervisé se connecte à l'ordinateur, Apple Configurator vérifie la configuration de cet appareil par rapport aux paramètres de référence spécifiés et les redéfinit si nécessaire. Les appareils supervisés ne peuvent pas être synchronisés avec une version d'Apple Configurator installée sur un autre ordinateur.

Chaque appareil supervisé fournit plus de paramètres à redéfinir via la stratégie Kaspersky Device Management for iOS qu'un appareil non supervisé. Par exemple, vous pouvez configurer un appareil proxy HTTP pour surveiller le trafic Internet sur un appareil du réseau d'entreprise. Par défaut, aucun appareil mobile n'est supervisé.

Appareil EAS

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

Appareil iOS MDM

Appareil mobile fonctionnant avec iOS et administré par le Serveur MDM iOS.

Bases antivirus

Base de données contenant des informations sur les menaces informatiques connues de Kaspersky depuis la publication des bases antivirus. Les entrées des bases antivirus permettent de détecter le code malveillant dans les objets. Les bases antivirus sont créées par des experts de Kaspersky et mises à jour toutes les heures.

Catégories Kaspersky

Catégories prédéfinies de données développées par les collaborateurs de Kaspersky. Il arrive que les catégories soient actualisées lors de la mise à jour des bases de données de l'application. Le spécialiste en sécurité de l'information ne peut pas modifier ou supprimer les catégories prédéfinies.

Certificat Apple Push Notification service (APNs)

Certificat signé par Apple, qui vous permet d'utiliser Apple Push Notification. Via Apple Push Notification, un serveur MDM iOS peut gérer des appareils iOS.

Code d'activation

Un code d'activation est une séquence unique de 20 caractères alphanumériques au format xxxxx-xxxxx-xxxxx-xxxxx. Vous pouvez utiliser le code d'activation pour activer la version premium de Kaspersky Endpoint Security.

La période d'abonnement commence à la date à laquelle le code d'activation est utilisé pour la première fois sur un appareil.

Si vous perdez ou supprimez accidentellement votre code d'activation après avoir activé l'application, contactez le Support Technique de Kaspersky.

Code de déverrouillage

Un code que vous pouvez obtenir dans Kaspersky Security Center. Il est nécessaire pour déverrouiller un appareil après l'exécution des commandes **Verrouiller et Géolocaliser**, **Alarme** ou **Photographier**, ainsi qu'au fonctionnement de l'autodéfense.

Contrat de licence utilisateur final

Accord juridique conclu entre vous et AO Kaspersky Lab qui prévoit les conditions selon lesquelles vous pouvez utiliser l'application que vous avez achetée.

Contrôle de conformité

Contrôle de la conformité des paramètres de l'appareil mobile et de Kaspersky Endpoint Security for Android aux exigences de sécurité de l'entreprise. Les exigences de sécurité de l'entreprise régulent l'utilisation des appareils. Par exemple, la protection en temps réel doit être activée sur l'appareil, les bases antivirus doivent être à jour et le mot de passe de l'appareil doit être suffisamment robuste. La vérification de la conformité s'opère sur la base d'une liste de règles. Une règle de conformité contient les éléments suivants :

- critères de vérification de l'appareil (par exemple, l'absence d'applications interdites sur l'appareil)
- délai octroyé à l'utilisateur de l'appareil pour résoudre le problème de non-conformité (par exemple, 24 heures)
- action qui sera exécutée sur l'appareil si l'utilisateur ne résout pas le problème de non-conformité à l'issue du délai octroyé (par exemple, verrouillage de l'appareil)

Durée de validité de la licence

Période au cours de laquelle vous pouvez utiliser les fonctions de l'application et les services complémentaires. Les services que vous pouvez utiliser dépendent du type de la licence.

Exchange Mobile Device Server

Composant de Kaspersky Endpoint Security qui vous permet de connecter des appareils mobiles Exchange ActiveSync au serveur d'administration.

Fichier clé

Fichier au format xxxxxxxx.key qui permet d'utiliser une application de Kaspersky selon les termes d'une licence d'évaluation ou commerciale. L'application génère le fichier clé sur la base du code d'activation. Vous pouvez utiliser l'application uniquement quand vous avez un fichier clé.

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.

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.

