kaspersky

MDM básico en Kaspersky Next Expert View (on-premise)

© 2026 AO Kaspersky Lab

Contenido

Basic MDM in Kaspersky Next Expert View (on-premise) help

What's new

Comparison of solution features by management tool

Working in Kaspersky Next Expert View (on-premise)

- About Basic MDM in Kaspersky Next Expert View (on-premise)
  - Distribution kit
  - About the Kaspersky Endpoint Security for Android app
  - About the Kaspersky Protection for iOS app
  - About Kaspersky Mobile Devices Protection and Management plug-in
  - Hardware and software requirements
    - Compatibility with other operating systems
  - Known issues and considerations
- Getting started
  - Solution architecture
  - Deployment scenarios
  - Deploying a mobile device management solution
    - Deploying Kaspersky Security Center Linux and Kaspersky Next Expert View (on-premise)
    - Deploying mobile management plug-ins
    - Configuring Administration Server settings for connecting mobile devices
      - Scenario: Configuring a connection gateway to connect mobile devices to Kaspersky Next Expert View (on-premise)
      - Adding installation packages to Administration Server repository
      - Adding a license key to the Administration Server repository
      - Installing Network Agent Linux
      - Configuring Kaspersky Security Center Linux Web Server settings
        - Configuring Web Server settings on a connection gateway (Network Agent for Linux)
        - Transferring the Web Server certificate to devices on the connection gateway
    - Migrating from Kaspersky Security Center Windows to Kaspersky Security Center Linux
      - Backing up and restoring Administration Server data using the klbackup utility
        - Backing up Administration Server data on a Windows device
        - Restoring Administration Server data on a Linux device
      - Backing up and restoring the iOS MDM Server data using the kliosbackup utility
  - Deploying an iOS device management system
    - About iOS device operating modes
    - About management profiles
    - Deploying Kaspersky Protection for iOS
      - About Kaspersky Protection for iOS
      - Installing Kaspersky Protection for iOS
      - Activating Kaspersky Protection for iOS
      - Updating Kaspersky Protection for iOS
      - Removing Kaspersky Protection for iOS

- Deploying a management system using the iOS MDM protocol
  - Deploying iOS MDM Server
    - Comparison of iOS MDM Server features depending on the management tools
    - Configuring an iOS MDM Server installation package
    - Installing iOS MDM Server using a remote installation task
    - Local installation of iOS MDM Server on a device via an installation package
    - Updating iOS MDM Server using a remote installation task or locally
    - Deleting iOS MDM Server using a remote uninstallation task
  - Viewing the list of installed iOS MDM Servers and configuring their settings
  - Configuring an iOS MDM Server certificate
  - Configuring a reserve iOS MDM Server certificate
  - Receiving or renewing an APNs certificate
  - Installing an APNs certificate on iOS MDM Server
  - Configuring access to Apple Push Notification service
  - iOS MDM Server events
  - Obtaining iOS MDM Server diagnostic data
- Deploying an Android device management system
  - About Android device operating modes
  - Using Firebase Cloud Messaging
  - Deploying Kaspersky Endpoint Security for Android
    - About the Kaspersky Endpoint Security for Android app
    - Installing Kaspersky Endpoint Security for Android
      - Creating the Kaspersky Endpoint Security for Android installation package
      - Manual installation of Kaspersky Endpoint Security for Android
  - Permissions for Kaspersky Endpoint Security for Android
  - Starting and stopping Kaspersky Endpoint Security for Android
  - Activating Kaspersky Endpoint Security for Android
  - Updating Kaspersky Endpoint Security for Android
  - Removing Kaspersky Endpoint Security for Android
    - Permitting users to remove Kaspersky Endpoint Security for Android
    - Removal of Kaspersky Endpoint Security for Android by the user
    - Remote removal of Kaspersky Endpoint Security for Android on corporate devices
- Managing mobile devices in Kaspersky Next Expert View (on-premise)
  - Creating administration groups
  - Configuring policies
    - Creating a policy
    - Modifying a policy
    - Copying a policy
    - Moving a policy to another administration group
    - Viewing the list of policies
    - Viewing the policy distribution results
    - Managing revisions to policies
    - Restricting permissions to configure policies
    - Configuring role-based access control
    - Configuring policy profiles
    - Deleting a policy

Connecting mobile devices to Kaspersky Next Expert View (on-premise)
Direct connection of Android devices to Kaspersky Security Center
Moving unassigned mobile devices to administration groups
Actions on mobile devices to connect to Administration Server
Configuring synchronization settings
Managing certificates of mobile devices
Reissuing the mobile Administration Server certificate
Configuring certificate issuance rules
Issuing mobile device certificates
Renewing mobile device certificates
Deleting mobile device certificates
Integration with Public Key Infrastructure
Viewing the list of mobile device certificates
Configuration and management
Control
Configuring restrictions
Configuring restrictions for personal Android devices
Configuring iOS MDM device restrictions
Configuring user access to websites
Configuring access to websites on Android devices
Configuring access to websites on iOS MDM devices
Compliance Control
Compliance Control of Android devices
App Control
App Control on Android devices
Mobile device protection levels
Software inventory on Android devices
Protection
Configuring anti-malware protection on Android devices
Protecting Android devices on the internet
Protection of data on a stolen or lost device
Sending commands to a lost or stolen mobile device
Unlocking a mobile device
Configuring the device unlock password strength
Configuring a strong unlock password for an Android device
Configuring a strong unlock password for an iOS MDM device
Configuring a virtual private network (VPN)
Configuring VPN on Android devices (only Samsung)
Configuring VPN on iOS MDM devices
Configuring Firewall on Android devices (only Samsung)
Protecting Kaspersky Endpoint Security for Android against removal
Detecting hacked devices
Configuring a global HTTP proxy on iOS MDM devices
Adding security certificates to iOS MDM devices
Adding a SCEP profile to iOS MDM devices

- Management of mobile devices
  - Managing Android devices
    - Enabling certificate-based authentication of devices
    - Creating a mobile application package for Android devices
    - Viewing information about an Android device
    - Disconnecting an Android device from management
  - Managing iOS MDM devices
    - Signing management profiles with a certificate
    - Adding a configuration profile
    - Installing a configuration profile on a device
    - Removing a configuration profile from a device
    - Configuring managed apps
    - Installing an app on a mobile device
    - Updating an app installed on a device
    - Removing an app from a device
    - Configuring roaming on an iOS MDM mobile device
    - Viewing information about an iOS MDM device
    - Disconnecting an iOS MDM device from management
- Management of mobile device settings
  - Configuring connection to a Wi-Fi network
    - Connecting Android devices to a Wi-Fi network
    - Connecting iOS MDM devices to a Wi-Fi network
  - Configuring email
    - Configuring a mailbox on iOS MDM devices
    - Configuring an Exchange mailbox on iOS MDM devices
    - Configuring an Exchange mailbox on Android devices
  - Configuring protection levels in Kaspersky Security Center
  - Creating a report on installed mobile apps
  - Configuring notifications for Kaspersky Endpoint Security for Android
  - Selecting the download manager for Android devices
  - Connecting iOS MDM devices to AirPlay
  - Connecting iOS MDM devices to AirPrint
  - Configuring the Access Point Name (APN)
    - Configuring APN on Android devices (only Samsung)
    - Configuring APN on iOS MDM devices
  - Corporate container
    - About corporate containers
    - Configuring a corporate container
    - Unlocking the corporate container
  - Adding an LDAP account
  - Adding a contacts account
  - Adding a calendar account
  - Configuring a calendar subscription
  - Configuring SSO
  - Managing Web Clips
  - Adding fonts

- Working with commands for mobile devices
  - Commands for mobile devices
  - Sending commands
  - Viewing the statuses of commands in the command history
- Managing the app by using third-party EMM solutions (Android only)
  - Getting started
  - How to install the app
  - Protecting devices on the internet
  - How to activate the app
  - How to connect a device to Kaspersky Security Center
  - Silent mode
  - AppConfig file
- Participating in Kaspersky Security Network
  - Information exchange with Kaspersky Security Network
  - Enabling and disabling the use of Kaspersky Security Network
  - Using Kaspersky Private Security Network
- Samsung Knox
  - Installation of Kaspersky Endpoint Security for Android via Knox Mobile Enrollment
    - Creating a Knox profile
    - Adding devices in Knox Mobile Enrollment
    - Installing the app
  - Configuring Knox
    - Configuring VPN in Knox
    - Configuring an Exchange mailbox in Knox
    - Configuring APN in Knox
    - Configuring Firewall in Knox

Using the Kaspersky Endpoint Security for Android app

- App features
- Main window at a glance
- Status bar icon
- Device scan
- Running a scheduled scan
- Changing the Protection mode
- Anti-malware database updates
- Scheduled database update
- Things to do if your device gets lost or stolen
- Web Protection
- Get Certificate
- Synchronizing with Kaspersky Security Center
- Activating the Kaspersky Endpoint Security for Android app without Kaspersky Security Center
- Installing and using mail and VPN certificates on the device
- Enabling accessibility on Android 13 or later
- Updating the app
- Removing the app
- Applications with a briefcase icon
- Knox app

Using the Kaspersky Protection for iOS app
App features
Installing the app
Activating the app
Activating the app with an activation code
Main window at a glance
Updating the app
Using diagnostics to troubleshoot issues
Removing the app
Application licensing
About the End User License Agreement
About the license
Viewing license information
About the subscription
About the license key
About the activation code
About the key file
Data provision in Kaspersky Endpoint Security for Android
Data provision in Kaspersky Protection for iOS
Contact Technical Support
How to get technical support
Technical support via Kaspersky CompanyAccount
Sources of information about the application
Glossary
Activating the application
Activation code
Administration group
Administration Server
Administrator's workstation
Android Work Profile
Anti-malware databases
Apple Push Notification service (APNs) certificate
Basic control
Basic protection
Certificate Signing Request
Compliance Control
Corporate container
Corporate device
Device administrator
End User License Agreement
Group task
IMAP
Installation package
iOS MDM device
iOS MDM Server
Kaspersky categories
Kaspersky Private Security Network (KPSN)

- Kaspersky Security Center Administrator
- Kaspersky Security Center Web Server
- Kaspersky Security Network (KSN)
- Kaspersky update servers
- Key file
- License
- License term
- Malware
- Management profile
- Manifest file
- Mobile management plug-in
- Network Agent
- Personal device
- Phishing
- Policy
- POP3
- Proxy server
- Quarantine
- SSL
- Standalone installation package
- Subscription
- Supervised device
- Unlock code
- Virtual Administration Server

Information about third-party code

Trademark notices

Ayuda para el MDM básico en Kaspersky Next Expert View (on-premise)

	**Novedades** Descubra las novedades de la última versión de la solución.		**Configurar la protección del dispositivo** Administre la protección de dispositivos móviles de forma remota. Las funciones incluyen Protección antimalware, Protección web, Antirrobo, y más.
	**Kit de distribución** Obtenga información acerca de varios componentes, según la versión de la solución elegida.		**Configurar los ajustes del dispositivo** Administre dispositivos móviles de forma remota: configure una conexión Wi-Fi, el correo electrónico, clips web y más.
	**Implementación** Aprenda a desplegar la solución en su organización y a configurar sistemas de administración para dispositivos Android y dispositivos iOS.		**Configurar el control de dispositivos** Supervise los dispositivos móviles de forma remota, incluida la configuración de restricciones, el acceso de los usuarios a los sitios web, el Control de cumplimiento, el Control de apps, y más.
	**Comandos** Administre los dispositivos móviles de forma remota con comandos móviles. Lock device, Wipe corporate data, Locate device, Take photos, Sound alarm, y más.		**Contenedor corporativo** Descubra los beneficios del contenedor corporativo y aprenda a configurarlo para su dispositivo.
	**Corporate App Catalog** Cree un Corporate App Catalog personalizado y use un navegador para descargar aplicaciones del catálogo a los dispositivos de los usuarios.		**Otro** Administre la seguridad de sus dispositivos Android con una solución de EMM de terceros o instale nuestra solución a través de Knox para mejorar la seguridad en los dispositivos Samsung.

Novedades

Versión 1.0

En esta versión, agregamos nuevas funciones al complemento Kaspersky Mobile Devices Protection and Management para Kaspersky Next Expert View (on-premise):

- Mejoras y correcciones de errores generales.

Comparación de las funciones de la solución por herramienta de administración

Disponibilidad de funciones por herramienta de administración

Características	MDM avanzado en Kaspersky Next Expert View (on-premise)	MDM básico en Kaspersky Next Expert View (on-premise)	MDM básico en Kaspersky Next Expert View (cloud)
	Kaspersky Next Expert View	Kaspersky Next Expert View	Kaspersky Next Expert View
Administración de dispositivos móviles			
Administración de dispositivos Android	✓	✓	✓
Administración de dispositivos iOS	✓	✓	✓
Protección de dispositivos Aurora	✓	—	—
Implementación			
Agregar dispositivos mediante un vínculo de App Store	✓	✓	✓
Agregar dispositivos mediante la creación de un paquete de instalación	✓	✓	—
Agregar dispositivos directamente al grupo de administración después de que los dispositivos se conectan	✓	✓	✓
Crear directivas divididas por modos de funcionamiento	✓	✓	✓
Enviar comandos a dispositivos móviles	✓	✓	✓ Conjunto limitado de comandos
Eliminar dispositivos móviles de Kaspersky Security Center	✓	✓	✓
Administración de certificados			
Emitir certificados de correo	✓	✓	✓ La configuración de los ajustes para la emisión no está disponible
Emitir certificados de VPN	✓	✓	✓ La configuración de los ajustes para la emisión no está disponible
Emitir certificados móviles	✓	✓	✓
Emitir certificados móviles mediante herramientas del Servidor de administración	✓	✓	✓
Especificar archivos de certificado	✓	✓	✓
Integrar con la infraestructura de clave pública (PKI)	✓	✓	—
Administración de directivas			
Acceso basado en roles para configurar las directivas de grupo	✓	✓	✓
Configurar la sincronización de dispositivos móviles con Kaspersky Security Center	✓	✓	✓
Configurar análisis de malware en dispositivos móviles	✓	✓	✓
Configurar actualizaciones de las bases de datos antimalware	✓	✓	✓

Configurar protección de dispositivos en Internet	✓	✓	✓
Configurar la protección de datos de dispositivos robados o perdidos	✓	✓	✓
Configurar seguridad de la contraseña de desbloqueo del dispositivo	✓	✓	✓ Conjunto limitado de configuraciones
Configurar el acceso de los usuarios a los sitios web	✓	✓	✓
Configurar Control de aplicaciones	✓	✓ Solo para Android	✓ Solo para Android
Configurar Control de cumplimiento	✓	✓ Solo para Android	✓ Solo para Android
Configurar Control de llamadas	✓ Solo para Android	—	—
Configurar reglas de concesión de permisos para aplicaciones instaladas	✓	—	—
Configurar contenedores corporativos	✓	✓ Conjunto limitado de configuraciones	✓ Conjunto limitado de configuraciones
Configurar restricciones de funciones del dispositivo	✓	✓ Conjunto limitado de configuraciones	✓
Configurar conexiones a redes Wi-Fi	✓	✓	✓
Configurar VPN	✓	✓ En iOS, Per App VPN y el protocolo IKEv2 no son compatibles. En Android, la VPN solo se puede configurar mediante Knox.	✓ En iOS, Per App VPN y el protocolo IKEv2 no son compatibles. En Android, la VPN solo se puede configurar mediante Knox.
Administrar configuraciones de aplicaciones	✓	—	—
Enviar archivos a dispositivos Android	✓	—	—
Samsung Knox	✓	✓ Conjunto limitado de configuraciones	✓
Control remoto para Android	✓	—	—
Características del Servidor de MDM para iOS			
Instalar y configurar el Servidor de MDM para iOS	✓	✓	✓ Solo la configuración aplicable
Actualizar y eliminar el Servidor de MDM para iOS	✓	✓	—
Emitir certificados de APNs	✓	✓	✓
Conectar dispositivos MDM con iOS	✓	✓	✓
Firmar un perfil de administración con un certificado	✓	✓	—
Eventos del Servidor de MDM para iOS	✓	✓	✓
Agregar un perfil de configuración	✓	✓	✓
Otras funciones			
Aceptación global del EULA en Kaspersky Security Center	✓	✓	✓
Configurar Kaspersky Private Security Network	✓	✓	—

Trabajar en Kaspersky Next Expert View (on-premise)

En esta sección de Ayuda, se describe la protección y administración de dispositivos móviles mediante el uso de Kaspersky Next Expert View (on-premise).

Acerca de MDM básico en Kaspersky Next Expert View (on-premise)

MDM básico en Kaspersky Next Expert View (on-premise) es una solución integrada para proteger y administrar dispositivos móviles corporativos, así como dispositivos móviles personales utilizados por los empleados de la empresa con fines corporativos.

Kit de distribución

El kit de distribución de MDM básico en Kaspersky Next Expert View (on-premise) puede incluir varios componentes, según la versión de la solución seleccionada. Para obtener información sobre la compatibilidad de la versión del complemento y las versiones de Kaspersky Security Center, consulte los requisitos de hardware y software.

Administración de dispositivos móviles en Kaspersky Next Expert View (on-premise)

> Este componente es compatible con Kaspersky Security Center Linux 15.1. Para obtener información acerca de la versión compatible con Kaspersky Security Center Windows, consulte la Ayuda de Kaspersky Secure Mobility Management 4.1.

- `on_prem_ksm_policies_<version>.zip`

  Archivo comprimido que contiene los archivos necesarios para la instalación del complemento Kaspersky Mobile Devices Protection and Management:

  - `plugin.zip`

    Archivo comprimido que contiene el complemento Kaspersky Mobile Devices Protection and Management.

  - `signature.txt`

    Archivo que contiene la firma del complemento Kaspersky Mobile Devices Protection and Management.

Complemento de configuración del Servidor de MDM para iOS

Este componente es compatible con Kaspersky Security Center Linux 15.1. Para obtener información acerca de la versión compatible con Kaspersky Security Center Windows, consulte la Ayuda de Kaspersky Secure Mobility Management 4.1.

- `on_prem_iosmdm_<version>.zip`

  Archivo comprimido que contiene los archivos necesarios para la instalación del complemento de configuración del Servidor de MDM para iOS:

  - `plugin.zip`

    Archivo comprimido que contiene el complemento de configuración del Servidor de MDM para iOS.

  - `signature.txt`

    Archivo que contiene la firma del complemento de configuración del Servidor de MDM para iOS.

Servidor de MDM para iOS

Este componente es compatible con Kaspersky Security Center Linux 15.1. Para obtener información acerca de la versión compatible con Kaspersky Security Center Windows, consulte la Ayuda de Kaspersky Secure Mobility Management 4.1.

- `kliosmdm-<architecture>-<version>-<package manager>_<language>.tar.gz`

  Archivo comprimido que contiene los archivos necesarios para la instalación del Servidor de MDM para iOS, según el administrador de paquetes y la arquitectura:

  - `kliosmdm.kpd`

    Archivo de descripción del Servidor de MDM para iOS.

  - `akinstall.sh`

    Script que le permite automatizar la instalación del Servidor de MDM para iOS.

  - `kliosmdm-<versión>.<arquitectura>.rpm` o `kliosmdm_<versión>_<arquitectura>.deb`

    Paquete de instalación del Servidor de MDM para iOS.

  - `kpd.loc/`

    Carpeta con archivos CFG que especifican las rutas a los Contratos de licencia de usuario final.

  - `license/`

    Carpeta con Contratos de licencia de usuario final y Política de privacidad en diferentes idiomas en formato TXT.

Aplicación Kaspersky Endpoint Security para Android

- `<version>_sc_package.zip`

  Archivo comprimido que contiene los archivos necesarios para instalar la aplicación de Kaspersky Endpoint Security para Android mediante la creación de paquetes de instalación:

  - `installer.ini`

    Archivo de configuración que contiene los ajustes de la conexión del Servidor de administración.

  - `kesandroid<version>_<languages>_Prod_Release.apk`

    Archivo de paquete de Android de la aplicación Kaspersky Endpoint Security para Android.

  - `eula/`

    Carpeta con Contratos de licencia de usuario final en diferentes idiomas en formato TXT.

  - `kpd.loc/`

    Archivos INI que especifican las rutas a los Contratos de licencia de usuario final.

  - `ksm.kpd`

    Archivo de descripción de la aplicación.

Archivo con Corporate App Catalog

`Install_<versión>.exe`: paquete de distribución de Corporate App Catalog. El paquete incluye los siguientes componentes:

- Corporate App Catalog
- Consola de administración de Corporate App Catalog
- Servidor Apache

Para obtener más información acerca de la instalación de Corporate App Catalog, consulte la *Ayuda de Corporate App Catalog*.

Documentación

- Ayuda para MDM básico en Kaspersky Next Expert View (on-premise).

Acerca de la aplicación Kaspersky Endpoint Security para Android

La aplicación Kaspersky Endpoint Security para Android garantiza la protección de dispositivos móviles contra amenazas web, virus y otros programas que suponen amenazas.

La aplicación Kaspersky Endpoint Security para Android incluye las siguientes características:

- **Antimalware**. Este componente detecta y neutraliza amenazas en el dispositivo mediante las bases de datos antimalware y el servicio en la nube de Kaspersky Security Network. Antimalware incluye los siguientes componentes:
  - **Protección**. Detecta amenazas en archivos abiertos, analiza aplicaciones nuevas y evita la infección del dispositivo en tiempo real.
  - **Análisis**. Se inicia a petición para el sistema de archivos completo, solo para aplicaciones instaladas o solo para un archivo o una carpeta seleccionados.
  - **Actualizar**. Le permite descargar nuevas bases de datos antimalware para la aplicación.
- **Antirrobo**. Este componente protege la información del dispositivo para impedir el acceso no autorizado en caso de pérdida o robo del dispositivo. Este componente le permite enviar los siguientes comandos al dispositivo:
  - **Locate device**. Le permite obtener las coordenadas de la ubicación del dispositivo.
  - **Sound alarm**. Provoca que el dispositivo emita un sonido de alarma fuerte.
  - **Wipe corporate data**. Borre los datos corporativos para proteger la información confidencial de la empresa.
- **Protección web** y **Control web**. Protección web bloquea los sitios web maliciosos diseñados para propagar código malicioso. Protección web también bloquea sitios web falsos (phishing) diseñados para robar datos confidenciales del usuario (por ejemplo, contraseñas de servicios bancarios en línea o sistemas de dinero electrónico) y acceder a la información financiera del usuario. Protección web usa el servicio en la nube de Kaspersky Security Network para analizar sitios web antes de que el usuario los abra. Tras el análisis, Protección Web permite que se carguen los sitios web de confianza y bloquea los que son maliciosos. Control web también admite la filtración de los sitios web según las categorías definidas en el servicio en la nube de Kaspersky Security Network. Esto permite que el administrador restrinja el acceso de usuarios a determinadas categorías de páginas web (por ejemplo, juegos de azar, loterías, sorteos o comunicación por Internet).
- **Control de apps**. Este componente le permite instalar aplicaciones recomendadas y requeridas en un dispositivo Android, así como eliminar aplicaciones bloqueadas que infringen los requisitos de seguridad corporativa.
- **Control de cumplimiento**. Este componente le permite comprobar si los dispositivos administrados cumplen con los requisitos de seguridad corporativa e imponer restricciones a ciertas funciones en los dispositivos que no los cumplan.

Puede configurar los componentes de la aplicación Kaspersky Endpoint Security para Android en Kaspersky Next Expert View (on-premise) al definir la configuración de la directiva correspondiente.

Acerca de la aplicación Kaspersky Protection para iOS

La aplicación Kaspersky Protection para iOS garantiza la protección de los dispositivos móviles contra el phishing y las amenazas web.

La aplicación Kaspersky Protection para iOS ofrece las siguientes funciones clave:

- **Protección web**. Este componente bloquea los sitios web maliciosos diseñados para propagar código malicioso. Protección web también bloquea sitios web falsos (phishing) diseñados para robar datos confidenciales del usuario (por ejemplo, contraseñas de servicios bancarios en línea o sistemas de dinero electrónico) y acceder a la información financiera del usuario. Protección web utiliza el servicio en la nube de Kaspersky Security Network para analizar sitios web antes de abrirlos. Tras el análisis, Protección Web permite que se carguen los sitios web de confianza y bloquea los que son maliciosos. Puede configurar este componente en Kaspersky Next Expert View (on-premise) al definir la configuración de las directivas de grupo.

- **Detección de jailbreak**. Cuando Kaspersky Protection para iOS detecta un jailbreak, muestra un mensaje crítico y le informa sobre el problema.

Acerca del complemento Kaspersky Mobile Devices Protection and Management

El complemento Kaspersky Mobile Devices Protection and Management le permite administrar los dispositivos móviles y las aplicaciones móviles instaladas en ellos en Kaspersky Next Expert View (on-premise). El complemento Kaspersky Mobile Devices Protection and Management se puede usar para lo siguiente:

- Crear directivas de seguridad de grupo para los dispositivos móviles.

- Definir de forma remota la configuración de la aplicación Kaspersky Endpoint Security para Android en dispositivos móviles de los usuarios.

- Recibir informes y estadísticas de funcionamiento de la aplicación móvil Kaspersky Endpoint Security para Android en los dispositivos de los usuarios.

- Configurar de forma remota dispositivos iOS conectados mediante el protocolo MDM para iOS (en adelante, "dispositivos MDM con iOS") y dispositivos iOS con la aplicación Kaspersky Protection para iOS.

- Configurar dispositivos Aurora de forma remota con la aplicación Kaspersky Endpoint Security for Aurora.

El complemento Kaspersky Mobile Devices Protection and Management se puede instalar al configurar Kaspersky Next Expert View (on-premise). Para obtener más información acerca de los escenarios de implementación, consulte Implementar complementos de administración móvil.

Requisitos de hardware y software

En esta sección se enumeran los requisitos de hardware y software que debe reunir el equipo del administrador que se utiliza para implementar las aplicaciones en dispositivos móviles, así como los sistemas operativos de dispositivos móviles que admite MDM básico en Kaspersky Next Expert View (on-premise).