IMAP

Protocole d'accès à l'email. A la différence du protocole POP3, IMAP offre de larges possibilités d'utilisation des boîtes aux lettres comme l'administration des dossiers, la manipulation des messages sans copie du contenu depuis le serveur de messagerie. Le protocole IMAP utilise le port 134.

Kaspersky Private Security Network (KSN privé)

Kaspersky Private Security Network est une solution qui permet aux utilisateurs d'appareils dotés d'applications de Kaspersky d'accéder aux bases de données de réputation de Kaspersky Security Network et à d'autres données statistiques, sans envoyer les données de leurs appareils à Kaspersky Security Network. Kaspersky Private Security Network est conçu pour les entreprises clientes qui ne peuvent pas participer au Kaspersky Security Network pour l'une des raisons suivantes :

- Les appareils des utilisateurs ne sont pas connectés à Internet.
- La transmission de toute donnée en dehors du pays ou du LAN de l'entreprise est interdite par la loi ou les politiques de sécurité de l'entreprise.

Kaspersky Security Network (KSN)

Infrastructure de services cloud offrant un accès à la base de données de Kaspersky avec des informations constamment mises à jour sur la réputation des fichiers, des ressources Internet et des logiciels. Kaspersky Security Network permet aux applications de Kaspersky de réagir plus rapidement aux menaces, augmente l'efficacité de fonctionnement de certains composants de la protection et réduit la possibilité de faux positifs.

Licence

Droit d'utilisation de l'application, limité dans le temps, et octroyé dans le cadre du Contrat de licence utilisateur final.

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'installation

Ensemble de fichiers qui assure l'installation à distance de l'application de Kaspersky à l'aide du système d'administration à distance. Un paquet d'installation est créé sur la base de fichiers dédiés inclus dans le paquet de distribution des applications. 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.

Phishing

Type de fraude sur Internet visant à obtenir un accès non autorisé aux données confidentielles des utilisateurs.

Plug-in d'administration de l'application

Un composant spécialisé qui fournit une interface pour administrer l'application de Kaspersky via la Console d'administration. Chaque application peut être administrée via Kaspersky Security Center SPE a son propre plug-in d'administration. Le plug-in d'administration est inclus dans toutes les applications Kaspersky qui peuvent être administrées via Kaspersky Security Center.

POP3

Protocole de réseau de réception des messages depuis le serveur de messagerie sur le client de messagerie.

Poste de travail de l'administrateur

Ordinateur sur lequel la Console d'administration de Kaspersky Security Center a été 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

Environnement sécurisé sur l'appareil de l'utilisateur et dans lequel l'administrateur peut gérer des applications et des comptes utilisateur 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 appareils mobiles iOS au Serveur d'administration. Ce profil permet de diffuser les profils de configuration iOS en arrière-plan à l'aide du Serveur des appareils mobiles iOS MDM et d'obtenir un diagnostic étendu sur les appareils mobiles. Vous devez envoyer le lien vers le profil iOS MDM à l'utilisateur pour permettre au serveur des appareils mobiles iOS MDM de détecter et de connecter son appareil mobile fonctionnant sous iOS.

Profil provisioning

Collecte de paramètres pour le fonctionnement des applications sur les appareils mobiles iOS. Un profil de provisionnement contient des informations sur la licence ; il est lié à une application spécifique.

Quarantaine

Dossier dans lequel l'application de Kaspersky place les fichiers probablement infectés détectés. Les objets sont stockés dans la Quarantaine sous forme chiffrée afin d'éviter tout impact sur l'ordinateur.

Requête Certificate Signing Request

Fichier avec les paramètres d'un Serveur d'administration, approuvé par Kaspersky, puis envoyé à Apple pour obtenir un certificat APNs.

Serveur d'administration

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

Serveur des appareils mobiles iOS MDM

Composant de Kaspersky Endpoint Security installé sur un appareil client et qui permet la connexion d'appareils mobiles au Serveur d'administration et la gestion d'appareils mobiles iOS à l'aide du service Apple Push Notifications (APNs).

Serveur proxy

Service dans les réseaux informatiques qui permet aux utilisateurs de réaliser des requêtes indirectes vers d'autres services du réseau. Un utilisateur se connecte d'abord au serveur proxy et demande une ressource (par exemple, un fichier) situé sur un autre serveur. Ensuite, le serveur proxy se connecte au serveur indiqué et obtient la ressource demandée ou récupère la ressource dans son cache (si le serveur proxy possède son propre cache). Dans certains cas, la requête du client ou la réponse du serveur peuvent être modifiées par le serveur proxy à des fins déterminées.