Este artículo enumera las versiones de software en las que se probó la aplicación y para las que se garantiza que funciona correctamente. La aplicación también puede funcionar con otras versiones de software, pero esas configuraciones no se sometieron a un ciclo de prueba completo y no se incluyen en la lista de versiones compatibles garantizadas.

Requisitos de hardware y software para el equipo del administrador

El servidor de Kaspersky Security Center Linux debe cumplir los siguientes requisitos:

- Requisitos de software:
  - Servidor de administración de Kaspersky Security Center Linux 15.2 o versiones posteriores
  - Web Console de Kaspersky Security Center Linux 15.2 o posterior
  - Complemento de Kaspersky Mobile Devices Protection and Management 10.53 o posterior
  - Servidor de MDM para iOS para Linux 15.2 o posterior
  - Complemento de configuración del Servidor de MDM para iOS 15.2 o posterior
- Requisitos de hardware:
  - Para implementar MDM básico en Kaspersky Next Expert View (on-premise), se deben cumplir los requisitos de hardware de Kaspersky Security Center.
  - Para el Servidor de MDM para iOS:
    - CPU con una frecuencia de funcionamiento de 1 GHz o superior. Para un sistema operativo de 64 bits, la frecuencia mínima de la CPU debe ser de 1.4 GHz
    - RAM: 4 GB
    - Espacio disponible en disco: 4 GB

Compatibilidad de versiones

Se admiten las siguientes combinaciones de versiones:

- La versión 10.53 del complemento Kaspersky Mobile Devices Protection and Management solo es compatible con Kaspersky Security Center Linux 15.1 o posteriores.
- Las versiones 10.54 o posteriores del complemento Kaspersky Mobile Devices Protection and Management solo son compatibles con Kaspersky Security Center Linux 15.2 o posteriores.

Las siguientes versiones son totalmente compatibles:

- Complemento Kaspersky Mobile Devices Protection and Management versión 10.53 y Kaspersky Security Center Linux versión 15.1 o posteriores.
- Complemento Kaspersky Mobile Devices Protection and Management versión 10.54 y Kaspersky Security Center Linux versión 15.2 o posteriores.
- Complemento Kaspersky Mobile Devices Protection and Management versión 10.55 y Kaspersky Security Center Linux versión 15.3 o posteriores.
- Complemento Kaspersky Mobile Devices Protection and Management versión 10.56 y Kaspersky Security Center Linux versión 16.1 o posteriores.
- Complemento Kaspersky Mobile Devices Protection and Management versión 10.57 y Kaspersky Security Center Linux versión 16.2 o posteriores.
- Complemento Kaspersky Mobile Devices Protection and Management versión 10.58 y Kaspersky Security Center Linux versión 16.3 o posteriores.

Requisitos de hardware y software para Kaspersky Endpoint Security para Android

Para Kaspersky Endpoint Security para Android, el dispositivo móvil debe cumplir los siguientes requisitos:

- Teléfono inteligente o tableta con una resolución de pantalla de 320x480 píxeles o más
- 65 MB de espacio libre en la memoria principal del dispositivo
- Sistema operativo (excepto edición Go):
  - Android 5.x (Lollipop)
  - Android 6.x (Marshmallow)
  - Android 7.x (Nougat)
  - Android 8.x (Oreo)
  - Android 9
  - Android 10

    - Android 11
    - Android 12, 12L
    - Android 13
    - Android 14
    - Android 15
    - Android 16
    - Android 17
- Arquitectura de procesador x86, x86-64, ARM5, ARM6, ARM7 o ARM8
- La aplicación se puede instalar únicamente en la memoria principal del dispositivo

Requisitos de hardware y software para Kaspersky Protection para iOS

Para Kaspersky Protection para iOS, el dispositivo móvil debe cumplir los siguientes requisitos:

- Sistema operativo:
    - iOS:
        - iOS 15.x
        - iOS 16.x
        - iOS 17.x
        - iOS 18.x
        - iOS 26.2, 26.3, 26.5
    - iPadOS:
        - iPadOS 15.x
        - iPadOS 16.x
        - iPadOS 17.x
        - iPadOS 26.2, 26.5
- Conexión a Internet

Requisitos de hardware y software para un perfil de administración

Para un perfil de administración, el dispositivo móvil debe cumplir con los siguientes requisitos:

- Sistema operativo:
  - iOS:
    - iOS 10.x
    - iOS 11.x
    - iOS 12.x
    - iOS 13.x
    - iOS 14.x
    - iOS 15.x
    - iOS 16.x
    - iOS 17.x
    - iOS 18.x
    - iOS 26, 26.1, 26.2, 26.3, 26.4, 26.5
  - iPadOS:
    - iPadOS 13.x
    - iPadOS 14.x
    - iPadOS 15.x
    - iPadOS 16.x
    - iPadOS 17.x
    - iPadOS 26.2, 26.4, 26.5
- Conexión a Internet

Compatibilidad con otros sistemas operativos

El MDM básico en Kaspersky Next Expert View (on-premise) es compatible con la protección y administración de dispositivos móviles que ejecutan otros sistemas operativos mediante la aplicación Kaspersky Endpoint Security para Android.

La tabla describe la compatibilidad de las versiones de la aplicación Kaspersky Endpoint Security para Android con otras versiones del sistema operativo.

Compatibilidad de Kaspersky Endpoint Security para Android con otros sistemas operativos

Versión de Kaspersky Endpoint Security para Android	Versión del sistema operativo	Limitaciones
10.57.1.37	kvadraOS 1.26 (Enterprise)	Problemas conocidos y consideraciones

Problemas conocidos y consideraciones

Los siguientes problemas conocidos no son críticos para el funcionamiento de la solución.

Problemas conocidos durante la conexión de dispositivos móviles a Kaspersky Security Center

- Es posible que el vínculo para conectar dispositivos móviles o el vínculo para descargar el paquete de instalación en el puerto HTTPS 8061 del Servidor web no se abra en el mismo navegador que Kaspersky Next Expert View (on-premise) debido al error `NET::ERR_CERT_AUTHORITY_INVALID`. Esto puede suceder si el Servidor web utiliza un certificado autofirmado. Para abrir el vínculo, cópielo y péguelo en un navegador diferente o reemplace el certificado autofirmado con un certificado personalizado emitido por la autoridad de certificación de confianza en las propiedades del Servidor de administración, en la pestaña **General** de la sección **Web Server**.

Problemas conocidos durante la administración de dispositivos móviles

- Si edita los campos **Nombre** y **Descripción** en la pestaña **General** de las propiedades del dispositivo, los cambios no se mostrarán en la lista de dispositivos móviles conectados a Kaspersky Security Center debido a limitaciones técnicas.
- El botón **Force synchronization** y la casilla **Do not disconnect from the Administration Server** en la ventana de propiedades del dispositivo no son compatibles con dispositivos móviles. Utilice el comando **Synchronize device** para forzar la sincronización de un dispositivo Android o un dispositivo MDM con iOS.
- En la lista de dispositivos móviles administrados, la capacidad de almacenamiento total que se muestra de los dispositivos iOS personales que operan en el modo de protección básica se redondea hacia arriba.

Problemas conocidos de Kaspersky Protection para iOS

- La aplicación Kaspersky Protection para iOS no puede funcionar debidamente cuando un cliente VPN con una conexión VPN activa se está ejecutando en el mismo dispositivo móvil.
- Para una operación estable de la aplicación Kaspersky Protection para iOS, la versión desactualizada se debe desinstalar del dispositivo.
- En algunos dispositivos iOS, las tareas en segundo plano (por ejemplo, la sincronización con Kaspersky Security Center o el reemplazo de la clave de activación) pueden ejecutarse más tarde de lo esperado si el usuario sale de Kaspersky Protection para iOS deslizando el dedo hacia arriba en el Selector de aplicaciones. Esto se debe a los límites de ejecución en segundo plano de iOS. Para forzar la ejecución, vuelva a abrir la aplicación.

Para aumentar las posibilidades de que se ejecuten tareas en segundo plano, asegúrese de lo siguiente:

- La aplicación Kaspersky Protection para iOS está abierta en el Selector de aplicaciones.
- El modo de datos bajos está desactivado y el dispositivo está conectado a una red Wi-Fi o un punto de acceso.
- El dispositivo está conectado a una red de alta calidad.
- El dispositivo se está cargando.
- El punto de acceso personal está apagado.

Problemas conocidos durante la instalación de Kaspersky Endpoint Security para Android

- Kaspersky Endpoint Security para Android solo se instala en la memoria principal del dispositivo.
- En dispositivos con Android 7, puede ocurrir un error al intentar deshabilitar derechos del administrador para Kaspersky Endpoint Security para Android en la configuración del dispositivo si Kaspersky Endpoint Security para Android tiene prohibido superponerse en otras ventanas. La causa de este problema es un defecto conocido de Android 7.
- Kaspersky Endpoint Security para Android no es compatible con el modo multiventana en dispositivos con Android 7.0 y versiones posteriores.
- Kaspersky Endpoint Security para Android no funciona en dispositivos de Chromebook que ejecutan el sistema operativo de Chrome.
- Kaspersky Endpoint Security para Android no funciona en dispositivos con sistemas operativos Android (edición Go).
- Al usar la aplicación Kaspersky Endpoint Security para Android con sistemas de EMM de terceros sin conectarse a Kaspersky Security Center, solo los componentes Antimalware y Protección web están disponibles. El administrador puede ajustar la configuración de Antimalware y Protección web en la consola del sistema EMM. En este caso, las notificaciones sobre la operación de la aplicación solo están disponibles en la interfaz de la aplicación Kaspersky Endpoint Security para Android (Informes).
- En dispositivos personales y dispositivos con un contenedor corporativo que ejecuta Android 15, los usuarios pueden crear su propio espacio privado. Kaspersky Endpoint Security para Android no puede analizar aplicaciones, fotos y otros archivos almacenados en un espacio privado. Protección web, Control web y Control de apps no funcionan para las aplicaciones instaladas en un espacio privado. No se admite la instalación de Kaspersky Endpoint Security para Android en un espacio privado.

Problemas conocidos durante la actualización de Kaspersky Endpoint Security para Android

- Puede actualizar Kaspersky Endpoint Security para Android solo a una versión más reciente de la aplicación. No se puede actualizar a una versión anterior de Kaspersky Endpoint Security para Android.

Problemas conocidos durante la eliminación de Kaspersky Endpoint Security para Android

- Antes de eliminar Kaspersky Endpoint Security para Android del dispositivo, desmarque la casilla **Block system apps** en la configuración de **App Control** de la directiva o deshabilite el Control de aplicaciones.

Problemas conocidos que afectan la red Wi-Fi

- En dispositivos MDM con iOS, si deshabilita la conexión automática a una red Wi-Fi existente en la configuración de la directiva, no podrá volver a habilitar la conexión automática a esta red. Esto se debe a un problema reconocido por Apple.

- En los dispositivos MDM con iOS que ejecutan iOS 18 y iOS 26, si se selecciona el tipo de protección de red **Personal network (any)** en la configuración de la directiva Wi-Fi, es posible que el dispositivo no se conecte automáticamente a una red Wi-Fi protegida por el protocolo WEP, WPA o WPA3, incluso si la casilla **Connect automatically** está marcada. Para conectarse automáticamente a una red Wi-Fi protegida por un protocolo requerido, especifique ese protocolo como el tipo de seguridad de la red.

Problemas conocidos que afectan el componente Antimalware

- Debido a limitaciones técnicas, Kaspersky Endpoint Security para Android no puede analizar archivos con un tamaño de 2 GB o más. Durante un análisis, la app omite dichos archivos sin notificarle que se omitieron.

- Para el análisis adicional de un dispositivo en busca de amenazas nuevas cuya información todavía no se agregó a las bases de datos antimalware, debe habilitar el uso de Kaspersky Security Network. *Kaspersky Security Network (KSN)* es una infraestructura de servicios en la nube que brinda acceso a la base de conocimientos en línea de Kaspersky, que contiene información sobre la reputación de los archivos, recursos web y software. Para utilizar KSN, el dispositivo móvil debe estar conectado a Internet.

- En algunos casos, puede fallar la actualización de las bases de datos antimalware desde el Servidor de administración en un dispositivo móvil. Si eso sucede, ejecute la tarea de actualización de las bases de datos antimalware en el Servidor de administración.

- En ciertos dispositivos, Kaspersky Endpoint Security para Android no detecta dispositivos conectados por USB OTG. No es posible ejecutar un análisis de malware en tales dispositivos.

- En dispositivos con Android 11 o versiones posteriores, la aplicación Kaspersky Endpoint Security para Android no puede analizar las carpetas "Android/datos" ni "Android/obb" ni detectar malware en ellas debido a limitaciones técnicas.

- En dispositivos con Android 11 o versiones posteriores, el usuario debe otorgar el permiso "Permitir el acceso para administrar todos los archivos".

- En dispositivos que ejecuten Android 7 o versiones posteriores, puede que la ventana de configuración de la planificación de ejecución de análisis de malware se muestre incorrectamente (no se muestran los elementos de administración). La causa de este problema es un defecto conocido de Android 7.

- En dispositivos que ejecutan Android 7, la protección en tiempo real en el modo extendido no detecta amenazas en archivos almacenados en una tarjeta SD externa.

- En dispositivos con Android 6, Kaspersky Endpoint Security para Android no detecta la descarga de archivos maliciosos a la memoria del dispositivo. El Antimalware puede detectar un archivo malicioso cuando se ejecuta el archivo o durante un análisis de malware en el dispositivo. La causa de este problema es un defecto conocido de Android 6. Para garantizar la seguridad del dispositivo, se recomienda configurar análisis de malware programados.

Problemas conocidos que afectan los componentes Protección web y Control web

- Control web en dispositivos Android solo es compatible con Google Chrome, el navegador HUAWEI, Samsung Internet y Yandex Browser.

- La función Pestañas personalizadas es compatible con Google Chrome, el navegador HUAWEI y Samsung Internet.

- Control web para el navegador HUAWEI, el navegador de Internet de Samsung y Yandex Browser no bloquea los sitios en un dispositivo móvil si se usa un contenedor corporativo y la Protección web está habilitada solo para el contenedor corporativo.

- Para que Protección web y Control web funcionen, debe habilitar el uso de Kaspersky Security Network. Control web bloquea sitios web según los datos que tenga KSN sobre la reputación y categoría de los sitios web.

- Los sitios web prohibidos pueden permanecer desbloqueados por Control web en dispositivos Android 6 con la versión 51 (o cualquier versión anterior) de Google Chrome instalada si el sitio web se abre de los siguientes modos (este problema es causado por un defecto conocido de Google Chrome):

  - Desde resultados de búsqueda.

  - Desde la lista de marcas.

  - Desde el historial de búsqueda.

  - Uso de la función de autocompletado de direcciones web.

  - Abrir el sitio web en una nueva pestaña en Google Chrome.

- Los sitios web bloqueados pueden quedar desbloqueados en Google Chrome 50 (o versiones anteriores) si el sitio web se abrió desde la página de resultados de búsqueda de Google cuando las funciones **Combinar pestañas y aplicaciones** están activadas en la configuración del navegador. El problema se debe a un defecto conocido de Google Chrome.

- Los sitios web de categorías bloqueadas pueden permanecer desbloqueados en Google Chrome si el usuario los abre desde apps de terceros, por ejemplo, desde una app cliente de mensajería instantánea. Este problema se relaciona con cómo el servicio de Accesibilidad funciona con la función de Chrome Custom Tabs.

- Los sitios web prohibidos pueden permanecer desbloqueados en Samsung Internet si el usuario los abre en segundo plano desde el menú contextual o desde apps de terceros, por ejemplo, desde una app cliente de mensajería instantánea.

- Kaspersky Endpoint Security para Android debe estar configurado como una función de accesibilidad para asegurar el correcto funcionamiento de Protección web y Control web.

- En algunos dispositivos Xiaomi, se deben otorgar los permisos "Mostrar ventana emergente" y "Mostrar ventanas emergentes mientras se ejecuta en segundo plano" para que funcionen Protección web y Control web.

- Los sitios web permitidos pueden bloquearse en Samsung Internet en el modo de Control web **Allow only listed websites** cuando se actualiza la página. Los sitios web se bloquean si una expresión regular contiene ajustes avanzados (por ejemplo, `^https?://example.com/pictures/`). Se recomienda usar expresiones regulares sin ajustes adicionales (por ejemplo, `^https?://example.com`).

- Si Control web está configurado en **Prohibit all websites**, Kaspersky Endpoint Security para Android no bloquea las búsquedas en el widget de Búsqueda de Google. En cambio, bloquea el acceso de los usuarios a los resultados de las búsquedas.

- En un contenedor corporativo, si Control web está configurado en **Prohibit all websites**, Kaspersky Endpoint Security para Android recarga sin parar la página de inicio de Google Chrome, bloquea el navegador e interfiere con el dispositivo.

- En Yandex Browser y Samsung Internet, las URL maliciosas y de phishing pueden permanecer desbloqueadas. Esto se debe a que solo se realiza el análisis del dominio del sitio web. Si se trata de un dominio malicioso o de phishing, Protección web bloquea la amenaza. Si el dominio no está clasificado como malicioso o como phishing, la URL específica no se bloquea.

- La lista de sitios web permitidos creada en la tarjeta **Web Control** no se muestra en Safari en dispositivos MDM con iOS que ejecutan iOS 26 o versiones anteriores. Sin embargo, Control web sigue funcionando y los usuarios solo pueden acceder a los sitios web permitidos. Para mostrar los sitios web permitidos en Safari, seleccione la casilla **Add to bookmarks on device** en la tarjeta **Web Control** y especifique el nombre del marcador para cada sitio web de la lista.

- Si la opción **Check full URL when using Custom Tabs** está habilitada en la sección Control web de la configuración de la directiva, el cambio a la versión completa de los navegadores compatibles solo funciona para sitios web maliciosos y de phishing.

- En dispositivos iOS que funcionan en el modo de protección básica, si cambia el idioma o reinicia el dispositivo, el componente Protección web se deshabilita. Si desea habilitar el componente Protección web, después de cambiar el idioma o reiniciar el dispositivo, espere aproximadamente un minuto y, luego, abra Kaspersky Protection para iOS.

Problemas conocidos que afectan el componente Antirrobo

- Para la entrega oportuna de comandos a dispositivos Android, la aplicación usa el servicio de Firebase Cloud Messaging (FCM). Si FCM no se configura, los comandos se entregarán al dispositivo solo durante la sincronización con Kaspersky Security Center según la programación definida en la directiva, por ejemplo, cada 24 horas.

- Para bloquear un dispositivo, Kaspersky Endpoint Security para Android debe estar configurado como administrador del dispositivo.

- Para bloquear dispositivos con Android 7 o posteriores, Kaspersky Endpoint Security para Android debe estar configurado como función de accesibilidad.

- En algunos dispositivos, los comandos Antirrobo pueden producir un error durante la ejecución si el modo de Ahorro de Batería ha sido habilitado en el dispositivo. Este defecto se confirmó en Alcatel 5080X.

- Para localizar dispositivos con Android 10 o posterior, el usuario debe otorgar el permiso "Todo el tiempo" para la ubicación del dispositivo.

Problemas conocidos que afectan el Control de aplicaciones

- Kaspersky Endpoint Security para Android debe estar configurado como función de Accesibilidad para garantizar el correcto funcionamiento del Control de apps.

- Para que la aplicación Control de apps (categorías de aplicaciones) funcione, debe habilitar el uso de Kaspersky Security Network. Control de apps determina la categoría de una aplicación según datos que están disponibles en KSN. Para utilizar KSN, el dispositivo móvil debe estar conectado a Internet. Para Control de apps, puede Agregar aplicaciones particulares a las listas de aplicaciones bloqueadas y permitidas. En este caso, KSN no se requiere.

- Al configurar Control de aplicaciones, se recomienda desactivar la casilla **Block system apps**. El bloqueo de aplicaciones del sistema puede provocar problemas en el funcionamiento del dispositivo.

- En dispositivos MDM con iOS, si especifica las aplicaciones permitidas en la lista de aplicaciones permitidas a instalar, todas las aplicaciones permanecen ocultas en la pantalla del dispositivo, excepto aquellas agregadas a la lista de aplicaciones permitidas y del sistema.

- En algunos dispositivos personales HUAWEI y Honor, las aplicaciones de las categorías de aplicaciones permitidas pueden estar bloqueadas y las aplicaciones de las categorías de aplicaciones prohibidas pueden permanecer desbloqueadas. Esto se debe a que la categoría de algunas aplicaciones de la Galería de aplicaciones no se puede definir correctamente.

- En algunos dispositivos Samsung y Oppo, los íconos de las aplicaciones pueden permanecer ocultos en la pantalla de inicio después de desmarcar la casilla **Block system apps**. Esto se debe a las limitaciones del sistema operativo Android.

- Cuando se configura un contenedor corporativo en el dispositivo, recomendamos desmarcar la casilla **Block system apps**. El bloqueo de aplicaciones del sistema puede ocasionar problemas durante la creación del contenedor corporativo.

- Si la casilla **Block system apps** está marcada, entre las aplicaciones del sistema, es posible que el mecanismo del sistema para solicitar permisos de aplicaciones esté bloqueado. Si desea desbloquear este mecanismo, busque su nombre (por ejemplo, `com.google.android.permissioncontroller`) en el registro de eventos y agréguelo a las excepciones.

Problemas conocidos durante la administración de certificados

- Cuando la opción **Integrate issuance of certificates with Microsoft Certification Authority (CA) via PKI** está habilitada en las **Issuance rules**, la configuración de los certificados de correo y VPN puede permanecer inactiva durante un cierto tiempo mientras se espera la respuesta de PKI.

- No puede renovar automáticamente un certificado de correo o VPN cargado desde un archivo (con la opción **Integrate issuance of certificates with Microsoft Certification Authority (CA) via PKI** deshabilitada en la sección **PKI settings** de las **Issuance rules**), ya que no hay acceso a la entidad de certificación (CA) de dicho certificado. Para renovar el certificado, debe cargar un nuevo archivo de certificado manualmente.

- No se puede instalar un nuevo certificado móvil, VPN o de correo para otro usuario en un dispositivo móvil si el dispositivo ya tiene instalado el certificado móvil para un usuario actual. Sin embargo, se pueden emitir nuevos certificados para el usuario actual.

Problemas conocidos durante la configuración de la seguridad de la contraseña de desbloqueo del dispositivo

- En dispositivos con Android 10 o posterior, Kaspersky Endpoint Security establece los requerimientos de seguridad de la contraseña en uno de los sistemas de valores: media o alta.

  Si la extensión de la contraseña requerida es de 1 a 4 símbolos, la aplicación solicitará que el usuario establezca una contraseña con seguridad media. Debe ser numérica (PIN), con una secuencia que no tenga números repetidos u ordenados en secuencias (por ejemplo, 1234), o alfanumérica. El PIN o la contraseña debe tener al menos 4 caracteres.

  Si la extensión de la contraseña requerida es de 5 símbolos o más, la aplicación solicitará que el usuario establezca una contraseña con seguridad alta. Debe ser o numérica (PIN) con una secuencia que no tenga números repetidos u ordenados, o alfanumérica (contraseña). Un PIN debe tener al menos 8 dígitos. La contraseña debe tener al menos 6 caracteres.

- En dispositivos con Android 7.1.1, si la contraseña de desbloqueo no cumple con los requisitos de seguridad corporativa (Control de cumplimiento), la app del sistema Configuración podría funcionar incorrectamente cuando se intenta cambiar la contraseña de desbloqueo mediante Kaspersky Endpoint Security para Android. El problema se debe a un defecto conocido de Android 7.1.1. En este caso, solo use la aplicación Configuración del sistema para cambiar la contraseña de desbloqueo.

- En algunos dispositivos con Android 6 o posterior, si los datos del dispositivo están protegidos mediante cifrado de datos, puede ocurrir un error cuando se ingresa la contraseña de desbloqueo de la pantalla. Este problema se debe a características específicas del servicio de Accesibilidad con firmware MIUI.

- En algunos dispositivos con MDM de iOS, si se especifica el valor **Minimum number of special characters** y se marca la casilla **Allow simple password**, el dispositivo muestra información sobre cómo establecer una contraseña de 6 o más caracteres, aunque es posible establecer una contraseña de 4 o más caracteres.

Problemas conocidos que afectan la protección contra la eliminación de Kaspersky Endpoint Security para Android

- Se debe configurar Kaspersky Endpoint Security para Android como un administrador del dispositivo.
- Para proteger la aplicación contra la eliminación en dispositivos con Android 7 o posterior, Kaspersky Endpoint Security para Android debe estar configurado como función de accesibilidad.
- En algunos dispositivos HUAWEI y Xiaomi, la protección contra la eliminación de Kaspersky Endpoint Security para Android no funciona. Este problema se debe a características específicas del firmware MIUI 7 y 8 en Xiaomi y del firmware EMUI en HUAWEI.

Problemas conocidos al configurar las restricciones del dispositivo

- En dispositivos personales y dispositivos con un perfil de trabajo con Android 10 o posterior, no se admite la prohibición del uso de redes Wi-Fi.
- En dispositivos con Android 11 o versiones posteriores, Kaspersky Endpoint Security para Android debe estar configurado como una función de Accesibilidad. Kaspersky Endpoint Security para Android solicita al usuario que configure la app como una función de Accesibilidad a través del Asistente de configuración inicial. El usuario puede omitir este paso o desactivar este servicio más adelante en los ajustes del dispositivo. Si este es el caso, no podrá restringir el uso de la cámara.
- En los dispositivos MDM con iOS, los usuarios pueden habilitar los resultados de búsqueda en Internet de Spotlight en las sugerencias de Siri incluso si la casilla **Prohibit Spotlight suggestions** está marcada. Esto se debe a un problema reconocido por Apple.
- En los dispositivos Android, cuando el uso de la cámara está prohibido, algunas aplicaciones pueden cerrarse automáticamente. Este problema se debe a la forma en que los servicios y las funciones como Android System Intelligence y Atención a la pantalla usan la cámara del dispositivo para mantener la pantalla encendida mientras el usuario la mira.

Problemas conocidos al enviar comandos a dispositivos móviles

- En dispositivos con Android 12 o posterior, si el usuario otorgó el permiso "Usar ubicación aproximada", la aplicación Kaspersky Endpoint Security para Android primero intenta obtener la ubicación precisa del dispositivo. Si esto no es posible, se devuelve la ubicación aproximada del dispositivo solo si se recibió en los últimos 30 minutos. De lo contrario, el comando **Locate device** falla.
- El comando **Locate device** no funciona en dispositivos Android si la Precisión de ubicación de Google está deshabilitada en la configuración. Tenga en cuenta que no todos los dispositivos Android vienen con esta configuración de ubicación.
- Si envía el comando **Enable Lost Mode** a un dispositivo MDM con iOS supervisado sin una tarjeta SIM y el dispositivo se reinicia, no podrá conectarse a la red Wi-Fi y recibir el comando **Disable Lost Mode**. Esta es una característica específica de los dispositivos iOS. Para evitar este problema, puede enviar el comando solo a dispositivos con una tarjeta SIM o insertar una tarjeta SIM en el dispositivo bloqueado para permitirle recibir el comando **Disable Lost Mode** a través de la red móvil.

- El comando **Reset to factory settings** no está disponible para dispositivos personales y dispositivos con un contenedor corporativo con Android 14 o posterior.

- Antes de ejecutar el comando **Reset password**, la pantalla del dispositivo debe bloquearse y desbloquearse al menos una vez.

Problemas conocidos que afectan dispositivos específicos

- En ciertos dispositivos (por ejemplo, HUAWEI, Meizu y Xiaomi), debe otorgar un permiso de inicio automático a Kaspersky Endpoint Security para Android o agregarla manualmente a la lista de aplicaciones que se inician al arrancar el sistema operativo. Si la aplicación no se agrega a la lista:

  - Kaspersky Endpoint Security para Android deja de realizar todas sus funciones después de reiniciar el dispositivo móvil.

  - Si se bloqueó el dispositivo, no puede usar un comando para desbloquear el dispositivo. Puede desbloquear el dispositivo solo usando un código de desbloqueo de uso único.

  - En dispositivos con Xiaomi HyperOS, es posible que Kaspersky Endpoint Security para Android no analice las notificaciones de los servicios de mensajería instantánea para detectar URL maliciosas y de phishing.

- En ciertos dispositivos (por ejemplo, Meizu y Asus) que funcionan con Android 6 o posterior, después de cifrar datos y reiniciar el dispositivo Android, debe escribir una contraseña numérica para desbloquear el dispositivo. Si el usuario usa una contraseña gráfica para desbloquear el dispositivo, debe convertir la contraseña gráfica a una contraseña numérica. Para obtener más información sobre la conversión de una contraseña gráfica en una contraseña numérica, consulte el sitio web del Servicio de soporte técnico del fabricante del dispositivo móvil. Este problema está relacionado con el funcionamiento del servicio de funciones de accesibilidad.

- En algunos dispositivos HUAWEI con Android 5.X, una vez que se establece Kaspersky Endpoint Security para Android como característica de Accesibilidad, el dispositivo puede mostrar incorrectamente un mensaje acerca de la falta de derechos adecuados. Para ocultar este mensaje, habilite la aplicación como aplicación protegida en la configuración del dispositivo.

- En algunos dispositivos HUAWEI con Android 5.X o 6.X, cuando el modo de Ahorro de batería está habilitado para Kaspersky Endpoint Security para Android, el usuario puede cerrar manualmente la aplicación. El dispositivo del usuario queda desprotegido. Este problema se debe a algunas características del software de HUAWEI. Para restaurar la protección del dispositivo, ejecute Kaspersky Endpoint Security para Android manualmente. Se recomienda desactivar el modo de Ahorro de batería para Kaspersky Endpoint Security para Android en la configuración del dispositivo.

- En dispositivos HUAWEI con firmware EMUI que ejecutan Android 7, el usuario puede ocultar la notificación sobre el estado de protección de Kaspersky Endpoint Security para Android. Este problema se debe a algunas características del software de HUAWEI.

- En ciertos dispositivos Xiaomi, al configurar la longitud de la contraseña con más de cinco caracteres en una directiva, se solicitará al usuario que cambie la contraseña de desbloqueo de la pantalla en vez del código PIN. No puede configurar un código PIN que tenga más de 5 caracteres. Este problema se debe a algunas características del software de Xiaomi.

- En dispositivos Xiaomi con firmware MIUI que ejecutan Android 6, el ícono de Kaspersky Endpoint Security para Android puede ocultarse en la barra de estado. Este problema se debe a algunas características del software de Xiaomi. Se recomienda permitir la visualización de íconos de notificaciones en la configuración de Notificaciones.

- En algunos dispositivos Nexus con Android 6.0.1 los privilegios requeridos para el correcto funcionamiento no se pueden otorgar mediante el Asistente de inicio rápido de Kaspersky Endpoint Security para Android. Este problema ocurre debido a un defecto conocido de Security Patch para Android de Google. Para garantizar el buen funcionamiento, los privilegios requeridos se deben habilitar manualmente en la configuración del dispositivo.

- En ciertos dispositivos Samsung con Android 7 o versiones posteriores, cuando el usuario intenta configurar métodos no admitidos para desbloquear el dispositivo (por ejemplo, una contraseña gráfica), el dispositivo se puede bloquear si se satisfacen las siguientes condiciones: la protección de eliminación de Kaspersky Endpoint Security para Android está habilitada y existen requisitos de seguridad de la contraseña de desbloqueo de la pantalla. Para desbloquear el dispositivo, debe enviar un comando especial al dispositivo.

- En ciertos dispositivos Samsung, es imposible bloquear el uso de huellas digitales para desbloquear la pantalla.

- Protección web y Control web no pueden habilitarse en algunos dispositivos Samsung si el dispositivo está conectado a una red 3G/4G, tiene habilitado el modo de Ahorro de batería y restringe los datos en segundo plano. Se recomienda desactivar la función que restringe los procesos en segundo plano en la configuración de Ahorro de batería.

- En ciertos dispositivos Samsung, si la contraseña de desbloqueo no cumple con los requisitos de seguridad corporativa, Kaspersky Endpoint Security para Android no bloquea el uso de huellas digitales para desbloquear la pantalla.

- En algunos dispositivos Honor y HUAWEI, no se puede restringir el uso de Bluetooth. Cuando Kaspersky Endpoint Security para Android intenta restringir el uso de Bluetooth, el sistema operativo muestra una notificación con las opciones para rechazar o permitir esta restricción. El usuario puede rechazar esta restricción y seguir utilizando Bluetooth.

- En los dispositivos Blackview, el usuario puede borrar la memoria de la aplicación Kaspersky Endpoint Security para Android. Como consecuencia, la protección y la administración del dispositivo se deshabilitan, todas las configuraciones definidas se vuelven ineficaces y la aplicación Kaspersky Endpoint Security para Android se elimina de las funciones de accesibilidad. Esto se debe a que los dispositivos de este proveedor brindan privilegios elevados a la aplicación de pantallas recientes personalizada. Esta aplicación puede anular la configuración de Kaspersky Endpoint Security para Android, y no se puede reemplazar porque es parte del sistema operativo Android.

- En algunos dispositivos Google Pixel que ejecutan Android 11 o versiones anteriores, la aplicación Kaspersky Endpoint Security para Android se bloquea inmediatamente después del inicio. Esto se debe a un problema en Android.

- En HUAWEI P60 Pro, no se puede crear un contenedor corporativo.

- En algunos dispositivos MDM con iOS y modo de funcionamiento de control básico que ejecutan iOS 18.2 - iOS 18.3.1, el uso de Safari puede estar prohibido. Esto se debe a un problema reconocido por Apple.

- En ciertos dispositivos personales (por ejemplo, OnePlus, Honor) con Android 10 o versiones posteriores, se puede solicitar una contraseña al conectarse a redes Wi-Fi protegidas por el protocolo WPA2 PSK. Esto se debe a algunos problemas con la forma en que la API de sugerencias funciona.

- En dispositivos MDM con iOS 18.0, no se puede enviar al dispositivo una directiva con AirPlay configurado. Esto se debe a un problema reconocido por Apple. Para garantizar un funcionamiento adecuado, actualice iOS en el dispositivo.

Problemas conocidos que afectan la aplicación en Android 13

- En Android 13, el usuario puede usar el Administrador de tareas de servicios en primer plano para detener la ejecución de Kaspersky Endpoint Security en segundo plano. La causa de este problema es un defecto conocido de Android 13.

- En Android 13, el permiso para enviar notificaciones se solicita durante la configuración inicial de la aplicación. Esto se debe a las especificaciones del sistema operativo Android 13.

Problemas conocidos que afectan los perfiles de directiva

- Si cambia a una licencia con funcionalidad básica, la configuración que está disponible solo con una licencia con funcionalidad extendida no se restablece a los valores predeterminados en los perfiles de directiva.

Problemas conocidos en el control de acceso basado en roles

- Si no se otorga el derecho de administración de claves de licencia, cuando se abre una directiva existente, puede ocurrir un error. Esto no afecta el funcionamiento de la directiva.

- Si no se otorga el derecho de administración de claves de licencia, puede crear una directiva sin seleccionar la licencia en el asistente de directivas móviles. Sin embargo, en este caso, no puede configurar la directiva.

Problemas conocidos durante la configuración del Servidor web en la puerta de enlace de conexión (Agente de red Linux)

- Cuando configura los ajustes del Servidor web en una puerta de enlace de conexión, si se modifican los puertos o se emiten o vuelven a emitir certificados, es posible que la nueva configuración tarde un poco en sincronizarse con Kaspersky Security Center. Espere hasta 15 minutos o haga clic en **Force synchronization** en la pestaña **General** de las propiedades del host de la puerta de enlace de conexión (**Asset management** → **Assets (Devices)**).

- Cuando configura un certificado de Servidor web personalizado, si las direcciones de los campos **Web Server address** y **Certificate address** no coinciden, se mostrará un error. En este caso, para guardar la configuración, debe cargar un certificado diferente. Sin embargo, si cambia la dirección del Servidor web en las propiedades del punto de distribución de Kaspersky Security Center y el certificado sigue siendo el mismo, aún puede guardar esta configuración, incluso si las direcciones no coinciden.

Problemas conocidos durante la migración de Kaspersky Security Center Windows a Kaspersky Security Center Linux

- Al migrar la configuración del Servidor de MDM para iOS de Kaspersky Security Center Windows 14.2 a Kaspersky Security Center Linux, la configuración de notificación y almacenamiento de los eventos del Servidor de MDM para iOS no se transfiere y, en su lugar, toma los valores predeterminados. Después de la migración, deberá especificar los valores requeridos manualmente.

- Si un usuario se eliminó o no se encuentra en el servidor durante la migración, el certificado para dispositivos móviles se muestra en la lista de certificados sin el nombre de usuario.

Problemas conocidos que afectan el Servidor de MDM para iOS

- Pueden pasar al menos 6 horas hasta que el certificado del Servidor de MDM para iOS de reserva emitido se envíe al dispositivo.

Problemas conocidos que afectan el proxy de KSN

- Si los dispositivos móviles están conectados a Kaspersky Security Center a través de la puerta de enlace de conexión, el proxy de KSN no funciona. En este caso, deshabilite el interruptor **Enable KSN Proxy on Administration Server Enabled** en la sección **KSN Proxy** de la ventana de propiedades del Servidor de administración. Para obtener información detallada sobre cómo habilitar y deshabilitar el uso del proxy de KSN, consulte la Ayuda de Kaspersky Security Center.

Problemas conocidos que afectan a los eventos

- Después de actualizar el complemento Kaspersky Mobile Devices Protection and Management, es posible que los eventos nuevos se muestren incorrectamente en una directiva creada anteriormente: en la pestaña **Event configuration**, los eventos aparecen habilitados, pero la información sobre ellos no se transmite. Para asegurarse de que el complemento actualizado proporcione una lista actual de eventos para una directiva creada anteriormente, debe volver a guardar esta directiva.

Primeros pasos

Esta sección está dirigida a los especialistas que instalan MDM básico en Kaspersky Next Expert View (on-premise), así como a los especialistas que brindan soporte técnico a las organizaciones que utilizan MDM básico en Kaspersky Next Expert View (on-premise).

Arquitectura de la solución

El MDM básico en Kaspersky Next Expert View (on-premise) incluye los siguientes componentes:

- App móvil Kaspersky Endpoint Security para Android

  La aplicación protege dispositivos Android contra amenazas web, virus y otras aplicaciones que representan amenazas.

- Aplicación de Kaspersky Protection para iOS

  La aplicación protege dispositivos iOS contra la suplantación de identidad (phishing) y las amenazas web, y le permite detectar la liberación en los dispositivos.

- Complemento Kaspersky Mobile Devices Protection and Management

  El complemento le permite administrar dispositivos con Android y iOS en Kaspersky Next Expert View (on-premise).

- Servidor de MDM para iOS

  El Servidor de MDM para iOS le permite conectar dispositivos iOS al Servidor de administración y administrar dispositivos iOS.

- Complemento de configuración del Servidor de MDM para iOS

  El complemento le permite establecer la configuración del Servidor de MDM para iOS.

Escenarios de implementación

El despliegue de MDM básico en Kaspersky Next Expert View (on-premise) en Kaspersky Next Expert View (on-premise) consta de los siguientes pasos:

1. Implementar Kaspersky Security Center Linux y Kaspersky Next Expert View (on-premise)
2. Implementar complementos de administración móvil
3. Configurar el Servidor de administración para la conexión de dispositivos móviles
4. Implementar un sistema de administración de dispositivos iOS
5. Implementar un sistema de administración de dispositivos Android
6. Administración de dispositivos móviles en Kaspersky Next Expert View (on-premise)

Implementación de una solución de administración de dispositivos móviles

Para conectar y administrar dispositivos móviles mediante Kaspersky Next Expert View (on-premise), debe implementar una solución de administración de dispositivos móviles. En esta sección, se describen las acciones recomendadas para comenzar a utilizar MDM básico en Kaspersky Next Expert View (on-premise).

Implementación de Kaspersky Security Center Linux y Kaspersky Next Expert View (on-premise)

Seleccione el dispositivo Linux que desee utilizar como estación de trabajo del administrador. Asegúrese de que el dispositivo cumpla con los requisitos de software y hardware e instale Kaspersky Security Center y Kaspersky Next Expert View (on-premise) en el dispositivo.

Para obtener instrucciones sobre cómo instalar Kaspersky Security Center Linux, consulte la Ayuda de Kaspersky Security Center.

Para obtener instrucciones sobre cómo instalar Kaspersky Next Expert View (on-premise), consulte la Ayuda de Kaspersky Security Center.

Implementar complementos de administración móvil

Para usar MDM básico en Kaspersky Next Expert View (on-premise) y conectar dispositivos móviles, debe agregar e instalar los siguientes complementos de administración móvil:

- Kaspersky Mobile Devices Protection and Management
  - `on_prem_ksm_policies_<version>.zip`

    Archivo comprimido que contiene los archivos necesarios para instalar el complemento Kaspersky Mobile Devices Protection and Management:
    - `plugin.zip`

      Archivo comprimido que contiene el complemento Kaspersky Mobile Devices Protection and Management.
    - `signature.txt`

      Archivo que contiene la firma del complemento Kaspersky Mobile Devices Protection and Management.
- Configuración del Servidor de MDM para iOS
  - `on_prem_iosmdm_<version>.zip`

    Archivo comprimido que contiene los archivos necesarios para instalar el complemento de configuración del Servidor de MDM para iOS:
    - `plugin.zip`

      Archivo comprimido que contiene el complemento de configuración del Servidor de MDM para iOS.
    - `signature.txt`

      Archivo que contiene la firma del complemento de configuración del Servidor de MDM para iOS.

Para instalar un complemento de administración, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Settings** → **Web plug-ins**.
2. En la ventana que se abre, haga clic en **Add**.

   Se muestra una lista de complementos disponibles.

3. En la lista de complementos disponibles, haga clic en el nombre del complemento que desee instalar para seleccionarlo.

   Se muestra una página de descripción del complemento.

4. En la página de descripción del complemento, haga clic en **Install plug-in**.

5. Cuando la instalación se haya completado, haga clic en **OK**.

   El complemento de administración se descarga con la configuración predeterminada y se muestra en la lista de complementos de administración.

Puede agregar complementos y actualizar los complementos descargados desde un archivo. Puede descargar los complementos de administración y los complementos de administración web desde la página web del Servicio de soporte técnico de Kaspersky.

Para cargar o actualizar un complemento desde un archivo, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Settings** > **Web plug-ins**.

2. En la ventana que se abre:

   - Haga clic en **Add from file** para cargar un complemento desde un archivo.
   - Haga clic en **Update from file** para cargar la actualización de un complemento desde un archivo.

3. Especifique el archivo y la firma del archivo.

4. Cargue los archivos especificados.

   El complemento de administración se descarga del archivo y se muestra en la lista de complementos de administración.

La función de actualizaciones (incluido el suministro de actualizaciones de las firmas antimalware y de la base de código) y la función de KSN pueden dejar de estar disponibles en el software en el territorio de EE. UU.

Para obtener información sobre la compatibilidad de la versión del complemento y las versiones de Kaspersky Security Center, consulte los requisitos de hardware y software.

Configurar el Servidor de administración para la conexión de dispositivos móviles

Antes de conectar dispositivos móviles a Kaspersky Next Expert View (on-premise), debe definir la configuración de conexión en las propiedades del Servidor de administración.

Para configurar el Servidor de Administración para la conexión de dispositivos móviles:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), haga clic en el nombre del Servidor de administración.

2. En la ventana de propiedades del Servidor de administración que se abre, configure el puerto del Servidor de administración que usarán los dispositivos móviles:

   a. En la pestaña **General**, seleccione **Additional ports**.

   b. Habilite el botón de alternancia **Open port for mobile devices**.

      Si se selecciona esta opción, el puerto para dispositivos móviles se abrirá en el Servidor de administración.

   c. En el campo **Port for mobile device synchronization**, especifique el puerto que el Servidor de administración usará para la conexión de dispositivos móviles.

      El puerto 13292 se utiliza de forma predeterminada.

      Si el botón de alternancia **Open port for mobile devices** está desactivado o se seleccionó un puerto de conexión incorrecto, los dispositivos móviles no se podrán conectar al Servidor de administración.

3. Si es necesario, edite el certificado que utilizarán los dispositivos móviles para conectarse al Servidor de administración.

   > De forma predeterminada, el Servidor de administración utiliza el certificado creado tras abrir el puerto para dispositivos móviles. Puede reemplazar el certificado emitido por el Servidor de Administración por otro certificado o volver a emitirlo.

   Para editar el certificado, siga los siguientes pasos:

   a. En la pestaña **General**, elija la sección **Certificates**.

   b. Defina la configuración que requiera.

      Para obtener más información sobre cómo trabajar con certificados en Kaspersky Security Center Linux, consulte la Ayuda de Kaspersky Security Center.

4. Haga clic en el botón **Save** para almacenar los cambios que realizó y salir de la ventana de propiedades del Servidor de administración.

Se configura la conexión del dispositivo móvil.

Escenario: configurar una pasarela de conexión para conectar dispositivos móviles a Kaspersky Next Expert View (on-premise)

Una puerta de enlace de conexión es un Agente de red que opera de un modo especial. El Agente de red es un componente de Kaspersky Security Center que permite la interacción entre el Servidor de administración y las aplicaciones de Kaspersky. Las puertas de enlace de conexión aceptan conexiones de otros Agentes de red y las hacen llegar al Servidor de administración a través de la conexión que mantiene con el mismo.

A diferencia de un Agente de red normal, una puerta de enlace de conexión se puede configurar para esperar conexiones del Servidor de administración, en lugar de establecer conexiones con él. Una puerta de enlace de conexión en la DMZ recibe las conexiones del Servidor de administración a través del puerto TLS 13000. El Servidor de administración crea y mantiene una conexión permanente (denominada conexión de señal) con la puerta de enlace. Esto es necesario porque la puerta de enlace, al encontrarse en la DMZ, no puede acceder a los puertos del Servidor. La conexión de señal no se utiliza para transferir información, sino para enviar una invitación para interactuar con la red. Cuando la puerta de enlace necesita conectarse con el Servidor de administración, se lo hace saber a través de esta conexión; el Servidor, tras recibir este aviso, crea la conexión requerida para la transferencia de datos.

Una puerta de enlace de conexión le permite usar las funciones de seguridad de manera más eficiente para brindar protección a la infraestructura de la red contra posibles vulnerabilidades.

- El uso de una puerta de enlace de conexión hace que sea más fácil supervisar la actividad sospechosa en un nodo de red independiente fuera de una LAN (red de área local). Ayuda a evitar ataques maliciosos directos a través de un protocolo móvil, ya que implementa un protocolo diferente para las comunicaciones entre la puerta de enlace de conexión y Kaspersky Security Center.

- La superficie de posibles ataques de red es menor, ya que una puerta de enlace de conexión recibe las conexiones del Servidor de administración a través de un único puerto (de manera predeterminada, 13000) a través del cual se procesan todas las solicitudes.

- El uso de una puerta de enlace de conexión permite verificar el certificado para dispositivos móviles fuera de una LAN y evitar que los dispositivos envíen datos a Kaspersky Security Center antes de que se autentiquen, lo que protege la infraestructura de la red contra vulnerabilidades en protocolos de bajo nivel como TLS/SSL.

Requisitos

Para que una puerta de enlace de conexión funcione correctamente con dispositivos móviles, se deben cumplir los siguientes requisitos:

- El puerto 13293 o 13292 debe estar abierto en el host con la puerta de enlace de conexión.

  Estos puertos están diseñados para conectar y sincronizar dispositivos móviles.

  - Al usar el puerto 13293, el certificado TLS se verifica en la puerta de enlace de conexión (sin enviarse al Servidor de administración).

  - Cuando se usa el puerto 13292, el certificado no se verifica (se ignora el indicador LP_MobileMustUseTwoWayAuthOnPort13292).

- El puerto 13000 debe estar abierto entre la puerta de enlace de conexión y Kaspersky Security Center, a través del cual la puerta de enlace de conexión recibe conexiones del Servidor de administración. No es necesario que esté abierto fuera de la zona desmilitarizada (DMZ).
- El host debe tener una dirección estática accesible desde Internet.

Etapas

La configuración sigue estos pasos:

1. **Instalar el Agente de red con la función de puerta de enlace de conexión en un host**

   Primero, debe instalar el Agente de red en el dispositivo host seleccionado que actúa como puerta de enlace de conexión.

   Para obtener información sobre cómo generar un paquete de instalación del Agente de red, consulte la Ayuda de Kaspersky Security Center.

   Puede instalar el Agente de red en modo interactivo especificando los parámetros de instalación paso a paso. También puede usarse un archivo de respuestas: un archivo de texto que contiene un conjunto personalizado de parámetros de instalación (variables con sus respectivos valores). El archivo de respuestas permite realizar la instalación en modo no interactivo, es decir, sin involucrar al usuario. Para obtener información sobre cómo instalar el Agente de red en modo silencioso, consulte la Ayuda de Kaspersky Security Center.

2. **Configurar la puerta de enlace de conexión en el Servidor de administración de Kaspersky Security Center**

   Una vez que haya instalado el Agente de red con la función de puerta de enlace de conexión, debe conectarlo al Servidor de administración. El Servidor de administración aún no reconoce el dispositivo con la puerta de enlace de conexión entre los dispositivos administrados porque no se intentó conectar la puerta de enlace de conexión al Servidor de administración.

   Debe crear un nuevo grupo en el grupo **Managed Devices** y agregar el dispositivo que actúa como puerta de enlace de conexión al grupo que creó. Para obtener información sobre cómo agregar dispositivos manualmente a grupos en Kaspersky Next Expert View (on-premise), consulte la Ayuda de Kaspersky Security Center.

   Después de eso, asigne el dispositivo como punto de distribución y configure el punto de distribución para que actúe como puerta de enlace de conexión en la sección **Connection gateway** de las propiedades del punto de distribución. A continuación, habilite las opciones **Open port for mobile devices (SSL authentication of the Administration Server only)** y **Open port for mobile devices (two-way SSL authentication)** y especifique los puertos y los nombres de dominio DNS del punto de distribución para conectar dispositivos móviles.

   > Si la restricción básica 'CA: true' no está configurada para el certificado del Servidor de administración de un dispositivo móvil personalizado, se usará el mismo certificado para la puerta de enlace de conexión que para el Servidor de administración. Si se establece la restricción básica 'CA: true', se usará un certificado diferente del certificado del Servidor de administración de un dispositivo móvil personalizado para la pasarela de conexión.

3. **Volver a emitir el certificado para dispositivos móviles**

   Vuelva a emitir el certificado para dispositivos móviles con una nueva dirección de conexión especificada al configurar la pasarela de conexión (en la ventana de propiedades del Servidor de administración, seleccione **General** → **Certificates**). Para obtener información detallada sobre la reemisión de certificados móviles, consulte la sección Volver a emitir el certificado del Servidor de administración móvil.

Resultados

Se configurará la puerta de enlace de conexión. Podrá agregar nuevos dispositivos móviles especificando la dirección de la puerta de enlace de conexión.

Para asegurarse de que los dispositivos móviles estén sincronizados con Kaspersky Security Center en la puerta de enlace de conexión, la dirección de conexión que estableció al configurar la puerta de enlace de conexión debe especificarse en las propiedades de los paquetes de instalación de Kaspersky Endpoint Security para Android (**Operations** → **Repositories** → **Installation packages**).