Serveur Web de Kaspersky Security Center

Composant de Kaspersky Security Center installé avec le Serveur d'administration. Le serveur Web est conçu pour la transmission, via un réseau, de paquets d'installation autonomes, de profils MDM iOS et de fichiers à partir d'un dossier partagé.

Serveurs de mise à jour de Kaspersky

Serveurs HTTP(S) de Kaspersky à partir desquels les applications de Kaspersky récupèrent les mises à jour des bases de données et des modules de l'application.

SSL

Protocole de chiffrement des données utilisé sur Internet et sur les réseaux locaux. Le protocole Secure Sockets Layer (SSL) est utilisé dans les applications Web afin d'établir des connexions sécurisées entre un client et un serveur.

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 prédéfinis pour toutes les fonctions des applications mobiles Kaspersky Endpoint Security.

Tâche de groupe

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

Virus

Programme qui en infecte d'autres en y ajoutant son propre code afin de pouvoir prendre les commandes lors du lancement des fichiers infectés. Cette définition simple permet d'identifier l'action principale effectuée par tout virus : infection.

Information sur le code tiers

Vous pouvez télécharger et lire l'information sur le code tiers dans le fichier legal_notices.txt .

Sur les appareils Android, les informations sur le code tiers sont accessibles dans l'application Kaspersky Endpoint Security for Android, via le bouton → **Infos sur l'application**.

Avis de marque

Les autres noms et marques déposés appartiennent à leurs propriétaires respectifs.

PostScript est une marque déposée ou une marque d'Adobe aux États-Unis et/ou dans d'autres pays.

AirDrop et AirPrint sont des marques d'Apple Inc.

Apple, Apple Configurator, AirPlay, AirPort Express, App Store, Apple TV, Bonjour, Face ID, FaceTime, FileVault, iBooks, iCal, iCloud, iPadOS, iPhone, iTunes, OS X, Safari, Spotlight et Touch ID sont des marques d'Apple Inc., déposées aux États-Unis et/ou dans d'autres pays.

Aruba Networks est une marque d'Aruba Networks, Inc. aux États-Unis et dans certains autres pays.

Le mot, la marque et les logos Bluetooth appartiennent à Bluetooth SIG, Inc.

Cisco, Cisco AnyConnect et IOS sont des marques déposées et des marques de Cisco Systems, Inc. et/ou de ses compagnies affiliées aux États-Unis et dans certains autres pays.

SecurID est une marque déposée ou une marque d'EMC Corporation aux États-Unis et/ou dans d'autres pays.

Google, Android, Chrome, Chromebook, Chromium, Crashlytics, Firebase, Google Analytics, Google Chrome, Google Mail, Google Maps, Google Play, Nexus et SPDY sont des marques de Google, Inc.

HTC est une marque déposée de HTC Corporation.

Huawei et EMUI sont des marques de Huawei Technologies Co., Ltd déposées en Chine et dans d'autres pays.

IBM et Maas360 sont des marques d'International Business Machines Corporation déposées dans plusieurs juridictions à travers le monde.

Juniper Networks, Juniper et JUNOS sont des marques ou des marques déposées de Juniper Networks, Inc. aux États-Unis et/ou dans d'autres pays.

Microsoft, ActiveSync, Microsoft Intune, Tahoma, Windows, Windows Mobile et Windows Phone sont des marques de commerce du groupe d'entreprises Microsoft.

MOTOROLA et le logo M stylisé sont des marques de commerce ou des marques déposées de Motorola Trademark Holdings, LLC.

Oracle et JavaScript sont des marques déposées d'Oracle et/ou de ses compagnies affiliées.

La marque commerciale BlackBerry appartient à Research In Motion Limited, déposée aux États-Unis et peut être déposée dans d'autres pays.

Samsung est une marque de SAMSUNG aux États-Unis ou dans d'autres pays.

SonicWALL, Aventail et SonicWALL Mobile Connect sont des marques de SonicWall, Inc.

SOTI et MobiControl sont des marques déposées de SOTI Inc. aux États-Unis et dans d'autres juridictions.

TouchDown est une marque ou une marque déposée de Symantec Corporation ou de ses compagnies affiliées aux États-Unis et dans d'autres pays.

La marque Symbian appartient à Symbian Foundation Ltd.