Agregar paquetes de instalación al repositorio del Servidor de administración

Para una mayor implementación de los sistemas de administración móviles, debe agregar los siguientes paquetes de instalación al repositorio del Servidor de administración:

- Paquete de instalación del Agente de red Linux (para la instalación posterior del Agente de red en una estación de trabajo).
- Paquete de instalación del Servidor de MDM para iOS (para la instalación posterior del Servidor de MDM para iOS a fin de conectar y administrar dispositivos iOS).
- Paquete de instalación de Kaspersky Endpoint Security para Android (para la instalación posterior de Kaspersky Endpoint Security para Android en dispositivos).

Para obtener instrucciones sobre cómo agregar paquetes de instalación al repositorio del Servidor de administración, consulte la Ayuda de Kaspersky Security Center.

Agregar una clave de licencia al repositorio del Servidor de administración

Para conectar dispositivos móviles a Kaspersky Next Expert View (on-premise) y administrarlos, debe especificar una clave de licencia que admita la solución de Administración de dispositivos móviles.

La licencia con la que se utiliza la solución determina el alcance de la configuración básica o avanzada que puede configurar. Con una licencia que no proporciona la funcionalidad ampliada de MDM básico en Kaspersky Next Expert View (on-premise), solo está disponible la configuración básica de protección de dispositivos en el complemento Kaspersky Mobile Devices Protection and Management. Para obtener información detallada sobre las licencias, consulte la sección Acerca de la licencia.

Para especificar una clave de licencia en la configuración de licencia actual de las propiedades del Servidor de administración, siga estos pasos:

- En la ventana principal de Kaspersky Next Expert View (on-premise), haga clic en el nombre del Servidor de administración.

En la ventana de propiedades del Servidor de administración que se abre:

a. En la pestaña **General**, vaya a la sección **License keys**.

b. En el bloque de configuración **Current license**, haga clic en **Select** y realice una de las siguientes acciones:

- Elija una de las claves de licencia existentes.
- Especifique el archivo CLAVE que desea agregar.

> La licencia que elija debe ser compatible con la solución de administración de dispositivos móviles.

c. Haga clic en **Save**.

La clave de licencia se especifica en la configuración de licencia actual de las propiedades del Servidor de administración.

Para agregar una clave de licencia al repositorio del Servidor de administración:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Operations** → **Licenses**.
2. Clic en el botón **Add**.
3. En la ventana que se abre, haga clic en el botón **Add key file**.
4. Haga clic en **Select key file** y luego especifique el archivo de clave que desea agregar.

> La licencia que elija debe ser compatible con la solución de administración de dispositivos móviles.

5. Haga clic en **Save**.

La clave de licencia se agrega al repositorio del Servidor de administración.

Instalar el Agente de red Linux

El Agente d red Linux es un componente de Kaspersky Security Center que permite la interacción entre el Servidor de administración y las aplicaciones de Kaspersky instaladas en una estación de trabajo o un servidor.

Para implementar un sistema de administración de dispositivos iOS, debe instalar el Agente de red en una estación de trabajo en la que se implementará el Servidor de MDM para iOS más adelante. Una vez instalado el Agente de red, podrá configurar e instalar el Servidor de MDM para iOS para conectarse y administrar dispositivos iOS posteriormente.

Para obtener instrucciones sobre cómo instalar el Agente de red en Linux, consulte la Ayuda de Kaspersky Security Center.

Configurar el Servidor web de Kaspersky Security Center Linux

Servidor web de Kaspersky Security Center Linux (Servidor web) es un componente de Kaspersky Security Center Linux instalado junto con el Servidor de administración. El Servidor web está diseñado para la transmisión por red de paquetes de instalación independientes, perfiles de administración y archivos desde una carpeta compartida.

Los paquetes de instalación creados se publican en el Servidor web automáticamente y se eliminan después de la primera descarga. El administrador puede enviar el nuevo vínculo al usuario de cualquier manera que le resulte conveniente (por ejemplo, por correo electrónico).

Para obtener más información, consulte la ayuda de Kaspersky Security Center.

Para conectar dispositivos móviles, asegúrese de que el FQDN del Servidor web esté especificado correctamente en las propiedades del Servidor de administración:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), haga clic en el nombre del Servidor de administración.
2. En la ventana de propiedades del Servidor de administración que se abre, en la pestaña **General**, seleccione la sección **Web Server**.
3. En el campo **Web Server FQDN**, compruebe si los servidores DNS pueden resolver el FQDN (nombre de dominio completo) especificado.

Configurar el Servidor web en una puerta de enlace de conexión (Agente de red Linux)

En el punto de distribución se implementa un servicio de Servidor web independiente en el modo de puerta de enlace de conexión, lo que permite trabajar con dispositivos móviles conectados a Kaspersky Security Center. Este servicio es responsable de transferir paquetes de instalación de aplicaciones y perfiles de administración a los dispositivos sin conectarlos directamente al Servidor de administración. Los archivos se transfieren a medida de que el servicio procesa solicitudes de archivos HTTP/HTTPS en una puerta de enlace de conexión.

El Servidor web en una puerta de enlace de conexión solo funciona para descargar los siguientes tipos de archivos en los dispositivos móviles:

- Aplicaciones móviles de Kaspersky

  Paquetes de instalación de aplicaciones móviles de Kaspersky agregados a las directivas por el administrador mediante Kaspersky Next Expert View (on-premise).

- Aplicaciones móviles de terceros

  Paquetes de instalación de aplicaciones móviles de terceros creados por el administrador para su posterior instalación en dispositivos desde un archivo local.

- Perfiles de administración para dispositivos MDM con iOS

Para conectar nuevos dispositivos a Kaspersky Security Center, los paquetes de instalación y los perfiles de administración se publican en la pasarela de conexión del Servidor web si se implementó.

Los vínculos a los paquetes de instalación se encuentran en la configuración de la directiva y en las secciones "Aplicaciones y archivos" y "Paquetes de instalación" de Kaspersky Security Center.

Esta funcionalidad está disponible en Kaspersky Security Center Linux 15.2 o posterior.

El servicio de servidor web en una puerta de enlace de conexión se instala junto con el Agente de red Linux. Para utilizar esta funcionalidad, debe asignar un dispositivo que actuará como punto de distribución en modo de puerta de enlace de conexión para ser utilizado como servidor web y luego especificar las configuraciones correspondientes.

Asignar un dispositivo que actuará como punto de distribución en un modo de puerta de enlace de conexión

Para asignar un dispositivo que actuará como punto de distribución en un modo de puerta de enlace de conexión:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), haga clic en el nombre del Servidor de administración.
2. En la ventana de propiedades del Servidor de administración que se abre, en la pestaña **General**, seleccione la sección **Distribution points**.
3. Haga clic en **Assign**.
4. En la ventana que se abre, seleccione el dispositivo que actuará como punto de distribución.
5. Haga clic en **Aceptar**.

   El dispositivo seleccionado aparece en la lista de puntos de distribución.
6. Haga clic en el nombre del dispositivo.
7. En la ventana de propiedades de los puntos de distribución que se abre, seleccione la sección **Connection gateway**.
8. Habilite el interruptor **Connection gateway**.
9. Especifique el nombre de dominio DNS del punto de distribución bajo el cual estará disponible para los dispositivos móviles.
10. Haga clic en **Aceptar**.

Se asigna un dispositivo que actuará como punto de distribución en el modo de puerta de enlace de conexión.

Configurar el Servidor web en una puerta de enlace de conexión

Para configurar el Servidor web en una puerta de enlace de conexión, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), haga clic en el nombre del Servidor de administración.
2. En la ventana de propiedades del Servidor de administración que se abre, en la pestaña **General**, seleccione la sección **Web Server**.
3. En el bloque de configuración **Web Server settings on connection gateway (Network Agent for Linux)**, seleccione la casilla **Launch an additional Web Server on connection gateway**.

   Este Servidor web se utilizará para transferir archivos a los dispositivos.
4. En el campo **Connection gateway** que aparece, especifique el host en el que se implementará el Servidor web para que actúe como puerta de enlace de conexión. Solo los hosts que admiten esta funcionalidad se muestran en la lista desplegable.

5. En el bloque **Web Server settings for selected connection gateway** que se abre, configure los puertos del Servidor web:

   a. Seleccione **Open Web Server HTTPS port** si desea que se pueda acceder al Servidor web en el puerto HTTPS y que gestione las solicitudes HTTPS. También deberá configurar un certificado correspondiente para proteger este puerto.

      a. Especifique el **HTTPS port**.

      b. Especifique el **Certificate source** para el puerto HTTPS del Servidor web.

      De manera predeterminada, se utiliza el certificado emitido por el Servidor de administración: tiene una validez de 397 días y se renueva automáticamente después de su vencimiento. Si es necesario, puede renovar este certificado manualmente haciendo clic en el botón **Reissue**.

      Para continuar usando este certificado, seleccione **Issue certificate through Administration Server**. Para cargar un certificado personalizado manualmente, seleccione **Upload certificate from file**.

      Para cargar un certificado desde un archivo, siga estos pasos:

      - Haga clic en **Upload from file**.
      - En la ventana que se abre, seleccione el **Certificate format**.
      - Para un certificado **PKCS #12**, especifique la ruta al archivo del certificado (P12 o PFX) e ingrese la contraseña del certificado.

        Para un certificado **X.509**, especifique la ruta a los archivos de clave pública y privada e ingrese la contraseña de la clave privada.
      - Haga clic en **Guardar**.

   c. Asegúrese de que las direcciones en los campos **Web Server address** (la dirección del Servidor web cuyas solicitudes serán procesadas por Kaspersky Security Center) y **Certificate address** (la dirección del certificado emitido) coincidan. De lo contrario, deberá volver a emitir el certificado emitido por el Servidor de administración o cargar un certificado personalizado diferente.

   Para que los dispositivos descarguen archivos de forma segura desde el Servidor web en una puerta de enlace de conexión a través de HTTPS, el certificado del Servidor web debe estar instalado en estos dispositivos.

   b. Seleccione **Open Web Server HTTP port** si desea que se pueda acceder al Servidor web en el puerto HTTP y que gestione las solicitudes HTTP.

      a. Especifique el **HTTP port**.

   c. Haga clic en **Guardar**.

Configuración del Servidor web en una puerta de enlace de conexión

Si se cambia la configuración del puerto HTTP o HTTPS, debe actualizar los vínculos a los paquetes de instalación publicados anteriormente para los dispositivos móviles conectados al Servidor web en la puerta de enlace de conexión. Vuelva a publicar los vínculos en la configuración de la directiva y en las secciones "Aplicaciones y archivos" y "Paquetes de instalación" de Kaspersky Security Center.

Para actualizar los vínculos a los paquetes de instalación, siga estos pasos:

- En la sección "Aplicaciones y archivos":

  a. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Apps & files**.

  b. Haga clic en **Android** o **iOS** según el sistema operativo requerido.

  c. En la lista de aplicaciones que se abre, realice una de las siguientes acciones:

  - Seleccione las casillas de verificación junto a los nombres de las aplicaciones cuyos vínculos del paquete de instalación desea actualizar y, a continuación, haga clic en **Republish**.
  - Haga clic en los nombres de las aplicaciones cuyos vínculos del paquete de instalación desea actualizar y, a continuación, haga clic en **Republish** en la ventana que se abre.

- En la sección "Paquetes de instalación", realice lo siguiente:

  a. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Operations** → **Repositories** → **Installation packages**.

  b. En la ventana que se abre, haga clic en **View the list of stand-alone packages**.

  c. Seleccione la aplicación cuyo vínculo del paquete de instalación desea actualizar y, a continuación, haga clic en **Unpublish**.

  d. Haga clic en **Publish**.

Se actualizan los vínculos de los paquetes de instalación.

Transferir el certificado del Servidor web a dispositivos en la puerta de enlace de conexión

Para que los dispositivos descarguen archivos de forma segura desde el Servidor web en una puerta de enlace de conexión a través de HTTPS, el certificado del Servidor web debe estar instalado en estos dispositivos.

Transferir el certificado del Servidor web a dispositivos de MDM con iOS

Al conectar nuevos dispositivos MDM con iOS, Kaspersky Security Center agrega automáticamente la clave pública del certificado del Servidor web en una pasarela de conexión a los perfiles de administración.

Esto permite que los dispositivos verifiquen la conexión HTTPS y descarguen de forma segura aplicaciones de terceros desde el Servidor web en la puerta de enlace de conexión.

Si el certificado cambia, se actualiza en los dispositivos de MDM con iOS durante la sincronización con el Servidor de MDM para iOS.

Transferir el certificado del Servidor web a dispositivos Android

Si utiliza el Servidor web con un certificado autofirmado en lugar de uno firmado por una autoridad de certificación (CA), el administrador de descargas estándar de Android solo le permite descargar aplicaciones y paquetes de instalación desde el Servidor web en una pasarela de conexión a través de HTTP.

Para descargar de forma segura aplicaciones y paquetes de instalación desde un Servidor web con un certificado autofirmado a los dispositivos, puede utilizar el administrador de descargas integrado de Kaspersky Endpoint Security para Android que siempre utiliza el protocolo HTTPS. Para obtener información detallada, consulte la sección Seleccionar el administrador de descargas para dispositivos Android.

Migrar de Kaspersky Security Center Windows a Kaspersky Security Center Linux

Puede migrar datos de dispositivos móviles de Kaspersky Security Center Windows a Kaspersky Security Center Linux transfiriendo la infraestructura de administración de dispositivos móviles de Windows a servidores Linux. Después de la migración, los dispositivos móviles se conectan automáticamente a Kaspersky Security Center Linux sin la necesidad de una reconexión manual y se administran con la misma directiva que en los servidores de Windows.

Requisitos previos

Antes de comenzar:

- Antes de la migración, asegúrese de que las funciones de Kaspersky Security Center Windows que necesite sean compatibles con Kaspersky Security Center Linux. Para obtener información detallada sobre las características principales de Kaspersky Security Center como una solución basada en Windows o una solución basada en Linux, consulte la Ayuda de Kaspersky Security Center.
- Familiarícese con los **DBMS y las versiones de Kaspersky Security Center y del Servidor de MDM para iOS** entre los cuales es posible realizar la migración.
  - Los datos del dispositivo móvil se pueden migrar entre los siguientes DBMS:
    - Kaspersky Security Center Windows + Microsoft SQL Server → Kaspersky Security Center Linux + PostgreSQL, Postgres Pro
    - Kaspersky Security Center Windows + MariaDB → Kaspersky Security Center Linux + PostgreSQL, Postgres Pro
    - Kaspersky Security Center Windows + MySQL → Kaspersky Security Center Linux + PostgreSQL, Postgres Pro
    - Kaspersky Security Center Windows + PostgreSQL, Postgres Pro → Kaspersky Security Center Linux + PostgreSQL, Postgres Pro
    - Kaspersky Security Center Windows + MariaDB → Kaspersky Security Center Linux + MariaDB
    - Kaspersky Security Center Windows + MySQL → Kaspersky Security Center Linux + MySQL

Para habilitar la migración a PostgreSQL o Postgres Pro, debe instalar el parche para la versión correspondiente del Servidor de administración de Kaspersky Security Center Windows. Comuníquese con el Servicio de soporte técnico de Kaspersky para obtener el parche requerido.

Para Kaspersky Secure Mobility Management basado en Kaspersky Security Center Windows 14.2: 14.2.0.26967-pf5

Para Kaspersky Security Center Windows 14.2: 14.2.0.48079-pf5

Para Kaspersky Security Center Windows 15.1: 15.1.0.20748-pf2

Los parches mencionados son obligatorios. Para evitar posibles errores durante la migración, recomendamos instalar no solo las versiones obligatorias del parche, sino también todas las versiones anteriores (comenzando con pf1) que correspondan a la versión de Kaspersky Security Center desde la que realiza la migración.

Si usa MySQL o MariaDB como DBMS para Kaspersky Security Center Windows y Kaspersky Security Center Linux, antes de crear una copia de seguridad de datos, asegúrese de que el parámetro `lower_case_table_names` coincida con el DBMS actual y el nuevo.

Cuando instala MySQL o MariaDB para Kaspersky Security Center Linux, debe establecer este parámetro con el mismo valor especificado para Windows. Para obtener información detallada sobre cómo realizar copias de seguridad y restaurar los datos del Servidor de administración cuando usa MySQL o MariaDB, consulte la Ayuda de Kaspersky Security Center.

- La migración entre las siguientes versiones de Kaspersky Security Center es posible:
  - Consola de administración basada en MMC de Kaspersky Security Center Windows 14.2 (local) → Kaspersky Security Center Linux 15.4 Web Console (local)
  - Consola de administración basada en MMC de Kaspersky Security Center Windows 14.2.0.48079 (local) (para Kaspersky Secure Mobility Management) → Kaspersky Security Center Linux 15.4 Web Console (local)
  - Consola de administración basada en MMC de Kaspersky Security Center Windows 15.1 (local) → Kaspersky Security Center Linux 15.4 Web Console (local)
  - Kaspersky Security Center Windows 14.2 Web Console y Cloud Console (local) → Kaspersky Security Center Linux 15.4 Web Console (local)
  - Kaspersky Security Center Windows 15.1 Web Console y Cloud Console (local) → Kaspersky Security Center Linux 15.4 Web Console (local)
- Es posible realizar la migración entre las siguientes versiones del Servidor de MDM para iOS:
  - Servidor de MDM para iOS Windows 14.2 (para Kaspersky Secure Mobility Management) → Servidor de MDM para iOS Linux 15.4
  - Servidor de MDM para iOS Windows 14.2 → Servidor de MDM para iOS Linux 15.4
  - Servidor de MDM para iOS Windows 15.1 → Servidor de MDM para iOS Linux 15.4

- Obtenga más información sobre los **datos que se transfieren durante la migración**.

  Se eliminan los siguientes datos:

  - Configuración de Kaspersky Security Center
    - FQDN para la conexión de dispositivos móviles a Kaspersky Security Center
    - Configuración específica para dispositivos móviles: licencias, configuración de integración de Firebase Cloud Messaging (FCM), certificados para firmar perfiles de administración, configuración para emitir certificados para dispositivos móviles, información sobre Contratos de licencia de usuario final aceptados, configuración de proxy de Kaspersky Security Network (KSN), archivos de configuración de Kaspersky Private Security Network (KPSN)

      Si utiliza Kaspersky Security Center compilación 14.2.0.26967, para migrar la configuración de FCM a Postgres correctamente, debe instalar el parche 14.2.0.26967-pf4. Si el parche no está instalado, la migración fallará debido a un error de la base de datos. En este caso, para evitar errores, elimine toda la configuración de FCM antes de la migración.

      La configuración de integración de PKI para emitir certificados para dispositivos móviles no se migra.

    - Archivos de configuración de control de acceso basado en roles
    - Configuración de actualización de la base de datos de Kaspersky Endpoint Security para Android.
    - Claves de firma para archivos APK de Kaspersky Endpoint Security para Android
  - Dispositivos móviles
    - Información sobre dispositivos móviles administrados por Kaspersky Endpoint Security para Android y Kaspersky Protection para iOS
    - Registros de eventos de dispositivos móviles administrados por Kaspersky Endpoint Security para Android y Kaspersky Protection para iOS
    - Historial de comandos ejecutados anteriormente y pendientes en dispositivos Android y sus resultados
    - Información sobre vínculos, paquetes de instalación y perfiles de administración creados para dispositivos móviles en espera de conexión
    - Configuración y paquetes de instalación de Kaspersky Endpoint Security para Android
    - Configuración y paquetes de instalación del Servidor de MDM para iOS

      La información sobre dispositivos Android en espera de conexión no se migra.

- Directivas
  - Directivas para la administración de dispositivos móviles en la Consola de administración de Kaspersky Security Center basada en MMC (dispositivos Android y dispositivos iOS)
  - Directivas para la administración de dispositivos móviles en Kaspersky Security Center Web Console y Cloud Console (dispositivos Android y dispositivos iOS)
- Certificados
  - Certificados del Servidor de administración móvil (certificados principal y de reserva, certificados del Servidor web)
  - Información sobre certificados de usuario (certificados móviles, de correo y VPN) y sus estados
- Servidores de MDM para iOS
  - Servidor de MDM para iOS instalados
  - Registros de eventos del Servidor de MDM para iOS
- Configuración del Servidor de MDM para iOS, certificados (certificado del Servidor de MDM para iOS, certificado de APNs) y perfiles de configuración

  Las aplicaciones del Servidor de MDM para iOS no se migran.

  Los datos específicos del host, como la información sobre los perfiles creados para dispositivos móviles en espera de conexión y los comandos en espera de ejecución, no se migran.

  Al migrar la configuración del Servidor de MDM para iOS de Kaspersky Security Center Windows 14.2 a Kaspersky Security Center Linux, la configuración de notificación y almacenamiento de los eventos del Servidor de MDM para iOS no se transfiere y, en su lugar, toma los valores predeterminados. Después de la migración, deberá especificar los valores requeridos manualmente.
- Servidor web
  - Configuración y paquetes de instalación de Kaspersky Endpoint Security para Android
  - Configuración y paquetes de instalación del Servidor de MDM para iOS

  Las aplicaciones para dispositivos móviles almacenadas en el Servidor web de Kaspersky Security Center no se migran mediante la utilidad klbackup y deben transferirse manualmente.
- Configuración de la puerta de enlace de conexión (Agente de red)

Los complementos de administración de dispositivos móviles instalados no se migran. Después de restaurar los datos del Servidor de administración y del Servidor de MDM para iOS desde una copia de

seguridad, debe descargar e instalar el complemento de Kaspersky Mobile Devices Protection and Management y el complemento del Servidor de MDM para iOS.

Etapas

El proceso de migración implica la creación de una copia de seguridad de datos mediante la utilidad *klbackup* para transferir los datos del Servidor de administración y usar la utilidad *kliosbackup* para transferir los datos del Servidor de MDM para iOS.

Para que los dispositivos móviles transferidos se muestren correctamente en Kaspersky Next Expert View (on-premise), se deben migrar tanto el Servidor de administración como el Servidor de MDM para iOS. Primero debe migrar el Servidor de administración y luego el Servidor de MDM para iOS, como se describe en el siguiente escenario.

La migración se realiza en etapas:

1. **Prepárese para la migración**

   1. Asegúrese de que tiene la cuenta de usuario interna del administrador con la que puede iniciar sesión en el Servidor de administración.

      La cuenta del administrador se utilizará para iniciar sesión en el Servidor de administración de Kaspersky Security Center Linux. Si no tiene esta cuenta e inició sesión solo con una cuenta local de Windows o con una cuenta de dominio, no podrá iniciar sesión en el Servidor de administración de Kaspersky Security Center Linux después de restaurar la copia de seguridad. El Servidor de administración de Kaspersky Security Center Linux no admite el inicio de sesión con la cuenta local de Windows. Es posible iniciar sesión con la cuenta de dominio, pero puede requerir una configuración adicional del Servidor de administración.

      Si no tiene la cuenta de administrador, tendrá que crear esta cuenta después de restaurar los datos de la copia de seguridad mediante la utilidad kladduser.

   2. En Kaspersky Security Center Windows, habilite la opción **Inherit settings from Administration Server or parent group** en la sección **Security** de la ventana de propiedades del grupo **Managed devices** para garantizar la herencia de los derechos y el acceso a la configuración de la directiva.

      La sección **Security** está disponible si la casilla **Display security settings sections** está marcada en la ventana de configuración de la interfaz.

   3. Cree una tarea para descargar actualizaciones al repositorio de Kaspersky Security Center.

      Esta tarea es necesaria para descargar el último archivo de configuración de control de acceso basado en roles de los servidores de Kaspersky al repositorio del Servidor de administración. Para obtener información detallada sobre cómo crear esta tarea, consulte la Ayuda de Kaspersky Security Center.

   4. Si necesita migrar las directivas creadas en el complemento de Kaspersky Security for Mobile (Policies) de Kaspersky Security Center Web Console y Cloud Console, elimine todos los perfiles de directivas. Las directivas de este complemento que contienen perfiles de directivas no se migrarán.

2. **Cree una copia de seguridad actualizada de los datos del Servidor de administración de Kaspersky Security Center Windows**

Según el tipo de DBMS utilizado para Kaspersky Security Center Windows y Kaspersky Security Center Linux, realice una de las siguientes acciones:

- Para la migración de MySQL o MariaDB a MySQL o MariaDB: cree una copia de seguridad con la utilidad klbackup en el dispositivo con el Servidor de administración instalado.
- Para la migración de Microsoft SQL Server a MySQL o MariaDB: cree una copia de seguridad con la utilidad klbackup, con la opción **Migrate to MySQL/MariaDB format** habilitada.
- Para la migración de Microsoft SQL Server a PostgreSQL o Postgres Pro:

  a. Instale un parche para la versión correspondiente del Servidor de administración de Windows de Kaspersky Security Center:

  - Para Kaspersky Secure Mobility Management basado en Kaspersky Security Center Windows 14.2: 14.2.0.26967-pf5
  - Para Kaspersky Security Center Windows 14.2: 14.2.0.48079-pf5
  - Para Kaspersky Security Center Windows 15.1: 15.1.0.20748-pf2

  Comuníquese con el Servicio de soporte técnico de Kaspersky para obtener estos parches.

  b. Cree una copia de seguridad con la utilidad klbackup.

  - Si ejecuta klbackup desde la línea de comandos, use el indicador `-migrate postgres`.
  - Si usa la interfaz de klbackup, habilite la opción **Migrate to Postgres format**.

  c. Desconecte el Servidor de administración de Kaspersky Security Center Windows de la red.

3 Prepare un nuevo dispositivo para la instalación de Kaspersky Security Center Linux

1. Seleccione un nuevo dispositivo en el que desea instalar el Servidor de administración. Este dispositivo debe cumplir con los requisitos de hardware y software.
2. Asegúrese de que los puertos usados en el Servidor de administración estén disponibles.
3. Asigne al nuevo dispositivo el mismo nombre de host y FQDN que en el servidor de Windows.
4. Configure la variable de entorno `KLCS_FF_UMDM_POLICIES_MIGRATION` en 1:

   ```
   export KLCS_FF_UMDM_POLICIES_MIGRATION=1
   ```

   Como alternativa, inmediatamente después de la instalación de Kaspersky Security Center Linux, use la utilidad klscflag para configurar el indicador del servidor correspondiente mediante el siguiente comando:

   ```
   klscflag -fset -pv .core/.independent -s klcsff -n KLCS_FF_UMDM_POLICIES_MIGRATION -t d -v 1
   ```

4 Instale y configure el DBMS

1. Elija el tipo de DBMS que proporciona un rendimiento óptimo teniendo en cuenta la cantidad de dispositivos en red, la topología de la red y la carga en la red. Puede elegir uno de los DBMS compatibles.
2. Instale el DBMS que corresponda al tipo de DBMS que seleccionó al crear la copia de seguridad. Para obtener información detallada sobre la instalación del DBMS seleccionado, consulte su documentación.

   La nueva versión de la base de datos no debe ser inferior a la vigente.

3. Configure el DBMS para trabajar con Kaspersky Security Center Linux.

5 Instale Kaspersky Security Center Linux y complete la migración del Servidor de administración

1. Instale Kaspersky Security Center Linux en el nuevo dispositivo.

   La cuenta de usuario interna del administrador creada durante la instalación, así como otros objetos (grupos, directivas, tareas, usuarios) creados antes de restaurar los datos del Servidor de administración desde la copia de seguridad, se perderán después de la restauración. Estos objetos serán reemplazados por objetos contenidos en la copia de seguridad.

2. Una vez completada la instalación, restaure los datos del Servidor de administración en el nuevo dispositivo mediante la utilidad klbackup.

   Debido a las limitaciones de PostgreSQL, es necesario otorgar temporalmente privilegios de superusuario de PostgreSQL a la cuenta que utiliza el Servidor de administración para conectarse al DBMS.

   Recomendamos que inicie el proceso de restauración de datos inmediatamente después de instalar Kaspersky Security Center Linux sin reinicios intermedios.

3. Si no tenía la cuenta de usuario interna del administrador con la que inició sesión en el Servidor de administración de Kaspersky Security Center Windows y utilizó una cuenta local de Windows o una cuenta de dominio, cree una cuenta de administrador mediante la utilidad kladduser:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <contraseña>
   ```

   donde el parámetro `<contraseña>` cumple con los siguientes requisitos:

   - La contraseña de usuario no puede tener menos de 8 caracteres ni más de 256.
   - La contraseña debe incluir caracteres de al menos tres de los grupos enumerados a continuación:
     - Letras mayúsculas (A-Z)
     - Letras minúsculas (a-z)
     - Números (0-9)
     - Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

4. Verifique el estado de restauración (por ejemplo, con el comando `journalctl -u kladminserver_srv.service -b`) para asegurarse de que las directivas de dispositivos móviles se migren correctamente.

5. Instale Kaspersky Security Center Web Console.

6. Iniciar sesión en Kaspersky Security Center Web Console con la cuenta de usuario interna del administrador.

   El proceso de inicialización de datos suele tardar hasta 15 minutos después de que se restauran los datos del Servidor de administración. El tiempo exacto depende del rendimiento del hardware y del volumen de datos del Servidor de administración. Durante este tiempo, es posible que Kaspersky Security Center Web Console no se conecte y muestre errores.

7. Implemente los complementos de administración de dispositivos móviles.

8. Instale el Agente de red Linux.

9. Una vez que la inicialización de los datos en la base de datos haya finalizado, asegúrese de comprobar que las principales funciones del Servidor de administración funcionen como es debido. Verifique que el Servidor de administración se sincronice con los dispositivos administrados y que se hayan restaurado los datos del Servidor de administración.

   La sincronización forzada con dispositivos móviles se realiza para verificar su conexión después de la migración.

10. Sondee los controladores de dominio para restaurar la información sobre la estructura del dominio, las cuentas de usuario, los grupos y los nombres DNS de los dispositivos incluidos en los dominios.

11. Si es necesario, desinstale el Servidor de administración y el servidor de bases de datos del dispositivo anterior.

    No debe haber varios servidores de administración en la misma red con la misma dirección de conexión y certificado de Servidor de administración.

    El administrador ahora tiene acceso a los datos y dispositivos del Servidor de administración administrados anteriormente por Kaspersky Security Center Windows, teniendo en cuenta la disponibilidad de funciones en Kaspersky Security Center Linux.

    Para que la opción **Guardar historial de ubicaciones** de la configuración de la directiva **Seguimiento de ubicaciones** funcione correctamente, agregue el tipo de evento **Historial de ubicaciones del dispositivo** en la pestaña **Configuración de eventos** y habilite su almacenamiento en la base de datos del Servidor de administración en las propiedades del evento. Esta acción debe realizarse para todas las directivas migradas.

6 Migre los datos de Windows del Servidor de MDM para iOS

Si tiene varios Servidores de MDM para iOS instalados, debe realizar el procedimiento de migración para cada uno de ellos.

1. Asegúrese de que el FQDN del Servidor de MDM para iOS de Linux sea el mismo que el FQDN del Servidor de MDM para iOS de Windows.
2. Si tiene certificados de reserva del Servidor de MDM para iOS, asegúrese de que el archivo kliosmdm.ini ubicado en el directorio de trabajo del Servidor de MDM para iOS contenga la contraseña SrvResCertPwd.

   Si no hay contraseña en el archivo kliosmdm.ini, vuelva a emitir o elimine el certificado de reserva del Servidor de MDM para iOS (kliosmdmserver2_cert.pem), cuya contraseña no se encuentra en el archivo.
3. Cree una copia de seguridad del Servidor de MDM para iOS con la utilidad kliosbackup.
4. Implemente el Servidor de MDM para iOS en el nuevo dispositivo con Kaspersky Security Center Linux instalado.
5. Transfiera los archivos con los datos de la copia de seguridad del Servidor de MDM para iOS al nuevo dispositivo.
6. Restaure los datos del Servidor de MDM para iOS con la utilidad kliosbackup.

   Si algún valor de configuración no se migra, se reemplazará con el valor predeterminado.

Una vez que se completa el proceso de migración, todos los dispositivos conectados se sincronizan automáticamente con el Servidor de MDM para iOS de Linux sin la necesidad de volver a conectarse.

Hacer una copia de seguridad y restaurar los datos del Servidor de administración con la utilidad klbackup

La migración de Kaspersky Security Center Windows a Kaspersky Security Center Linux se realiza mediante la utilidad klbackup, que se incluye en el kit de distribución de Kaspersky Security Center. Una vez instalado el Servidor de administración, encontrará la utilidad en la raíz de la carpeta de destino especificada durante la instalación de la aplicación.

Para migrar los datos de Windows del Servidor de administración mediante la utilidad klbackup, siga estos pasos:

1. Cree una copia de seguridad de los datos del Servidor de administración en un dispositivo Windows que tenga el Servidor de administración instalado
2. Restaure los datos del Servidor de administración a partir de la copia de seguridad creada en un dispositivo Linux

Hacer una copia de seguridad de los datos del Servidor de administración en un dispositivo Windows

Puede hacer una copia de seguridad de los datos de Windows del Servidor de administración mediante la utilidad klbackup, que se ejecuta en dos modos:

- Interactivo
- No interactivo

Hacer una copia de seguridad de los datos de Windows del Servidor de administración en modo interactivo

Para crear una copia de seguridad de los datos de Windows del Servidor de administración en modo interactivo, siga estos pasos:

1. En un dispositivo Windows, ejecute la utilidad klbackup ubicada en la carpeta de instalación de Kaspersky Security Center (de manera predeterminada, `C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center\klbackup.exe`).

2. En la primera ventana del asistente, seleccione **Perform backup of Administration Server data**.

   Haga clic en **Next**.

3. En la siguiente ventana del asistente, haga lo siguiente:

   a. Especifique la **Backup destination folder**.

   b. Habilite la opción **Migrate database**.

   c. Seleccione una de las siguientes opciones:

      a. **Migrar al formato de MySQL/MariaDB**

      Habilite esta opción si el Servidor de administración utiliza SQL Server como DBMS y usted desea migrar los datos de SQL Server a un DBMS de MySQL o MariaDB. Kaspersky Security Center creará una copia de seguridad compatible con MySQL y MariaDB. Podrá restaurar los datos de esa copia en MySQL o MariaDB.

      b. **Migrate to Postgres format**

      Habilite esta opción si el Servidor de administración utiliza SQL Server como DBMS y usted desea migrar los datos de SQL Server a un DBMS de PostgreSQL o Postgres Pro. Kaspersky Security Center creará una copia de seguridad compatible con PostgreSQL y Postgres Pro. Después de eso, podrá restaurar los datos de la copia de seguridad en PostgreSQL o Postgres Pro.

      Esta opción está disponible solo si instala un parche para la versión correspondiente del Servidor de administración de Windows de Kaspersky Security Center. Comuníquese con el Servicio de soporte técnico de Kaspersky para obtener el parche requerido.

      Para Kaspersky Secure Mobility Management basado en Kaspersky Security Center Windows 14.2: 14.2.0.26967-pf5

      Para Kaspersky Security Center Windows 14.2: 14.2.0.48079-pf5

      Para Kaspersky Security Center Windows 15.1: use el 15.1.0.20748-pf2

   d. Habilite la opción **Include current date and time in the name of the backup destination folder**

e. Configure una contraseña para la protección de los datos confidenciales.

Haga clic en **Next** para iniciar el proceso de copia de seguridad.

Se crea una copia de seguridad de los datos del Servidor de administración.

Puede ocurrir un error al restaurar los datos del Servidor de administración a partir de una copia de seguridad creada con la utilidad klbackup en modo interactivo. Si crea una copia de seguridad con la utilidad klbackup con el parche 15.1.0.20748-pf2 instalado y la opción **Migrate database** deshabilitada, se produce un error al restaurar esta copia (para todos los DBMS, excepto MySQL y MariaDB). Si desea crear una copia de seguridad con el parche 15.1.0.20748-pf2 instalado sin migrar a otro DBMS, ejecute la utilidad klbackup desde la línea de comandos.

Hacer una copia de seguridad de los datos de Windows del Servidor de administración en modo silencioso

Para crear una copia de seguridad de los datos de Windows del Servidor de administración en modo silencioso, ejecute la utilidad klbackup con el conjunto de claves requerido desde la línea de comandos del dispositivo que tiene el Servidor de administración instalado.

Ejemplo:

```
cd 'C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center\'
klbackup.exe -migrate postgres -path BACKUP_PATH -use_ts -password PASSWORD
```

Si no se especificó una contraseña en la línea de comandos de klbackup, la utilidad solicitará que se ingrese la contraseña de modo interactivo.

Descripciones de las claves:

- `-path BACKUP_PATH`: guarde la información en la carpeta `BACKUP_PATH` (parámetro obligatorio).

  La cuenta del servidor de bases de datos y la utilidad klbackup deben contar con permisos para modificar los datos de la carpeta `BACKUP_PATH`.

- `-migrate mysql`: cree una copia de seguridad de los datos del Servidor de administración almacenados en la base de datos de SQL Server que es compatible con MySQL (incluido MariaDB). Puede restaurar los datos de esa copia en MySQL.

- `-migrate postgres`: cree una copia de seguridad de los datos del Servidor de administración almacenados en la base de datos de SQL Server que es compatible con PostgreSQL y Postgres Pro. Puede restaurar los datos de la copia de seguridad en PostgreSQL o Postgres Pro.

  Esta opción está disponible solo si instala un parche para la versión correspondiente del Servidor de administración de Windows de Kaspersky Security Center. Comuníquese con el Servicio de soporte técnico de Kaspersky para obtener el parche requerido.

  Para Kaspersky Secure Mobility Management basado en Kaspersky Security Center Windows 14.2: 14.2.0.26967-pf5

  Para Kaspersky Security Center Windows 14.2: 14.2.0.48079-pf5

  Para Kaspersky Security Center Windows 15.1: 15.1.0.20748-pf2

- `-use_ts`: al guardar datos, copie la información a la carpeta `BACKUP_PATH`, a la subcarpeta con un nombre en el formato `klbackup YYYY-MM-DD # HH-MM-SS`, que incluye la fecha y hora actuales de la hora de operación de copia de respaldo en UTC. Si no se especifica una clave, la información se guarda en la raíz de la carpeta `BACKUP_PATH`.

  Aparece un mensaje de error durante cualquier intento de guardar información en una carpeta que ya almacena una copia de seguridad. En este caso, no se actualiza información.

  La clave `-use_ts` le permite mantener un archivo comprimido de datos del Servidor de administración. Por ejemplo, si la clave `-path` indica la carpeta `C:\KLBackups`, entonces la carpeta `klbackup 2025/6/19 # 11-30-18` almacena información sobre el estado del Servidor de administración con fecha de 19 de junio de 2025, a las 11:30:18 h.

- `-password PASSWORD`: contraseña para proteger los datos confidenciales.

  Si olvida la contraseña, no podrá recuperarla. No hay requisitos para la contraseña. La longitud de la contraseña es ilimitada y también puede tener una longitud cero (es decir, sin contraseña).

Para ver una lista completa de las claves de la utilidad, consulte la Ayuda de Kaspersky Security Center.

Restaurar los datos del Servidor de administración en un dispositivo Linux

Puede restaurar los datos de Windows del Servidor de administración desde un depósito de copias de seguridad en un dispositivo Linux en modo silencioso; para ello, ejecute la utilidad klbackup con el conjunto de claves requerido desde la línea de comandos.

Cuando utiliza la utilidad klbackup, los indicadores del Agente de red no se restauran y deben configurarse manualmente.

Ejemplo:

```
/opt/kaspersky/ksc64/sbin/klbackup -path BACKUP_PATH -restore -password PASSWORD
```

Descripciones de las claves:

- `-path BACKUP_PATH`: utilice los datos de la carpeta `BACKUP_PATH` para la restauración (parámetro obligatorio).

  La cuenta del servidor de bases de datos y la utilidad klbackup deben contar con permisos para modificar los datos de la carpeta `BACKUP_PATH`.

- `-restore`: restaure los datos del Servidor de administración. Los datos se restauran con la información contenida en la carpeta `BACKUP_PATH`. Si no se especifica una clave, se crea una copia de seguridad de los datos en la carpeta `BACKUP_PATH`.

- `-password PASSWORD`: contraseña para proteger los datos confidenciales.

  Cuando restaura los datos, debe ingresar la contraseña especificada durante la creación de la copia de seguridad.

Para ver una lista completa de las claves de la utilidad, consulte la Ayuda de Kaspersky Security Center.

Hacer una copia de seguridad y restaurar los datos del Servidor de MDM para iOS con la utilidad kliosbackup

La migración del Servidor de MDM para iOS de Windows al Servidor de MDM para iOS de Linux se realiza mediante la utilidad kliosbackup, que le permite realizar una copia de seguridad y restaurar la información en todos los dispositivos de MDM con iOS conectados y sus propiedades. La utilidad se ejecuta en modo silencioso.

Para que los dispositivos móviles transferidos se muestren correctamente en Kaspersky Next Expert View (on-premise), se deben migrar tanto el Servidor de administración como el Servidor de MDM para iOS. Para obtener información detallada sobre el escenario de migración, consulte la sección Migrar de Kaspersky Security Center Windows a Kaspersky Security Center Linux.

De manera predeterminada, la utilidad kliosbackup se encuentra en la siguiente carpeta de instalación:

- Para Windows: `C:\Program Files (x86)\Kaspersky Lab\Mobile Device Management for IOS`
- Para Linux: `/opt/kaspersky/iosmdm/bin/`

Para migrar los datos de Windows del Servidor de MDM para iOS mediante la utilidad kliosbackup, siga estos pasos:

1. Cree una copia de seguridad de los datos del Servidor de MDM para iOS en un dispositivo Windows que tenga instalado el Servidor de MDM para iOS.

   Ejecute kliosbackup con el conjunto de claves requerido desde la línea de comandos.

   Ejemplo:
   ```
   kliosbackup -backup -path BACKUP_PATH [-pwd PASSWORD]
   ```

2. Restaure los datos del Servidor de MDM para iOS a partir de la copia de seguridad creada en un dispositivo Linux.

   Transfiera los archivos con los datos de la copia de seguridad del Servidor de MDM para iOS a un dispositivo Linux y luego ejecute kliosbackup con el conjunto de claves requerido desde la línea de comandos.

   Ejemplo:
   ```
   kliosbackup -restore -path BACKUP_PATH [-pwd PASSWORD]
   ```

Descripciones de las claves:

- `-backup`: cree una copia de seguridad de los datos del Servidor de MDM para iOS.
- `-restore`: restaure los datos del Servidor de MDM para iOS. Los datos se restauran con la información contenida en la carpeta `BACKUP_PATH`.
- `-path BACKUP_PATH`: especifique una ruta local a la carpeta con los datos de la copia de seguridad.
- `-pwd PASSWORD`: establezca una contraseña para la copia de seguridad.

Implementar un sistema de administración de dispositivos iOS

MDM básico en Kaspersky Next Expert View (on-premise) le permite administrar dispositivos móviles con iOS. En esta sección se describe la implementación de un sistema de administración de dispositivos iOS.

Acerca de los modos de funcionamiento del dispositivo iOS

El modo de funcionamiento del dispositivo depende del propietario del dispositivo móvil (personal o corporativo) y los requisitos corporativos de seguridad. Puede elegir el modo de funcionamiento que sea más conveniente para la empresa y usar varios modos al mismo tiempo.

Los siguientes modos de funcionamiento del dispositivo están disponibles para dispositivos iOS:

- Protección básica
- Control básico
- Supervisado

Protección básica

La *protección básica* es el modo de funcionamiento del dispositivo para dispositivos iOS personales o corporativos. Este modo de funcionamiento le permite protegerse contra las amenazas de web y detectar el jailbreaking en los dispositivos mediante la aplicación Kaspersky Protection para iOS.

Control básico

El control básico es el modo de funcionamiento del dispositivo para dispositivos iOS personales. Este modo de funcionamiento le permite brindar protección y realizar una administración básica de dispositivos.

En este modo, el usuario tiene permiso para usar un Apple ID personal, trabajar con cualquier aplicación y almacenar datos personales en el dispositivo. Puede configurar la directiva para controlar el acceso del usuario a los recursos corporativos y administrar otros requisitos de seguridad.

Para administrar dispositivos iOS en el modo de funcionamiento de control básico, debe tener un Servidor de MDM para iOS instalado y configurado.

Supervisado

Supervisado es el modo de funcionamiento para los dispositivos iOS corporativos. Este modo de funcionamiento proporciona una gama más amplia de configuraciones para definir a través de la directiva que los dispositivos en otros modos de funcionamiento, por ejemplo:

- Envíe comandos adicionales para administrar la configuración de Bluetooth, actualizar el sistema operativo, localizar el dispositivo o activar la alarma en Modo perdido.
- Administrar restricciones avanzadas:
  - Restricciones de red (prohibir la modificación de la configuración del punto de acceso personal, prohibir la creación de configuraciones de VPN, forzar la activación de Wi-Fi y permitir la conexión a redes Wi-Fi específicas, prohibir la modificación de la configuración de Bluetooth).
  - Restricciones de aplicaciones (por ejemplo, prohibir la instalación de aplicaciones desde Apple Configurator e iTunes).
  - Prohibir el acceso a dispositivos USB en Archivos y deshabilitar el acceso a dispositivos USB cuando el dispositivo está bloqueado.
- Ajuste la configuración avanzada de Control de aplicaciones (por ejemplo, cree listas personalizadas de aplicaciones permitidas y aplicaciones prohibidas).
- Ajuste la configuración de Control web.
- Configure un servidor proxy HTTP para supervisar el tráfico de Internet en un dispositivo dentro de la red corporativa.

Para administrar dispositivos iOS en el modo de funcionamiento supervisado, debe tener un Servidor de MDM para iOS instalado y configurado y los dispositivos cambiados al estado supervisado en Apple Configurator. Para obtener información detallada sobre cómo trabajar con Apple Configurator, consulte el sitio web del Servicio de soporte técnico de Apple.

Acerca de los perfiles de administración

Un *perfil de administración* es un perfil que contiene la configuración para conectar dispositivos móviles iOS a Kaspersky Security Center. Después de la instalación del perfil de administración y la sincronización del dispositivo con el Servidor de MDM para iOS, el dispositivo se convierte en un dispositivo administrado (dispositivo MDM con iOS). Los dispositivos MDM con iOS se administran a través del Servicio de notificaciones push de Apple (APNs).

Con un perfil de administración, puede hacer lo siguiente:

- Configurar de forma remota dispositivos iOS mediante directivas.
- Enviar comandos a dispositivos MDM con iOS.
- Instalar remotamente aplicaciones de Kaspersky y aplicaciones de terceros.

El despliegue de un perfil de administración se lleva a cabo a través de Kaspersky Next Expert View (on-premise) mediante el Asistente de conexión de dispositivos móviles. El usuario instala el perfil de administración después de recibir un correo electrónico con los detalles para conectar el dispositivo móvil a Kaspersky Security Center. No se requieren preparaciones adicionales para el perfil.

Antes de instalar un perfil de administración, debe desplegar un sistema de administración de dispositivos iOS.

Implementar Kaspersky Protection para iOS

Los dispositivos iOS en el modo de funcionamiento de protección básica están protegidos por la aplicación Kaspersky Protection para iOS instalada en los dispositivos de los usuarios.

Esta sección contiene información sobre las funciones de la aplicación Kaspersky Protection para iOS, así como el proceso de instalación, activación, actualización y eliminación.

Acerca de Kaspersky Protection para iOS

Kaspersky Protection para iOS garantiza la protección de los dispositivos móviles contra el phishing y las amenazas web. Kaspersky Protection para iOS ofrece las siguientes funciones clave:

- Protección web
- Detección de liberación

Protección web

Protección web bloquea los sitios web maliciosos diseñados para propagar código malicioso y también bloquea sitios web fraudulentos diseñados para robar datos confidenciales del usuario (por ejemplo, contraseñas de servicios bancarios en línea o sistemas de dinero electrónico) y acceder a la información financiera del usuario. Protección web también supervisa la actividad de red de las aplicaciones y todo el tráfico del sistema en el dispositivo del usuario.

Protección web usa el servicio en la nube de Kaspersky Security Network para analizar sitios web antes de que se abran. Tras el análisis, Protección Web permite que se carguen los sitios web de confianza y bloquea los que son maliciosos.

Solo se analiza el dominio del sitio web. Si se trata de un dominio malicioso o de phishing, Protección web bloquea la amenaza. Si el dominio no está clasificado como malicioso o como phishing, la URL específica no se bloquea.

La Protección web requiere lo siguiente para funcionar en un dispositivo administrado:

- El uso de Kaspersky Security Network está habilitado en la configuración de la directiva de Kaspersky Next Expert View (on-premise).
- El usuario permitió que la aplicación Kaspersky Protection para iOS agregara una configuración de VPN.

Puede configurar este componente de la aplicación en Kaspersky Next Expert View (on-premise) al especificar la configuración de directivas correspondiente.

Detección de liberación

Cuando la aplicación de Kaspersky Protection para iOS detecta un jailbreak, muestra un mensaje crítico y le informa sobre el problema.

Una liberación permite evadir las funciones de seguridad del sistema operativo, por lo que no se puede garantizar la seguridad del dispositivo del usuario y pueden surgir varios problemas, incluidos los siguientes:

- Vulnerabilidades de seguridad
- Problemas de estabilidad
- Interrupción de los servicios de Apple
- Posibles fallas y bloqueos
- Reducción de la duración de la batería
- Imposibilidad de aplicar las actualizaciones de iOS

Instalación de Kaspersky Protection para iOS

Después de completar el Asistente de conexión de dispositivos móviles, la aplicación se puede instalar de las siguientes maneras:

- Si elige la opción **Send a message to users' email addresses**, los usuarios especificados recibirán correos electrónicos con códigos QR y vínculos para conectar dispositivos móviles al Servidor de administración. El vínculo contiene toda la información sobre la configuración de conexión que se transferirá automáticamente a la aplicación durante la instalación.

  El vínculo de invitación es válido durante 24 horas. Si el usuario no logra instalar la aplicación a tiempo, cree y envíe una nueva invitación.

  Una vez que el usuario instale Kaspersky Protection para iOS, el dispositivo iOS en el modo de funcionamiento de protección básica se conectará al Servidor de administración y aparecerá en la pestaña **Devices** de Kaspersky Next Expert View (local).

  Si el dispositivo del usuario no está conectado a Kaspersky Security Center, el usuario puede activar la aplicación manualmente utilizando el código de activación que envíe.

- Si elige la opción **Show the details after completing the wizard**, los detalles de la conexión estarán disponibles en la pantalla Finalizar. Escanee el código QR con la cámara del dispositivo iOS en el que desea instalar la aplicación.

Activar Kaspersky Protection para iOS

En Kaspersky Security Center, la licencia puede cubrir varios grupos de funciones. Para garantizar que la aplicación Kaspersky Protection para iOS sea totalmente funcional, la licencia de Kaspersky Security Center adquirida por la organización debe admitir la funcionalidad de Administración de dispositivos móviles.

Para obtener información detallada sobre las opciones de licencia, consulte la sección Acerca de la licencia.

La aplicación Kaspersky Protection para iOS se activa en un dispositivo móvil al proporcionar información de licencia válida a la aplicación. La información de la licencia se envía al dispositivo junto con la configuración de la directiva al sincronizar el dispositivo con Kaspersky Security Center.

Si la activación de la aplicación móvil no se completa en 30 días a partir del momento en que se instala en el dispositivo móvil, la aplicación cambia automáticamente al modo de funcionalidad limitada. En este modo, la mayoría de los componentes de la aplicación no son operativos. En modo de funcionalidad limitada, la aplicación deja de realizar la sincronización automática con Kaspersky Security Center. Por lo tanto, en caso de no haberse completado la activación de la aplicación 30 días después de la instalación, el usuario debe sincronizar manualmente el dispositivo con Kaspersky Security Center.

Si Kaspersky Security Center no está implementado en su organización o no está accesible a los dispositivos móviles, los usuarios pueden activar la aplicación móvil en sus dispositivos de forma manual.

Para activar la aplicación móvil:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Haga clic en el botón **License**.

4. En la ventana que se abre, utilice la lista desplegable para seleccionar la clave de licencia requerida del almacenamiento de claves del Servidor de administración.

   Los detalles de la clave de licencia se muestran en los campos a continuación.

   Si se selecciona un archivo de clave del almacenamiento de claves de Kaspersky Security Center y se envía al dispositivo, Kaspersky Security para iOS no podrá procesarlo, ya que no admite este método de activación. Para activar Kaspersky Protection para iOS, debe agregar un código de activación a Kaspersky Security Center.

   Puede reemplazar la clave de activación existente en el dispositivo móvil si es diferente de la seleccionada en la lista desplegable anterior. Para hacerlo, seleccione la casilla **Replace with selected key if the key on devices is different**.

   Sin embargo, en algunos dispositivos iOS, la clave de activación existente puede ser reemplazada por una nueva en segundo plano más tarde de lo esperado si el usuario sale de Kaspersky Protection para iOS deslizando hacia arriba en el Selector de aplicaciones. Para forzar una actualización de licencia, el usuario debe volver a abrir la aplicación. Para obtener más información sobre las restricciones y recomendaciones relacionadas con la optimización de la ejecución de tareas en segundo plano, consulte la sección Problemas conocidos de Kaspersky Protection para iOS.

5. Haga clic en el botón **Save** para guardar los cambios que realizó.

La aplicación se activa después de la siguiente sincronización del dispositivo con el Servidor de administración.

El usuario también puede comunicarse con el administrador para obtener un código de activación e ingresarlo manualmente.

Actualización de Kaspersky Protection para iOS

Kaspersky Protection para iOS se actualiza siguiendo el procedimiento de actualización estándar de las aplicaciones en la plataforma de iOS. Para obtener información detallada sobre la actualización, consulte la sección Actualizar la aplicación.

Eliminación de Kaspersky Protection for iOS

Un usuario elimina la aplicación Kaspersky Protection para iOS de forma manual siguiendo el procedimiento de eliminación de aplicaciones estándar en la plataforma de iOS. Para obtener información detallada acerca de la eliminación, consulte la sección Eliminar la aplicación.

Implementar un sistema de administración mediante el protocolo MDM de iOS

Los dispositivos iOS con los modos de funcionamiento de control básico y supervisado se administran mediante el protocolo MDM para iOS. Para implementar un sistema de administración de dispositivos móviles mediante el protocolo MDM para iOS y conectar dispositivos iOS a Kaspersky Security Center, siga estos pasos:

1. **Implementar el Servidor de MDM para iOS**
2. **Recibir un certificado de APNs**
3. **Instalar el certificado de APNs en el Servidor de MDM para iOS**
4. **Conectar los dispositivos iOS a Kaspersky Security Center**

Implementar un Servidor de MDM para iOS

El Servidor de MDM para iOS es un componente de MDM básico en Kaspersky Next Expert View (on-premise) que permite que los dispositivos MDM con iOS se conecten a Kaspersky Security Center y facilita la administración de estos dispositivos a través de Apple Push Notifications (APNs) mediante la instalación de perfiles de administración exclusivos en ellos.

El Servidor de MDM para iOS recibe conexiones entrantes de dispositivos móviles a través de su puerto TLS (de forma predeterminada, puerto 443), que es administrado por Kaspersky Security Center mediante el Agente de red. El Agente de red se instala localmente en un dispositivo que tiene también instalado un Servidor de MDM para iOS.

El número de copias del Servidor de MDM para iOS que se debe instalar se puede seleccionar según el hardware disponible o el número total de dispositivos móviles cubiertos.

Tenga en cuenta que la cantidad máxima recomendada de dispositivos móviles que se administrarán a través del Servidor de MDM para iOS es de 50 000. A fin de reducir la carga, el grupo completo de dispositivos se puede distribuir entre varios servidores que tengan instalado el Servidor de MDM para iOS.

Comparación de las funciones del Servidor de MDM para iOS según las herramientas de administración

Las funciones disponibles del Servidor de MDM para iOS dependen de las herramientas de administración.

Puede administrar la configuración del Servidor de MDM para iOS utilizando las siguientes consolas de Kaspersky Security Center:

- Kaspersky Security Center Web Console
- Kaspersky Security Center Cloud Console

La siguiente tabla compara las funciones disponibles en estas herramientas.

Disponibilidad de funciones por herramienta de administración

	Web Console	Cloud Console
General		
Instalar servidor MDM para iOS	Disponible	Disponible
Actualizar servidor MDM para iOS	Disponible	No disponible
Eliminar servidor MDM para iOS	Disponible	No disponible
Ver la lista de Servidores de MDM para iOS instalados	Disponible	Disponible
Ver y modificar la configuración de Servidores de MDM para iOS instalados	Disponible	Disponible
Seleccionar un certificado para firmar un perfil de administración	Disponible	No disponible
Ver la lista de eventos de Servidor de MDM para iOS	Disponible	Disponible
Configurar eventos de Servidor de MDM para iOS	Disponible	Disponible
Servidor proxy de APNs		
Configurar un proxy para acceder a APNs	Disponible	No disponible
Certificados		
Recibir, renovar e instalar un certificado de APNs	Disponible	Disponible
Administrar un certificado de Servidor de MDM para iOS	Disponible	No disponible
Administrar un certificado de reserva de Servidor de MDM para iOS	Disponible	No disponible
Administrar un certificado raíz de Servidor de MDM para iOS	Disponible	No disponible
Configuración de conexión		
Configurar un período de sincronización	Disponible	Disponible
Configurar un punto de acceso local	Disponible	No disponible
Configurar un punto de acceso externo	Disponible	No disponible
Configurar un perfil de administración	Disponible	Disponible
Perfiles de configuración		
Administrar perfiles de configuración	Disponible	Disponible

Configurar un paquete de instalación del Servidor de MDM para iOS

Antes de instalar el Servidor de MDM para iOS, debe configurar las propiedades del paquete de instalación del Servidor de MDM para iOS.

El paquete de instalación del Servidor de MDM para iOS es un archivo comprimido que contiene los archivos necesarios para la instalación del Servidor de MDM para iOS según el administrador de paquetes y la arquitectura:
`kliosmdm-<arquitectura>-<versión>-<administrador de paquetes>_<idioma>.tar.gz`

Para configurar un paquete de instalación del Servidor de MDM para iOS, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Operations → Repositories → Installation packages**.

2. En la ventana que se abre, haga clic en el paquete de instalación del Servidor de MDM para iOS que desee configurar.

   Se abre la ventana de propiedades del paquete de instalación.

3. En la pestaña **Configuración**, especifique las propiedades del Servidor de MDM para iOS.

   a. En el grupo de ajustes **Connection settings**, configure las siguientes propiedades:

   Se recomienda utilizar los valores predeterminados.

   - **iOS MDM external connection port**. En este campo, especifique un puerto externo para conectar los dispositivos móviles al servicio MDM para iOS.

     Los dispositivos móviles usan el puerto externo 5223 para comunicarse con el servidor de APNs. Asegúrese de que el puerto 5223 esté abierto en el firewall para la conexión con el intervalo de direcciones 17.0.0.0/8.

     El puerto 443 se utiliza para la conexión con el Servidor de MDM para iOS de forma predeterminada. Si el puerto 443 ya está siendo utilizado por otro servicio o aplicación, puede ser remplazado con, por ejemplo, el puerto 9443.

     El Servidor de MDM para iOS utiliza el puerto 2197 para enviar notificaciones al servidor de APNs. Los servidores de APNs se ejecutan en el modo de balance de cargas. Los dispositivos móviles no siempre se conectan a las mismas direcciones IP para recibir notificaciones. El rango de direcciones 17.0.0.0/8 está reservado para Apple, motivo por el que se recomienda que especifique este rango completo como un rango permitido en la configuración del Firewall.

   - **Network Agent connection port**. En este campo, especifique un puerto para conectar el servicio MDM para iOS al Agente de red. El número de puerto predeterminado es 9799.

   - **iOS MDM local connection port**. En este campo, especifique un puerto local para conectar el Agente de red al servicio MDM para iOS. El número de puerto predeterminado es 9899.

   b. En el grupo de configuraciones de **iOS MDM Server address**, especifique la dirección de la estación de trabajo en la que se instalará el Servidor de MDM para iOS. Esta dirección se usará para conectar dispositivos móviles administrados al servicio MDM para iOS. La estación de trabajo debe estar disponible para establecer la conexión de los dispositivos MDM con iOS.

   Seleccione una de las siguientes opciones:

   - **Use FQDN device name**. Se utilizará el nombre de dominio completo (FQDN) del dispositivo.

   - **Use specified address**. Especifique la dirección específica del dispositivo manualmente.

     No agregue el esquema de URL y el número de puerto en la cadena de direcciones. Estos valores se agregarán automáticamente.

4. Haga clic en **Guardar**.

Las propiedades del paquete de instalación del Servidor de MDM para iOS están configuradas. Ahora puede instalar el Servidor de MDM para iOS con la configuración especificada.

Instalar el Servidor de MDM para iOS mediante una tarea de instalación remota

Kaspersky Next Expert View (on-premise) le permite instalar el Servidor de MDM para iOS de forma remota mediante una tarea de instalación remota. Esta tarea se crea y se asigna a hasta 1000 dispositivos a través del asistente correspondiente. El asistente ayudará a instalar el Servidor de MDM para iOS en un grupo de administración, en dispositivos con direcciones IP específicas o en una selección de dispositivos administrados.

Tenga en cuenta que no podrá especificar la configuración del Servidor de MDM para iOS durante la instalación. La configuración se establece en las propiedades del paquete de instalación del Servidor de MDM para iOS.

Antes de instalar el Servidor de MDM para iOS en un dispositivo, asegúrese de que los complementos de Kaspersky Mobile Devices Protection and Management y de Configuración del Servidor de MDM para iOS estén instalados.

Para instalar el Servidor de MDM para iOS mediante una tarea de instalación remota, siga estos pasos:

1. Instale el Agente de red en la estación de trabajo en la que se implementará el Servidor de MDM para iOS.
2. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **iOS MDM Servers**.
3. Haga clic en **Install**.

   Se inicia el Asistente para crear una nueva tarea. Realice las acciones que le indica el asistente usando el botón **Siguiente**.
4. En la ventana **New task settings** que se abre:
   a. En el campo **Task name**, especifique un nombre personalizado para la tarea, si es necesario (el nombre predeterminado es "Instalar el Servidor de MDM para iOS").
   b. En el grupo de configuraciones **Devices to which the task will be assigned**, seleccione **Specify device addresses manually or import addresses from a list**. Puede especificar los nombres DNS, las direcciones IP y las subredes IP de los dispositivos a los cuales desee asignar la tarea.
5. En el paso **Task scope**:
   a. Haga clic en **Add devices**.
   b. En la ventana que se abre, en la lista desplegable, seleccione la opción **Select networked devices detected by Administration Server**.
   c. Seleccione dispositivos o una selección de dispositivos.
   d. Haga clic en **Agregar**.

   Después de agregar los dispositivos, se muestran en la tabla.

6. En el paso **Installation packages**, defina los siguientes ajustes:

   a. En el campo **Select installation package**, seleccione el paquete de instalación del Servidor de MDM para iOS configurado.

   b. En el campo **Select Network Agent**, seleccione el Agente de red instalado.

   c. En el grupo de configuración **Force installation package download**, seleccione la casilla **Using Network Agent** para distribuir los archivos necesarios para la instalación del Servidor de MDM para iOS a través del Agente de red.

   d. En el campo **Maximum number of concurrent downloads**, especifique el número máximo permitido de dispositivos a los que el Servidor de administración puede transmitir simultáneamente los archivos.

   e. En el campo **Maximum number of installation attempts**, especifique el número máximo de veces que se permitirá la ejecución del instalador.

   f. Especifique la siguiente configuración adicional:

   - Haga clic en la casilla **Do not re-install application if it is already installed** La aplicación no se volverá a instalar si ya se instaló en el dispositivo.

   - Haga clic en la casilla **Verify operating system type before downloading**. Antes de transmitir los archivos a los dispositivos, Kaspersky Security Center verifica si la configuración de la utilidad de Instalación puede aplicarse al sistema operativo del dispositivo. Si la configuración no es corresponde, Kaspersky Security Center no transmite los archivos y no intenta instalar la aplicación. A modo de ejemplo, si necesita instalar una aplicación en los dispositivos de un grupo de administración que contenga dispositivos con sistemas operativos diferentes, puede asignar la tarea de instalación al grupo de administración y habilitar esta opción para que la tarea no afecte a aquellos dispositivos que no tengan el sistema operativo pertinente.

7. En el siguiente paso del asistente, se le pedirá que seleccione la acción que se realizará si el proceso de instalación le solicita que reinicie el sistema operativo. Seleccione la opción **Do not restart the device** u omita este paso, ya que no se aplica al sistema operativo Linux.

8. En el paso **Select accounts to access devices**, seleccione la opción **No account required (Network Agent installed)**. Si selecciona esta opción, no necesitará especificar la cuenta con la que se ejecutará el instalador de la aplicación. Para ejecutar la tarea, se usará la cuenta con la que se haya iniciado el servicio del Servidor de administración. Esta opción no está disponible si el Agente de red no se instaló en los dispositivos.

9. En el paso **Finish task creation**, haga clic en el botón **Finish** para crear la tarea y cerrar el asistente.

El Servidor de MDM para iOS se instala mediante una tarea de instalación remota.

Al reinstalar el Servidor de MDM para iOS desde cero, debe eliminar la carpeta /var/opt/kaspersky/iosmdm en el host con el Servidor de MDM para iOS instalado. Si la carpeta no se eliminó, el certificado del antiguo Servidor de MDM para iOS se usará automáticamente durante la instalación y se emitirá un certificado de reserva a la dirección del Servidor de MDM para iOS recién instalado, si se cambió.

Si solo necesita actualizar el Servidor de MDM para iOS sin reinstalarlo desde cero, no es necesario que elimine la carpeta especificada.

Para obtener más información sobre la configuración adicional, los métodos de distribución de archivos y la sección Asignación de la tarea a un dispositivo, consulte la ayuda de Kaspersky Security Center.

Instalación local del Servidor de MDM para iOS en un dispositivo a través de un paquete de instalación

Kaspersky Next Expert View (on-premise) le permite instalar el Servidor de MDM para iOS en un dispositivo local usando un paquete de instalación, es decir, sin ingresar interactivamente la configuración de instalación.

Antes de instalar el Servidor de MDM para iOS en un dispositivo, asegúrese de que los complementos de Kaspersky Mobile Devices Protection and Management y de Configuración del Servidor de MDM para iOS estén instalados.

Para instalar y configurar manualmente el Servidor de MDM para iOS en un dispositivo local, siga estos pasos:

1. Instale el Servidor MDM para iOS:

   a. Lea el contrato de licencia de usuario final. Use el comando a continuación únicamente si comprende y acepta los términos del Contrato de licencia de usuario final.

   b. Según su sistema operativo, ejecute uno de los siguientes comandos para iniciar el archivo de instalación:

      a. Para Debian:
      ```
      apt install /<ruta>/kliosmdm_<número_de_versión>_amd64.deb
      ```

      b. Para Red Hat Enterprise Linux:
      ```
      yum install /<ruta>/kliosmdm_<número_de_versión>.x86_64.rpm -y
      ```

      Se instala el Servidor de MDM para iOS. El instalador ofrece iniciar el procedimiento de configuración mediante la ejecución del script postinstall.pl.

2. Configure el Servidor de MDM para iOS con uno de los siguientes métodos:

   a. Configuración con los parámetros *posteriores a la instalación* especificados por el asistente interactivo paso a paso:

      a. Ejecute el siguiente comando:
      ```
      /opt/kaspersky/iosmdm/lib/bin/setup/postinstall.pl
      ```

   b. Configuración con los argumentos clave especificados como parámetros *posteriores a la instalación*:

      a. Ejecute el siguiente comando:
      ```
      opt/kaspersky/bin/postinstall.pl -- < parámetros >
      ```

      donde `< parámetros >` es uno de los parámetros especificados en la tabla de *configuración de instalación del Servidor de MDM para iOS* a continuación.

En la siguiente tabla se enumeran los nombres y valores posibles de los parámetros que pueden configurarse al instalar el Servidor de MDM para iOS. Puede especificar estos parámetros en el orden que le convenga.

Nombre de configuración	Descripción de la configuración	Valores
EULA_ACCEPTED	Aceptación de los términos del Contrato de licencia de usuario final. Esta configuración es obligatoria.	• *1*: leí, comprendo y acepto en su totalidad los términos del Contrato de licencia de usuario final. • *Otro valor o ningún valor*: no acepto los términos del Contrato de licencia (no se realizará la instalación).
DONT_USE_ANSWER_FILE	Usar o no un archivo de respuesta TXT con la configuración de instalación del Servidor de MDM para iOS. El archivo se incluye en el paquete de instalación o se almacena en el Servidor de administración. No tiene que especificar una ruta adicional al archivo. Esta configuración es obligatoria.	• *1*: no usar una respuesta con la configuración • *Otro valor o sin valor*: usar un archivo de respuesta con la configuración
CONNECTORPORT	Puerto local para conectar el servicio MDM para iOS al Agente de red. El número de puerto predeterminado es 9799. Esta configuración es opcional.	Valor numérico: *9799*
LOCALSERVERPORT	Puerto local para conectar un Agente de red al servicio MDM para iOS. El número de puerto predeterminado es 9899. Esta configuración es opcional.	Valor numérico: *9899*
EXTERNALSERVERPORT	Puerto para conectar un dispositivo al Servidor de MDM para iOS. El número de puerto predeterminado es 443. Esta configuración es opcional.	Valor numérico: *443*
EXTERNAL_SERVER_URL	La dirección externa del dispositivo en el cual se debe instalar el Servidor de MDM para iOS. Esta dirección se usará para conectar dispositivos móviles administrados al servicio MDM para iOS. El dispositivo debe estar disponible para la conexión a través de MDM para iOS. La dirección no debe incluir el esquema de la URL y el número del puerto ya que estos valores se agregarán automáticamente. Esta configuración es opcional.	FQDN del dispositivo: *example.fqdn.com*

Ejemplo:

```
/opt/kaspersky/bin/postinstall.pl --EULA 1 --DONT_USE_ANSWER_FILE 1 --EXTERNALSERVERPORT 9443 --CONNECTORPORT 9799
```

Para instalar y configurar automáticamente el Servidor de MDM para iOS en modo silencioso con un archivo de respuesta, siga estos pasos:

Un *archivo de respuesta* es un archivo de texto que contiene un conjunto personalizado de configuraciones de instalación (variables y sus valores correspondientes).

1. Cree un archivo de respuesta (en formato TXT) en el directorio donde se realizará la instalación: `/tmp/answers.txt`.
2. Especifique los valores requeridos en el archivo de respuesta:
   - EULA_ACCEPTED=1

     Aceptación de los términos del Contrato de licencia de usuario final.
   - KLIOSMDM_AUTOINSTALL=1

     Usar un archivo de respuesta TXT con la configuración de instalación del Servidor de MDM para iOS.

- EXTERNALSERVERPORT=443

  Puerto para conectar un dispositivo al Servidor de MDM para iOS.

- CONNECTORPORT=9799

  Puerto local para conectar el servicio MDM para iOS al Agente de red.

- LOCALSERVERPORT=9899

  Puerto local para conectar un Agente de red al servicio MDM para iOS.

- EXTERNAL_SERVER_URL=example.fqdn.com

  La dirección externa del dispositivo en el cual se debe instalar el Servidor de MDM para iOS.

3. Asigne el nombre completo del archivo de respuestas (con su ruta de acceso) a la variable de entorno KLAUTOANSWERS, por ejemplo `export KLAUTOANSWERS=/tmp/answers.txt`.

4. Ejecute la instalación del Servidor de MDM para iOS.

El Servidor de MDM para iOS se instala y configura en modo silencioso automáticamente con un archivo de respuesta.

Al reinstalar el Servidor de MDM para iOS desde cero, debe eliminar la carpeta /var/opt/kaspersky/iosmdm en el host con el Servidor de MDM para iOS instalado. Si la carpeta no se eliminó, el certificado del antiguo Servidor de MDM para iOS se usará automáticamente durante la instalación y se emitirá un certificado de reserva a la dirección del Servidor de MDM para iOS recién instalado, si se cambió.

Si solo necesita actualizar el Servidor de MDM para iOS sin reinstalarlo desde cero, no es necesario que elimine la carpeta especificada.

Actualizar el Servidor de MDM para iOS mediante una tarea de instalación remota o local

Kaspersky Next Expert View (on-premise) le permite actualizar el Servidor de MDM para iOS mediante una tarea de instalación remota o localmente en un dispositivo.

Tenga en cuenta que no podrá especificar la configuración del Servidor de MDM para iOS durante la actualización. La configuración se establece en las propiedades del paquete de instalación del Servidor de MDM para iOS.

Para actualizar el Servidor de MDM para iOS mediante una tarea de instalación remota, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **iOS MDM Servers**.

2. Haga clic en **Update**.

   Se inicia el Asistente para crear una nueva tarea. Realice las acciones que le indica el asistente usando el botón **Siguiente**.

3. En la ventana **New task settings** que se abre:

    a. En el campo **Task name**, especifique un nombre personalizado para la tarea, si es necesario (el nombre predeterminado es Actualizar Servidor de MDM para iOS).

    b. En el grupo de configuración **Devices to which the task will be assigned**, se mostrará el dispositivo en el que está instalado el Servidor de MDM para iOS.

4. En el paso **Installation packages**, defina los siguientes ajustes:

    a. En el campo **Select installation package**, seleccione el paquete de instalación del Servidor de MDM para iOS configurado.

    b. En el grupo de configuración **Force installation package download**, seleccione la casilla **Using Network Agent** para distribuir los archivos necesarios para actualizar el Servidor de MDM para iOS a través del Agente de red.

    c. En el campo **Maximum number of concurrent downloads**, ingrese el número máximo permitido de dispositivos cliente a los que el Servidor de administración podrá transmitir simultáneamente los archivos.

    d. En el campo **Maximum number of installation attempts**, especifique el número máximo de veces que se permitirá la ejecución del instalador.

    e. Especifique la siguiente configuración adicional:

    - Haga clic en la casilla **Do not re-install application if it is already installed** La aplicación no se volverá a instalar si ya se instaló en este dispositivo.

    - Haga clic en la casilla **Verify operating system type before downloading**. Antes de transmitir los archivos a los dispositivos, Kaspersky Security Center verifica si la configuración de la utilidad de Instalación puede aplicarse al sistema operativo del dispositivo. Si la configuración no es corresponde, Kaspersky Security Center no transmite los archivos y no intenta instalar la aplicación. A modo de ejemplo, si necesita instalar una aplicación en los dispositivos de un grupo de administración que contenga dispositivos con sistemas operativos diferentes, puede asignar la tarea de instalación al grupo de administración y habilitar esta opción para que la tarea no afecte a aquellos dispositivos que no tengan el sistema operativo pertinente.

5. En el siguiente paso del asistente, se le pedirá que seleccione la acción que se realizará si la instalación de la aplicación le solicita que reinicie el sistema operativo. Seleccione la opción **Do not restart the device** u omita este paso, ya que no se aplica al sistema operativo Linux.

6. En el paso **Select accounts to access devices**, seleccione la opción **No account required (Network Agent installed)**. Si selecciona esta opción, no necesitará especificar la cuenta con la que se ejecutará el instalador de la aplicación. Para ejecutar la tarea, se usará la cuenta con la que se haya iniciado el servicio del Servidor de administración. Esta opción no está disponible si el Agente de red no se instaló en los dispositivos.

7. En el paso **Finish task creation**, haga clic en el botón **Finish** para crear la tarea y cerrar el asistente.

El Servidor de MDM para iOS se actualiza mediante la tarea de instalación remota.

Para actualizar el Servidor de MDM para iOS localmente, siga los pasos descritos para la instalación local del Servidor de MDM para iOS en un dispositivo a través del paquete de instalación utilizando la versión más reciente del paquete de instalación.

Eliminar el Servidor de MDM para iOS mediante una tarea de desinstalación remota

Kaspersky Next Expert View (on-premise) le permite eliminar el Servidor de MDM para iOS de forma remota mediante una tarea de desinstalación remota.

Antes de eliminar el Servidor de MDM para iOS, asegúrese de que el paquete de instalación del Servidor de MDM para iOS se haya creado y agregado al repositorio del Servidor de administración (**Operations** > **Repositories** > **Installation packages**).

Para eliminar el Servidor de MDM para iOS, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **iOS MDM Servers**.

2. Seleccione el Servidor de MDM para iOS que desee desinstalar y, a continuación, haga clic en **Delete**.

   Se inicia el Asistente para crear una nueva tarea. Siga los pasos del asistente descritos en la Ayuda de Kaspersky Security Center.

Ver la lista de Servidores de MDM para iOS instalados y ajustar su configuración

Kaspersky Next Expert View (on-premise) le permite ver la lista de Servidores de MDM para iOS instalados y acceder a su configuración.

Para ver los Servidores de MDM para iOS instalados, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **iOS MDM Servers**.

2. En la lista de Servidores de MDM para iOS instalados que se abre:

   a. Para instalar el Servidor de MDM para iOS, haga clic en **Install**.

   b. Para actualizar el Servidor de MDM para iOS, haga clic en **Update**.

   c. Para eliminar el Servidor de MDM para iOS, haga clic en **Delete**.

   d. Para ver o configurar la configuración del Servidor de MDM para iOS, realice una de las siguientes acciones:

   - Seleccione la casilla junto al Servidor de MDM para iOS cuya configuración desea ver o modificar y, a continuación, haga clic en **Modify settings**.

     Se abre la pestaña **Application settings** de la ventana de configuración del Servidor de MDM para iOS.

   - Haga clic en el nombre del Servidor de MDM para iOS cuya configuración desea ver o modificar.

     En la ventana de configuración del Servidor de MDM para iOS que se abre, vaya a la pestaña **Application settings**.

Para ver o modificar la configuración del Servidor de MDM para iOS:

1. Vaya a la pestaña **Application settings** de la ventana de configuración del Servidor de MDM para iOS siguiendo las instrucciones anteriores.

   a. En la sección **General**, puede ver las propiedades generales del Servidor de MDM para iOS.

   - **Name**. El nombre personalizado del Servidor de MDM para iOS.
   - **Version**. La versión del Servidor de MDM para iOS instalado.
   - **Modified**. La fecha y hora de la última actualización o modificación del Servidor de MDM para iOS.
   - **Host name**. El nombre del dispositivo en el que está instalado el Servidor de MDM para iOS.
   - **Host path**. La ruta al Servidor de MDM para iOS en el dispositivo en el que está instalado.

   > No puede modificar la configuración en esta sección.

   b. En la sección **APNs proxy server**, puede especificar la siguiente configuración para Apple Push Notification Service (APNs):

   - **Address**. Dirección del servidor proxy de APNs.
   - **Port**. Puerto del servidor proxy de APNs.
   - **User name**. Nombre de usuario del proxy de APNs.
   - **Password**. Contraseña del proxy de APNs.

   > Si tiene la intención de acceder a APNs desde el servicio MDM para iOS a través de un servidor proxy, la opción **Use proxy server to connect to APNs** debe estar habilitada.

   > Para obtener información detallada sobre el servidor proxy de APNs, consulte la sección Configuración del acceso al servicio de Apple Push Notification.

   c. En la sección **Certificates**, puede administrar los certificados necesarios para el funcionamiento del Servidor de MDM para iOS.

   - **Apple Push Notification service (APNs) certificate**. El certificado de APNs está firmado por Apple y le permite usar la notificación push de Apple. A través de Apple Push Notification, un servidor de MDM para iOS puede administrar los dispositivos iOS. Para obtener información detallada sobre el certificado de APNs, consulte la sección Recibir o renovar un certificado de APNs.
   - **iOS MDM Server certificate**. El certificado del Servidor de MDM para iOS se utiliza para establecer la conexión y verificar la confianza entre los dispositivos iOS y el Servidor de MDM para iOS.

- **iOS MDM Server reserve certificate**. El certificado de reserva del Servidor de MDM para iOS garantiza un cambio sin problemas de dispositivos iOS después de que caduca el certificado principal del Servidor de MDM para iOS. Para obtener información detallada sobre el certificado de reserva del Servidor de MDM para iOS, consulte la sección Configuración de un certificado de reserva de Servidor de MDM para iOS.

- **iOS MDM Server root certificate**. Kaspersky Security Center almacena y administra el certificado raíz del Servidor de MDM para iOS. Se envía al Servidor de MDM para iOS durante la conexión a Kaspersky Security Center y se utiliza para emitir certificados móviles de Kaspersky Security Center para autenticar dispositivos MDM con iOS a través del protocolo mTLS.

d. En la sección **Connection settings**, puede ver y configurar los ajustes para la conexión del dispositivo móvil al Servidor de MDM para iOS.

- En el bloque de configuración **Synchronization**, puede habilitar o deshabilitar la sincronización de dispositivos administrados con el Servidor de MDM para iOS y especificar el **Synchronization period (min)**.

- En el bloque de configuración **Local access point**, puede especificar el **Network Agent connection port** (un puerto para conectar dispositivos iOS al Agente de red) y el **iOS MDM local connection port** (un puerto local para conectar el Agente de red al servicio MDM para iOS). Para obtener información detallada sobre estos valores, consulte la sección Configurar un paquete de instalación del Servidor de MDM para iOS.

- En el bloque de configuración **External access point**, puede especificar el **iOS MDM external connection port** (puerto externo para conectar dispositivos móviles al servicio de MDM para iOS).

- En el bloque de configuración **Device management profile**, puede configurar las propiedades del perfil de instalación. Puede especificar el **Profile name** (un campo obligatorio), la **Company** y la **Profile description**.

  Tenga en cuenta que la configuración de esta sección se aplica a los dispositivos MDM con iOS recién conectados o a los dispositivos MDM con iOS conectados anteriormente cuando se renuevan sus certificados móviles.

- En la sección **Configuration profiles**, puede ver y administrar los perfiles de configuración, que se utilizan para definir de forma centralizada la configuración de los dispositivos iOS administrados y restringir las funciones de estos dispositivos. Para obtener información detallada sobre la administración de perfiles de configuración, consulte las secciones Agregar un perfil de configuración, Instalar un perfil de configuración en un dispositivo y Eliminar un perfil de configuración de un dispositivo.

Configurar un certificado del Servidor de MDM para iOS

El certificado del Servidor de MDM para iOS se utiliza para establecer una conexión y verificar la confianza entre el dispositivo MDM con iOS y el Servidor de MDM para iOS.

Kaspersky Security Center emite el certificado del Servidor de MDM para iOS automáticamente en el momento de la implementación inicial del Servidor de MDM para iOS y se instala en un dispositivo en el que se haya implementado el Servidor de MDM para iOS. Si desea usar un certificado emitido por su autoridad de certificación, debe especificar un archivo de certificado personalizado que se usará como un certificado del Servidor de MDM para iOS.

Si especifica un certificado personalizado del Servidor de MDM para iOS, el botón **Issue** para el certificado de reserva del Servidor de MDM para iOS dejará de estar disponible. Debe especificar el certificado de reserva manualmente; para ello, haga clic en **Install**.

Para especificar un certificado personalizado de Servidor de MDM para iOS, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management → Mobile → iOS MDM Servers**. En la lista de Servidores de MDM para iOS que se abre, haga clic en el Servidor de MDM para iOS cuya configuración desea modificar.

2. En la ventana de configuración del Servidor de MDM para iOS, seleccione **Application settings**.

3. Seleccione la pestaña **Certificates**.

   a. En el bloque de configuración **iOS MDM Server certificate**, haga clic en **Install**.

   b. En la ventana del Explorador de archivos que se abre, especifique un archivo de certificado en formato PEM, PFX o P12 y, a continuación, haga clic en **Abrir**.

   Asegúrese de que el certificado que instale cumpla con los siguientes requisitos de seguridad:

   - Se especifica el nombre común (CN);
   - se especifica un nombre alternativo del sujeto (SAN) de DNS;
   - se especifica un editor de certificados;
   - se especifica una fecha de caducidad correcta del certificado;
   - la cadena de certificados está completa;
   - el uso de clave extendido (EKU) es XKU_SSL_SERVER (1.3.6.1.5.5.7.3.1 serverAuth);
   - el tamaño de la clave RSA en la cadena de certificados es de al menos 2048 bits;
   - el tamaño de la clave RSA del certificado raíz es de al menos 4096 bits;
   - el algoritmo hash en la cadena de certificados es de la familia SHA-2.

c. En la ventana **Installing certificate** que se abre, ingrese la contraseña del certificado y luego haga clic en **Install**.

d. Haga clic en **Save**.

Su certificado personalizado se especifica como el certificado del Servidor de MDM para iOS. Los detalles del certificado se muestran en el bloque de configuración **iOS MDM Server certificate**.

Si necesita renovar el certificado del Servidor de MDM para iOS, le recomendamos que utilice el certificado de reserva del Servidor de MDM para iOS sin volver a emitir el certificado principal.

Si aún desea renovar el certificado del Servidor de MDM para iOS, primero detenga las aplicaciones Kaspersky Security Center, el Agente de red y el Servidor de MDM para iOS, elimine el certificado kliosmdmserver_cert.pem y su contraseña (cadena SrvCertPwd = en el archivo kliosmdm.ini) y luego reinicie Kaspersky Security Center, el Agente de red y el Servidor de MDM para iOS. Tenga en cuenta que estas acciones provocarán la pérdida de la conexión del Servidor de MDM para iOS con los dispositivos.

Configurar un certificado de reserva del Servidor de MDM para iOS

La funcionalidad del Servidor de MDM para iOS le permite emitir un certificado de reserva. Este certificado está diseñado para su uso en perfiles de administración, para garantizar un cambio sin problemas de los dispositivos iOS administrados después de que caduque el certificado del Servidor de MDM para iOS.

Si su Servidor de MDM para iOS utiliza un certificado predeterminado emitido por Kaspersky, puede emitir un certificado de reserva (o especificar su propio certificado personalizado como reserva) antes de que caduque el certificado del Servidor de MDM para iOS. De manera predeterminada, el certificado de reserva se emite automáticamente 60 días antes de que caduque el certificado del Servidor de MDM para iOS. El certificado de reserva del Servidor de MDM para iOS se convierte en el certificado principal inmediatamente después de que caduca el certificado del Servidor de MDM para iOS. La clave pública se distribuye a todos los dispositivos administrados a través de perfiles de configuración, por lo que no tiene que transmitirla manualmente.

Tenga en cuenta que el certificado de reserva del Servidor de MDM para iOS no se emite automáticamente si utiliza un certificado personalizado del Servidor de MDM para iOS. Si utiliza un certificado personalizado, le recomendamos que especifique un certificado de reserva al instalar el Servidor de MDM para iOS, a más tardar, 30 días antes de la caducidad del certificado del Servidor de MDM para iOS existente.

Si el certificado caduca y no se especificó ninguna reserva, se perderá la conexión entre el Servidor de MDM para iOS y los dispositivos MDM con iOS. En este caso, para volver a conectar los dispositivos, debe especificar un nuevo certificado y reinstalar los perfiles de administración en cada uno de los dispositivos administrados.

Para emitir un certificado de reserva del Servidor de MDM para iOS o especificar un certificado de reserva personalizado, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management → Mobile → iOS MDM Servers**. En la lista de Servidores de MDM para iOS que se abre, haga clic en el Servidor de MDM para iOS cuya configuración desea modificar.

2. En la ventana de configuración del Servidor de MDM para iOS, seleccione **Application settings**.

3. Seleccione la pestaña **Certificates**.

4. En el bloque de configuración **iOS MDM Server reserve certificate**, realice una de las siguientes acciones:

- Si planea continuar usando un certificado autofirmado (el emitido por Kaspersky), siga estos pasos:

  a. Haga clic en **Issue**.

  > Si tiene un certificado personalizado del Servidor de MDM para iOS, el botón **Emitir** para el certificado de reserva del Servidor de MDM para iOS no estará disponible. Debe especificar el certificado de reserva manualmente; para ello, haga clic en **Install**.

  b. En la ventana **Apply iOS MDM Server reserve certificate** que se abre, seleccione una de las dos opciones para la fecha en que se debe aplicar el certificado de reserva:

  - Si desea aplicar el certificado de reserva antes de que caduque el certificado actual, seleccione la opción **After the current certificate expires**.
  - Si desea aplicar el certificado de reserva antes de que caduque el certificado actual, seleccione la opción **After specified period (days)**. En el campo de entrada junto a esta opción, especifique la duración del período después del cual el certificado de reserva debe reemplazar al certificado actual.

  > El período de validez del certificado de reserva que especifique no puede exceder el período de validez del certificado actual del Servidor de MDM para iOS.

  c. Haga clic en **OK**.

  El certificado de reserva autofirmado del Servidor de MDM para iOS se emite y se especifica como el certificado de reserva del Servidor de MDM para iOS.

  > Tenga en cuenta que cuando especifique la fecha en la que se debe aplicar el certificado de reserva, el certificado se emitirá antes de guardar los cambios en la sección **Certificates**. Si desea emitir un nuevo certificado de reserva, abra la configuración del Servidor de MDM para iOS nuevamente, elimine el certificado de reserva emitido anteriormente haciendo clic en **Delete** y emita un nuevo certificado de reserva siguiendo las instrucciones anteriores.

- Si planea utilizar un certificado personalizado emitido por su autoridad de certificación, siga estos pasos:

  a. Haga clic en **Install**.

  b. En la ventana del Explorador de archivos que se abre, especifique un archivo de certificado en formato PEM, PFX o P12 y, a continuación, haga clic en **Abrir**.

  Asegúrese de que el certificado que instale cumpla con los siguientes requisitos de seguridad:

  - se especifica un Nombre alternativo del sujeto (SAN) correcto;
  - se especifica un editor de certificado correcto;
  - se especifica una fecha de caducidad correcta del certificado;
  - la cadena de certificados está completa;
  - el uso de clave extendido (EKU) es XKU_SSL_SERVER (1.3.6.1.5.5.7.3.1 serverAuth);

- el tamaño de la clave RSA en la cadena de certificados es de al menos 2048 bits;
- el tamaño de la clave RSA del certificado raíz es de al menos 4096 bits;
- el algoritmo hash en la cadena de certificados es de la familia SHA-2.

c. En la ventana **Installing certificate** que se abre, ingrese la contraseña del certificado y luego haga clic en **Install**.

d. Haga clic en **Save**.

Su certificado personalizado se especifica como el certificado de reserva del Servidor de MDM para iOS.

Tenga en cuenta que cuando especifique la fecha en la que se debe aplicar el certificado de reserva, el certificado se emitirá antes de guardar los cambios en la sección **Certificates**. Si desea emitir un nuevo certificado de reserva, abra la configuración del Servidor de MDM para iOS nuevamente, elimine el certificado de reserva emitido anteriormente haciendo clic en **Delete** y emita un nuevo certificado de reserva siguiendo las instrucciones anteriores.

Tiene un certificado de reserva del Servidor de MDM para iOS especificado. Los detalles del certificado de reserva se muestran en el bloque de configuración **iOS MDM Server reserve certificate**.

Recibir o renovar un certificado de APNs

Para asegurar un correcto funcionamiento del servicio de MDM para iOS y las respuestas oportunas de los dispositivos móviles a los comandos del administrador, tiene que especificar un certificado del servicio de Apple Push Notification (certificado de APNs) en la configuración del Servidor de MDM para iOS.

Si ya tiene un certificado de APNs, considere renovarlo en lugar de crear uno nuevo. Cuando reemplaza el certificado de APNs existente por uno recién creado, el Servidor de administración ya no puede administrar los dispositivos MDM con iOS conectados anteriormente.

Para crear o renovar un certificado de APNs, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management → Mobile → iOS MDM Servers**. En la lista de Servidores de MDM para iOS que se abre, haga clic en el Servidor de MDM para iOS cuya configuración desea modificar.
2. En la ventana de configuración del Servidor de MDM para iOS, seleccione **Application settings**.
3. Seleccione la pestaña **Certificates**.
4. En el bloque de configuración **Apple Push Notification service (APNs) certificate**, haga clic en **Issue or renew**.

   Se abre el asistente del certificado de APNs. Haga clic en **Start** y luego avance por el asistente con los botones **Back** y **Next**.

   Cuando se crea la solicitud de firma de certificado (CSR) en el primer paso del asistente, su clave privada se almacena en la memoria RAM del dispositivo. En consecuencia, todos los pasos del asistente deben completarse sin interrupción dentro de una sola sesión.

Paso 1. Create a Certificate Signing Request (CSR)

Para crear una CSR, siga estos pasos:

a. Especifique la información requerida para generar un archivo de solicitud: **Common Name (CN)**, **Organization Name (O)**, **Organization Unit Name (OU)**, **City (L)**, **Region (S)**, **Country (C)**.

b. Haga clic en **Descargar**.

Después de guardar los cambios, se generará un archivo CSR y la clave privada del certificado se guardará en la memoria del dispositivo.

Paso 2. Sign the CSR file

En este paso, envíe el archivo CSR que recibió en el paso anterior del asistente a Kaspersky para que lo firme:

a. Haga clic en **Go to Kaspersky CompanyAccount**.

b. Envíe el archivo CSR creado a Kaspersky para que lo firme.

> Tenga en cuenta que podrá firmar el archivo CSR solo después de cargar una clave que le permita usar la solución de administración de dispositivos móviles.

c. Después de procesar su solicitud correctamente, recibirá un archivo CSR firmado por Kaspersky.

d. Guarde el archivo recibido.

Paso 3. Receive the APNs certificate public key

En este paso, realice una de las siguientes acciones si desea emitir un nuevo certificado o renovar uno existente:

Para emitir un nuevo certificado, siga estos pasos:

a. Haga clic en **Go to Apple portal**.

b. Inicie sesión en el portal de Apple con un Apple ID corporativo.

> Le recomendamos que evite usar un Apple ID personal. Cree un ID de Apple específico para usarlo como corporativo. Después de haber creado un ID de Apple, vincúlelo con el buzón de correo de la organización, no con el buzón de correo de un empleado.

c. Cargue un archivo CSR firmado.

El archivo se utilizará para generar la clave pública del certificado de APNs.

d. Después de que Apple procesa su CSR, recibirá la clave pública del certificado de APNs.

Guarde el archivo recibido.

Para renovar un certificado, haga lo siguiente:

a. Haga clic en **Go to Apple portal**.

b. Inicie sesión en el portal de Apple con un Apple ID corporativo.

> Le recomendamos que evite usar un Apple ID personal. Cree un ID de Apple específico para usarlo como corporativo. Después de haber creado un ID de Apple, vincúlelo con el buzón de correo de la organización, no con el buzón de correo de un empleado.

c. Especifique el certificado que desea renovar.

d. Cargue un archivo CSR firmado.

El archivo se utilizará para generar la clave pública del certificado de APNs.

e. Después de que Apple procesa su CSR, recibirá la clave pública del certificado de APNs.

Guarde el archivo recibido.

Paso 4. Specify the APNs certificate public key

En este paso, cargue el archivo de clave pública recibido de Apple en el paso anterior del asistente:

a. Haga clic en **Select**.

b. En la ventana del Explorador de archivos que se abre, especifique un archivo de certificado en formato PEM, PFX o P12 y, a continuación, haga clic en **Abrir**.

Paso 5. Specify the APNs certificate private key password

En este paso, ingrese el nombre del certificado y la contraseña de la clave privada:

a. En el campo **Certificate name**, especifique un nombre personalizado para el certificado.

b. En el campo **Private key password**, especifique la contraseña de la clave privada para el certificado.

Esta contraseña se utilizará para instalar el certificado de APNs en el Servidor de MDM para iOS.

c. En **Confirm password**, ingrese la contraseña nuevamente.

Paso 6. Complete the CSR

En este paso, el certificado de APNs se genera y está listo para instalarse en el Servidor de MDM para iOS.

a. Para completar la CSR, haga clic en **Download APNs certificate** para guardar el certificado creado.

b. Haga clic en **Listo** para salir del asistente.

Las claves privada y pública del certificado se combinan, y el certificado de APNs se guarda en formato PEM.

Ahora puede instalar el certificado de APNs en el Servidor de MDM para iOS.

Instalar un certificado de APNs en el Servidor de MDM para iOS

Una vez recibido el certificado de APNs, puede instalarlo en el Servidor de MDM para iOS.

Para instalar el certificado de APNs en el Servidor de MDM para iOS, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **iOS MDM Servers**. En la lista de Servidores de MDM para iOS que se abre, haga clic en el Servidor de MDM para iOS cuya configuración desea modificar.

2. En la ventana de configuración del Servidor de MDM para iOS, seleccione **Application settings**.

3. Seleccione la pestaña **Certificates**.

4. En el bloque de configuración **Apple Push Notification service (APNs) certificate**:

   a. Haga clic en **Install**.

   b. En la ventana del Explorador de archivos que se abre, especifique un archivo de certificado en formato PEM y luego haga clic en **Abrir**.

   Asegúrese de que el certificado que instale cumpla con los siguientes requisitos de seguridad:

   - Se especifica el nombre común (CN);
   - se especifica un tema de APNs;
   - se especifica un editor de certificados;
   - se especifica una fecha de caducidad correcta del certificado.

   c. En la ventana **Installing certificate** que se abre, ingrese la contraseña de la clave privada especificada al recibir el certificado de APNs y luego haga clic en **Install**.

El certificado de APNs se instalará en el Servidor de MDM para iOS. Los detalles del certificado se mostrarán en el bloque de configuración **Apple Push Notification service (APNs) certificate**.

Configuración del acceso al servicio de Apple Push Notification

Para asegurar un correcto funcionamiento del servicio de MDM para iOS y las respuestas oportunas de los dispositivos móviles a los comandos del administrador, tiene que especificar un certificado de Apple Push Notification Service (Certificado de APNs) en la configuración del Servidor de MDM para iOS.

Al interactuar con el servicio de Apple Push Notification (APNs), el servicio de MDM para iOS se conecta a la dirección externa api.push.apple.com a través del puerto 2197 (saliente). Por lo tanto, el servicio de MDM para iOS requiere acceso al puerto TCP 2197 para el rango de direcciones 17.0.0.0/8. Desde el dispositivo iOS, esta interacción requiere acceso al puerto TCP 5223 para el rango de direcciones 17.0.0.0/8.

Si tiene la intención de acceder a las APNs desde el servicio de MDM para iOS a través de un servidor proxy, debe habilitar el uso de un servidor proxy para conectarse a las APNs.

Para habilitar el uso de un servidor proxy para conectarse a las APNs, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management → Mobile → iOS MDM Servers**. En la lista de Servidores de MDM para iOS que se abre, haga clic en el Servidor de MDM para iOS cuya configuración desea modificar.
2. En la ventana de configuración del Servidor de MDM para iOS, seleccione **Application settings**.
3. Seleccione la pestaña **APNs proxy server**.
4. En la ventana que se abre, habilite el interruptor **Use proxy server to connect to APNs**.
5. Especifique la siguiente configuración:
   a. En el campo **Address**, especifique la dirección del servidor proxy de APNs.
   b. En el campo **Port**, especifique el puerto del servidor proxy de APNs.
   c. En el campo **User name**, especifique el nombre de usuario del proxy de APNs.
   d. En el campo **Password**, especifique la contraseña del proxy de APNs.
6. Haga clic en **Save**.

El servidor proxy ahora se usa para conectarse a las APNs.

Eventos del Servidor de MDM para iOS

Kaspersky Next Expert View (on-premise) le permite ver los eventos relacionados con el Servidor de MDM para iOS. Los eventos tienen diferentes niveles de gravedad: *Información*, *Advertencia*, *Crítico*, *Error funcional*.

Para cada evento que pueda generar el Servidor de MDM para iOS, puede especificar la configuración de notificación y almacenamiento en la pestaña **Event configuration** de la configuración del Servidor de MDM para iOS. Recomendamos que ajuste la configuración para cada tipo de evento después de implementar el Servidor de MDM para iOS para limitar el número de eventos que se muestra y reducir el tiempo de carga de la lista de eventos.

Si desea ajustar la configuración de notificación para todos los eventos a la vez, ajuste la configuración de notificación general en las propiedades del Servidor de administración. Para obtener información detallada sobre las notificaciones, consulte la Ayuda de Kaspersky Security Center.

Para ver los eventos del Servidor de MDM para iOS, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management → Mobile → iOS MDM Servers**. En la lista de Servidores de MDM para iOS que se abre, haga clic en el Servidor de MDM para iOS cuyos eventos desea ver.
2. En la ventana de configuración del Servidor de MDM para iOS, seleccione **Application settings**.
3. Seleccione la pestaña **Eventos**.

Se muestran los eventos del Servidor de MDM para iOS.

Para obtener información detallada sobre cómo ver eventos en Kaspersky Next Expert View (on-premise), consulte la Ayuda de Kaspersky Security Center.

La siguiente tabla muestra los eventos del servidor de MDM para iOS de Kaspersky Security Center que tienen el nivel de gravedad *Información*.

Eventos informativos del Servidor de MDM para iOS

Nombre que se muestra para el tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Información general sobre el dispositivo móvil solicitada	DEVICEINFORMATION_COMMAND_SUCCESSFUL	30 días
Información de seguridad solicitada	SECURITYINFO_COMMAND_SUCCESSFUL	30 días
Nuevo dispositivo móvil conectado	NEW_DEVICE_CONNECTED	30 días
Lista de perfiles solicitados	PROFILELIST_COMMAND_SUCCESSFUL	30 días
Perfil instalado	INSTALLPROFILE_COMMAND_SUCCESSFUL	30 días
Perfil eliminado	REMOVEPROFILE_COMMAND_SUCCESSFUL	30 días
Lista de perfiles de aprovisionamiento solicitados	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFUL	30 días
Perfil de aprovisionamiento instalado	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFUL	30 días
Perfil de aprovisionamiento eliminado	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFUL	30 días
Lista de certificados instalados solicitados	CERTIFICATELIST_COMMAND_SUCCESSFUL	30 días
Lista de aplicaciones instaladas solicitadas	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFUL	30 días
Lista de aplicaciones administradas solicitadas	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFUL	30 días
Instalación de la aplicación solicitada	INSTALLAPPLICATION_COMMAND_SUCCESSFUL	30 días
Se aplicó la configuración de la app	APPCONFIG_APPLIED_SUCCESSFUL	30 días
Aplicación administrada eliminada	REMOVEAPPLICATION_COMMAND_SUCCESSFUL	30 días
Código de canje de la aplicación establecido	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFUL	30 días
Dispositivo móvil bloqueado	DEVICELOCK_COMMAND_SUCCESSFUL	30 días
Restablecimiento de contraseña	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 días
Datos del dispositivo móvil borrados	ERASEDEVICE_COMMAND_SUCCESSFUL	30 días
Actualización del sistema operativo programada	SCHEDULEOSUPDATE_COMMAND_SUCCESSFULL	30 días
Configuración de itinerancia aplicada	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 días
Configuración de Bluetooth aplicada	SETBLUETOOTHSETTINGS_COMMAND_SUCCESSFUL	30 días
Modo perdido habilitado	ENABLE_LOST_MODE_COMMAND_SUCCESSFUL	30 días
Sonido reproducido en Modo perdido	PLAY_LOST_MODE_SOUND_COMMAND_SUCCESSFUL	30 días
Ubicación de dispositivo móvil recibida	GET_DEVICE_LOCATION_COMMAND_SUCCESSFUL	30 días
Modo perdido deshabilitado	DISABLE_LOST_MODE_COMMAND_SUCCESFUL	30 días
Código de omisión de bloqueo de activación recibido	GET_ACTIVATION_LOCK_BYPASS_CODE_COMMAND_SUCCESSFUL	30 días
Verificación de control de cumplimiento iniciada	COMPLIANCE_CONTROL_CHEKING_RULES_STARTED	30 días
Comprobación de Control de cumplimiento completada	COMPLIANCE_CONTROL_CHEKING_RULES_COMPLETED	30 días

Nombre que se muestra para el tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Respuesta de Control de cumplimiento iniciada	COMPLIANCE_CONTROL_ACTION_STARTED	30 días
Respuesta de Control de cumplimiento completada	COMPLIANCE_CONTROL_ACTION_COMPLETED	30 días

En la siguiente tabla se muestran los eventos del Servidor de MDM para iOS que tienen el nivel de gravedad *Advertencia*.

Eventos de advertencia del servidor de MDM para iOS

Nombre que se muestra para el tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Se detectó un intento de conectar el dispositivo móvil bloqueado	INACTICE_DEVICE_TRY_CONNECTED	30 días
Perfil de administración eliminado	MDM_PROFILE_WAS_REMOVED	30 días
Se detectó un intento de reutilizar el certificado de usuario	CLIENT_CERT_ALREADY_IN_USE	30 días
Se detectó un incumplimiento del criterio de Control de cumplimiento	COMPLIANCE_CONTROL_CONDITIONS_MATCH_DETECTED	30 días
No se pudo realizar una respuesta de Control de cumplimiento	COMPLIANCE_CONTROL_ACTION_FAILED	30 días
Se detectó un dispositivo móvil inactivo	FOUND_INACTIVE_DEVICE	30 días
Se requiere el código de canje	NEED_REDEMPTION_CODE	30 días
Perfil de administración eliminado del dispositivo móvil	UMDM_PROFILE_WAS_REMOVED	30 días

La siguiente tabla muestra los eventos del Servidor de MDM para iOS que tienen el nivel de gravedad *Error funcional*.

Eventos de errores funcionales del Servidor de MDM para iOS

Nombre que se muestra para el tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Error al solicitar información general sobre el dispositivo móvil	DEVICEINFORMATION_COMMAND_FAILED	30 días
Error al solicitar la información de seguridad	SECURITYINFO_COMMAND_FAILED	30 días
Error al solicitar la lista de perfiles	PROFILELIST_COMMAND_FAILED	30 días
Error al instalar el perfil	INSTALLPROFILE_COMMAND_FAILED	30 días
Error al eliminar el perfil	REMOVEPROFILE_COMMAND_FAILED	30 días
Error al solicitar la lista de perfiles de aprovisionamiento	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 días
Error al instalar perfil de aprovisionamiento	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 días
Error al eliminar el perfil de aprovisionamiento	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 días
Error al solicitar la lista de certificados instalados	CERTIFICATELIST_COMMAND_FAILED	30 días
Error al solicitar la lista de aplicaciones instaladas	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 días
Error al solicitar la lista de aplicaciones administradas	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 días
Error al solicitar la instalación de la aplicación	INSTALLAPPLICATION_COMMAND_FAILED	30 días

Nombre que se muestra para el tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Error al aplicar la configuración de la aplicación	APPCONFIG_APPLIED_FAILED	30 días
Error al eliminar la aplicación administrada	REMOVEAPPLICATION_COMMAND_FAILED	30 días
Error al establecer el código de canje de la aplicación	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 días
Error al bloquear el dispositivo móvil	DEVICELOCK_COMMAND_FAILED	30 días
No se pudo restablecer la contraseña	CLEARPASSCODE_COMMAND_FAILED	30 días
Error al eliminar los datos del dispositivo móvil	ERASEDEVICE_COMMAND_FAILED	30 días
Error al programar la actualización del sistema operativo	SCHEDULEOSUPDATE_COMMAND_FAILED	30 días
Error al aplicar la configuración de itinerancia	SETROAMINGSETTINGS_COMMAND_FAILED	30 días
Error al aplicar la configuración de Bluetooth	SETBLUETOOTHSETTINGS_COMMAND_FAILED	30 días
Error al habilitar el Modo perdido	ENABLE_LOST_MODE_COMMAND_FAILED	30 días
Error al reproducir sonido en el Modo perdido	PLAY_LOST_MODE_SOUND_COMMAND_FAILED	30 días
Error al recibir la ubicación del dispositivo móvil	GET_DEVICE_LOCATION_COMMAND_FAILED	30 días
Error al deshabilitar el Modo perdido	DISABLE_LOST_MODE_COMMAND_FAILED	30 días
Error al recibir el código de omisión para el bloqueo de activación	GET_ACTIVATION_LOCK_BYPASS_CODE_COMMAND_FAILED	30 días
Error en el funcionamiento de la aplicación	PRODUCT_FAILURE	30 días
El resultado del comando contiene datos incorrectos	MALFORMED_COMMAND	30 días
No se pudo enviar el mensaje	SEND_PUSH_NOTIFICATION_FAILED	30 días
Error al enviar el comando (Control de cumplimiento)	SEND_COMMAND_FAILED	30 días
Error al buscar el dispositivo	DEVICE_NOT_FOUND	30 días
Error al configurar Per App VPN para la aplicación	PERAPP_VPN_SETUP_FAILED	30 días

Obtener datos de diagnóstico del Servidor de MDM para iOS

Cuando crea una solicitud para el Servicio de soporte técnico de Kaspersky, es posible que se le solicite que cree y adjunte un archivo de seguimiento. El Servicio de soporte técnico utiliza los archivos de seguimiento con fines de diagnóstico. Contienen todos los pasos de ejecución del comando de la aplicación escritos en el archivo, lo que permite detectar el paso en el que se produce un error.

Le recomendamos que obtenga los seguimientos del Servidor de MDM para iOS junto con los seguimientos del Agente de red, ya que contienen los detalles del conector del Servidor de MDM para iOS.

Hay varios niveles de seguimiento para el Servidor de MDM para iOS:

- 0: CRÍTICO
- 1: ERROR

- 2: MENSAJE
- 3: DEPURACIÓN

Pregunte a un ingeniero de soporte qué nivel de seguimiento debe establecer. Si el ingeniero de Servicio de soporte técnico no especificó el nivel de seguimiento, recomendamos obtener seguimientos de nivel 2.

Para habilitar el seguimiento del Servidor de MDM para iOS y crear archivos de seguimiento, siga estos pasos:

1. Abra el archivo de configuración del Servidor de MDM para iOS `/var/opt/kaspersky/iosmdm/settings.ini`.
2. Especifique los valores necesarios para habilitar el seguimiento. Le recomendamos que especifique los siguientes valores predeterminados:
   - *LogCommEnabled*=1

     Habilitar o deshabilitar el seguimiento del Servidor de MDM para iOS y la biblioteca de comunicaciones del conector.
   - *LogSettingsEnabled*=1

     Habilitar o deshabilitar el seguimiento del Servidor de MDM para iOS y la biblioteca de configuración del conector.
   - *LogCommVerboseLevel*=2

     El nivel de seguimiento del Servidor de MDM para iOS y la biblioteca de comunicaciones del conector.
   - *LogSettingsVerboseLevel*=2

     El nivel de seguimiento del Servidor de MDM para iOS y la biblioteca de configuración del conector.
   - *LogVerboseLevel*=2

     El nivel de seguimiento del Servidor de MDM para iOS.
   - *LogFolder*=/var/opt/kaspersky/iosmdm

     El directorio para escribir archivos de seguimiento.
3. Reinicie el Servidor de MDM para iOS y los servicios del Agente de red mediante los siguientes comandos:

   ```
   systemctl restart klnagent
   systemctl restart kliosmdm
   ```

El seguimiento del Servidor de MDM para iOS está habilitado. Los archivos de seguimiento se crean en el directorio que especificó como valor de *LogFolder*: *klcon_comm.log*, *klcon_settings.log*, *klsrv.log*, *klsrv_comm.log*, *klsrv_settings.log*.

Para deshabilitar el seguimiento del Servidor de MDM para iOS, siga estos pasos:

1. Abra el archivo de configuración del Servidor de MDM para iOS `/var/opt/kaspersky/iosmdm/settings.ini`.
2. Modifique el archivo eliminando las cadenas que se crearon para habilitar el seguimiento:
   - *LogCommEnabled*=1
   - *LogSettingsEnabled*=1
   - *LogCommVerboseLevel*=2
   - *LogSettingsVerboseLevel*=2
   - *LogVerboseLevel*=2
   - *LogFolder*=/var/opt/kaspersky/iosmdm
3. Reinicie el Servidor de MDM para iOS y los servicios del Agente de red mediante los siguientes comandos:

   ```
   systemctl restart klnagent
   systemctl restart kliosmdm
   ```

El seguimiento del Servidor de MDM para iOS está deshabilitado.

Implementar un sistema de administración de dispositivos Android

MDM básico en Kaspersky Next Expert View (on-premise) le permite administrar dispositivos móviles con Android. En esta sección se describe la implementación de un sistema de administración de dispositivos Android.

Acerca de los modos de funcionamiento del dispositivo Android

El modo de funcionamiento del dispositivo depende del propietario del dispositivo móvil (personal o corporativo) y los requisitos corporativos de seguridad. Puede elegir el modo de funcionamiento que sea más conveniente para la empresa y usar varios modos al mismo tiempo.

Los siguientes modos de funcionamiento del dispositivo están disponibles para dispositivos Android:

- Dispositivo personal
- Dispositivo con contenedor corporativo
- Dispositivo corporativo

Dispositivo personal

Dispositivo personal es el modo de funcionamiento del dispositivo para dispositivos Android personales. Este modo de funcionamiento le permite brindar protección y realizar una administración básica de dispositivos.

Dispositivo con contenedor corporativo

Dispositivo con contenedor corporativo es el modo de funcionamiento del dispositivo para dispositivos Android personales con un perfil de trabajo de Android, que proporciona un entorno corporativo aislado en un dispositivo.

Este modo de funcionamiento le permite administrar aplicaciones y cuentas de usuario en un entorno seguro en un dispositivo sin restringir el uso de datos personales por parte del usuario. Cuando se crea un perfil de trabajo en el dispositivo móvil del usuario, se instalan las siguientes aplicaciones corporativas automáticamente en el contenedor (si corresponde): Google Play Market, Google Chrome, Descargas, Kaspersky Endpoint Security para Android y otros. Las aplicaciones corporativas instaladas en el perfil de trabajo y sus notificaciones se marcan con un ícono de maletín azul. Las aplicaciones instaladas en el perfil de trabajo aparecen en la lista común de aplicaciones.

Dispositivo corporativo

Dispositivo corporativo es el dispositivo es el modo de funcionamiento del dispositivo para los dispositivos Android propiedad de la empresa. Este modo de funcionamiento le permite tener control total sobre todo el dispositivo y configurar un conjunto extendido de configuraciones y funciones de seguridad:

- Restricciones en las funciones de Android
- Administración de la configuración de Google Chrome
- Instalación silenciosa de aplicaciones requeridas y eliminación de aplicaciones bloqueadas en Control de aplicaciones
- Modo de quiosco
- Administración de Exchange ActiveSync
- Integración de NDES y SCEP

Usar Firebase Cloud Messaging

Para garantizar que los comandos se entreguen a los dispositivos Android en tiempo y forma, Kaspersky Security Center utiliza el mecanismo de notificaciones push. Los dispositivos Android y el Servidor de administración intercambian notificaciones push a través de Firebase Cloud Messaging (en adelante, FCM). En Kaspersky Next Expert View (on-premise), puede especificar la configuración de Firebase Cloud Messaging para conectar los dispositivos Android al servicio.

Para obtener los ajustes de Firebase Cloud Messaging, debe tener una cuenta de Google.

Para habilitar el uso de FCM:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.
2. Abra el menú de 3 puntos (⋮) y seleccione **Forced Android device synchronization**.
3. En el campo **Firebase project number**, ingrese el id. del remitente de FCM.
4. En el campo **Private key**, seleccione el archivo de clave privada.

   En la siguiente sincronización con el Servidor de administración, los dispositivos Android se conectarán a Firebase Cloud Messaging.

Cuando se cambia a otro proyecto de Firebase, se debe esperar 10 minutos para que FCM reanude su ejecución.

El servicio de FCM opera en los siguientes intervalos de direcciones:

- Del lado del dispositivo Android, se requiere acceso a los puertos 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) y 5230 (HTTPS) de las siguientes direcciones:
  - google.com
  - fcm.googleapis.com
  - oauth2.googleapis.com
  - android.apis.google.com
  - Todas las direcciones IP incluidas en el ASN 15169, perteneciente a Google
- Del lado del Servidor de administración, se requiere acceso al puerto 443 (HTTPS) de las siguientes direcciones:
  - fcm.googleapis.com
  - Todas las direcciones IP incluidas en el ASN 15169, perteneciente a Google

Si se especificó la configuración del servidor proxy en las propiedades del Servidor de administración en Kaspersky Next Expert View (on-premise), se utilizará para la interacción con FCM.

Configuración de FCM: obtener el id. del remitente y el archivo de clave privada

Para configurar FCM:

1. Regístrese en el Portal de Google.
2. Vaya a la consola de Firebase.
3. Realice una de las siguientes acciones:
   - Para crear un proyecto nuevo, haga clic en **Crear un proyecto** y siga las instrucciones en pantalla.
   - Abra un proyecto existente.
4. Haga clic en el ícono de ajustes y seleccione **Configuración del proyecto**.
   Se abre la ventana **Configuración del proyecto**.
5. Seleccione la pestaña **Mensajería en la nube**.
6. Obtenga el Id. del remitente correspondiente del campo **Id. del remitente** en la sección **API de Firebase Cloud Messaging (V1)**.
7. Seleccione la pestaña **Cuentas de servicio** y haga clic en **Generar nueva clave privada**.
8. En la ventana que se abre, haga clic en **Generar clave** para generar y descargar un archivo de clave privada.

Firebase Cloud Messaging queda configurado.

Implementar Kaspersky Endpoint Security para Android

Esta sección contiene una descripción general de Kaspersky Endpoint Security para Android y los métodos para instalar, actualizar y eliminar la aplicación.

Para obtener información detallada sobre Kaspersky Endpoint Security para Android, consulte la sección Uso de la aplicación Kaspersky Endpoint Security para Android.

Acerca de la aplicación Kaspersky Endpoint Security para Android

La aplicación Kaspersky Endpoint Security para Android garantiza la protección de dispositivos móviles contra amenazas web, virus y otros programas que suponen amenazas.

La aplicación Kaspersky Endpoint Security para Android incluye las siguientes características:

- **Antimalware**. Este componente detecta y neutraliza amenazas en el dispositivo mediante las bases de datos antimalware y el servicio en la nube de Kaspersky Security Network. Antimalware incluye los siguientes componentes:
  - **Protección**. Detecta amenazas en archivos abiertos, analiza aplicaciones nuevas y evita la infección del dispositivo en tiempo real.
  - **Análisis**. Se inicia a petición para el sistema de archivos completo, solo para aplicaciones instaladas o solo para un archivo o una carpeta seleccionados.
  - **Actualizar**. Le permite descargar nuevas bases de datos antimalware para la aplicación.
- **Antirrobo**. Este componente protege la información del dispositivo para impedir el acceso no autorizado en caso de pérdida o robo del dispositivo. Este componente le permite enviar los siguientes comandos al dispositivo:
  - **Locate device**. Le permite obtener las coordenadas de la ubicación del dispositivo.
  - **Sound alarm**. Provoca que el dispositivo emita un sonido de alarma fuerte.
  - **Wipe corporate data**. Borre los datos corporativos para proteger la información confidencial de la empresa.
- **Protección web** y **Control web**. Protección web bloquea los sitios web maliciosos diseñados para propagar código malicioso. Protección web también bloquea sitios web falsos (phishing) diseñados para robar datos confidenciales del usuario (por ejemplo, contraseñas de servicios bancarios en línea o sistemas de dinero electrónico) y acceder a la información financiera del usuario. Protección web usa el servicio en la nube de Kaspersky Security Network para analizar sitios web antes de que el usuario los abra. Tras el análisis, Protección Web permite que se carguen los sitios web de confianza y bloquea los que son maliciosos. Control web también admite la filtración de los sitios web según las categorías definidas en el servicio en la nube de Kaspersky Security Network. Esto permite que el administrador restrinja el acceso de usuarios a determinadas categorías de páginas web (por ejemplo, juegos de azar, loterías, sorteos o comunicación por Internet).
- **Control de apps**. Este componente le permite instalar aplicaciones recomendadas y requeridas en un dispositivo Android, así como eliminar aplicaciones bloqueadas que infringen los requisitos de seguridad corporativa.
- **Control de cumplimiento**. Este componente le permite comprobar si los dispositivos administrados cumplen con los requisitos de seguridad corporativa e imponer restricciones a ciertas funciones en los dispositivos que no los cumplan.

Puede configurar los componentes de la aplicación Kaspersky Endpoint Security para Android en Kaspersky Next Expert View (on-premise) al definir la configuración de la directiva correspondiente.

Instalación de Kaspersky Endpoint Security para Android

Existen varios métodos para implementar la aplicación Kaspersky Endpoint Security para Android. Puede usar el escenario de instalación más adecuado para su empresa o combinar varios escenarios de instalación.

Los métodos de instalación incluyen los siguientes:

- Instalación a través de Kaspersky Security Center mediante una de las fuentes de instalación:
  - **Sitio web de Kaspersky** (para todos los modos de funcionamiento)

    Elija este método para dispositivos móviles que pueden acceder a Internet para descargar el archivo de instalación APK desde el sitio web de Kaspersky. Luego, la aplicación se actualizará desde el sitio web de Kaspersky o desde HUAWEI AppGallery, Samsung Galaxy Store, RuStore o Xiaomi GetApps.

  - **Paquete de instalación** (para todos los modos de funcionamiento)

    El paquete de instalación de Kaspersky Endpoint Security para Android se descargará del servidor de Kaspersky Security Center y se actualizará a través de Kaspersky Security Center mediante la configuración de la directiva. Puede elegir este método si los dispositivos móviles de su empresa no tienen acceso a Internet.

    Para esta fuente de instalación, antes de conectar dispositivos móviles, cree el paquete de instalación de Kaspersky Endpoint Security para Android.
- Instalación manual

Crear el paquete de instalación de Kaspersky Endpoint Security para Android

La aplicación Kaspersky Endpoint Security para Android se puede implementar con el paquete de instalación.

Puede utilizar este método de instalación si los dispositivos móviles de su empresa no tienen acceso a Internet.

Para este método de instalación, debe crear un paquete de instalación de Kaspersky Endpoint Security para Android antes de conectar los dispositivos Android a Kaspersky Security Center. El paquete de instalación se descargará de Kaspersky Security Center y se actualizará a través de Kaspersky Security Center utilizando la configuración de la directiva.

El paquete de instalación de Kaspersky Endpoint Security para Android es un archivo que contiene los archivos necesarios para instalar la aplicación Kaspersky Endpoint Security para Android:

- `installer.ini`

  Archivo de configuración que contiene los ajustes de la conexión del Servidor de administración.

- `kesandroid<version>_<languages>_Prod_Release.apk`

  Archivo de paquete de Android de la aplicación Kaspersky Endpoint Security para Android.

- `ksm.kpd`

  Archivo de descripción de la aplicación.

- `eula/`

  Carpeta con Contratos de licencia de usuario final en diferentes idiomas en formato TXT.

- `kpd.loc/`

  Archivos INI que especifican las rutas a los Contratos de licencia de usuario final.

Para crear el paquete de instalación de Kaspersky Endpoint Security para Android:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Operations** → **Repositories** → **Installation packages**.

2. En la lista de paquetes de instalación que se abre, haga clic en **Add**. Se inicia el Asistente para nuevo paquete. Siga las instrucciones del asistente que se describen en la Ayuda de Kaspersky Security Center para crear un paquete de instalación a partir de un archivo o crear un paquete de instalación independiente.

Para configurar el paquete de instalación de Kaspersky Endpoint Security para Android:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Operations** → **Repositories** → **Installation packages**.

2. En la lista de paquetes de instalación que se abre, haga clic en el paquete de instalación de Kaspersky Endpoint Security para Android que desee configurar.

3. En la ventana de propiedades del paquete de instalación, seleccione la pestaña **Configuración**.

   a. En el grupo de configuración **Conexión al Servidor de administración**, configure los siguientes valores:

      - **Dirección del servidor**. Especifique la dirección del servidor al que se conectarán los dispositivos Android.

      - **Puerto SSL para la sincronización de dispositivos**. Especifique el número del puerto abierto en el Servidor de administración para conectar dispositivos móviles. El puerto 13292 se utiliza de forma predeterminada.

   b. Para los paquetes de instalación independientes, en el campo **Nombre de subgrupo** del grupo de configuración **Subgrupo en dispositivos no asignados**, especifique el nombre del grupo al que se agregarán los dispositivos Android después de la primera sincronización con el Servidor de administración. Se utiliza KES10 de manera predeterminada.

   c. En el grupo de configuración **Acciones durante la instalación en el dispositivo**, haga clic en la casilla **Solicitar al usuario la dirección de correo electrónico** si desea que Kaspersky Endpoint Security para Android solicite a los usuarios que proporcionen su dirección de correo electrónico corporativa cuando la aplicación se inicie por primera vez.

      La dirección de correo electrónico del usuario se emplea para asignar un nombre al dispositivo móvil cuando se agrega al grupo de administración.

4. Haga clic en **Guardar**.

Se configura el paquete de instalación de Kaspersky Endpoint Security para Android.

Instalación manual de Kaspersky Endpoint Security para Android

Puede instalar Kaspersky Endpoint Security para Android manualmente desde el sitio web de Kaspersky, HUAWEI AppGallery, Samsung Galaxy Store, RuStore o Xiaomi GetApps.

Instalar la aplicación

Para instalar la aplicación desde una tienda de aplicaciones, siga el procedimiento de instalación estándar para la plataforma Android.

Para instalar Kaspersky Endpoint Security para Android desde el sitio web de Kaspersky:

1. Vaya al sitio web de Kaspersky.
2. Busque Kaspersky Security para dispositivos móviles en el sitio web.
3. Toque **Mostrar descargas**.
4. Seleccione una versión de la aplicación y toque **Descargar**.
5. Abra el archivo APK descargado y siga las instrucciones en pantalla.

   Es posible que deba permitir que su navegador instale aplicaciones de fuentes que no sean Google Play en la sección **Aplicaciones → Acceso especial a aplicaciones → Instalar aplicaciones desconocidas** en la configuración del dispositivo. La ubicación de esta configuración puede diferir en dispositivos de diferentes proveedores.

La aplicación se instalará en el dispositivo.

Configuración de la aplicación

Después de instalar Kaspersky Endpoint Security para Android, debe configurar la aplicación manualmente. El procedimiento de configuración depende de si el administrador le envió una dirección de servidor o un vínculo para descargar la aplicación.

Si desea configurar Kaspersky Endpoint Security para Android mediante un vínculo de descarga para la aplicación:

1. Abra Kaspersky Endpoint Security para Android.
2. Lea el contrato de licencia de usuario final. Si acepta el contrato de licencia de usuario final, seleccione la casilla correspondiente y toque **Continue**.
3. Toque **Continue** y otorgue a la aplicación los permisos requeridos.
4. En el campo **Server**, especifique el vínculo que recibió del administrador.
5. Toque **Continue**.

Kaspersky Endpoint Security para Android se configuró.

Para configurar Kaspersky Endpoint Security para Android mediante una dirección de servidor:

1. Abra Kaspersky Endpoint Security para Android.
2. Lea el contrato de licencia de usuario final. Si acepta el contrato de licencia de usuario final, seleccione la casilla correspondiente y toque **Continue**.
3. Toque **Continue** y otorgue a la aplicación los permisos requeridos.
4. En el campo **Server**, especifique la dirección del servidor de administración que le proporcionó el administrador.
5. Toque **Continue**.

6. Toque **Enable** para habilitar la aplicación como administrador del dispositivo.

7. Toque **Allow** y otorgue a la aplicación los permisos requeridos.

Kaspersky Endpoint Security para Android se configuró.

El acceso a Internet debe estar habilitado en el dispositivo móvil para que se realice la sincronización con el servidor de administración.

Permisos para Kaspersky Endpoint Security para Android

Para todas las funciones de las aplicaciones, Kaspersky Endpoint Security para Android solicita al usuario una lista de permisos. Kaspersky Endpoint Security para Android solicita permisos obligatorios mientras completa el Asistente de instalación, así como después de la instalación y antes de usar las funciones individuales de las aplicaciones. Es imposible instalar Kaspersky Endpoint Security para Android sin proporcionar los permisos obligatorios.

En ciertos dispositivos (por ejemplo, HUAWEI, Meizu y Xiaomi), debe agregar manualmente Kaspersky Endpoint Security para Android a la lista de aplicaciones que se inician cuando el sistema operativo se inicia en la configuración del dispositivo. Si la aplicación no se agrega a la lista, Kaspersky Endpoint Security para Android deja de realizar todas sus funciones después de que el dispositivo móvil se reinicia.

En dispositivos con Android 11 o posterior o Android 6 a 10 con servicios de Google Play, debe deshabilitar la configuración del sistema **Eliminar permisos si no se usa la aplicación**. De lo contrario, cuando la aplicación no se utiliza durante unos meses, el sistema restablece automáticamente los permisos que el usuario otorgó a la aplicación.

Permisos solicitados por Kaspersky Endpoint Security para Android

Permiso	Función de la aplicación
Teléfono (lea el estado y la identidad del teléfono)	Identifique el dispositivo mediante su IMEI (para Android 5 a 9; para Android 10 o posterior en el modo de funcionamiento del dispositivo corporativo; para Android 10 a 11 para el dispositivo con modo de funcionamiento de contenedor corporativo)
	Control de cumplimiento: compruebe si la tarjeta SIM del dispositivo se reemplazó o eliminó
Almacenamiento (obligatorio)	Antimalware
Acceso para administrar todos los archivos (para Android 11 o versiones posteriores)	Antimalware
Dispositivos cercanos (para Android 12 o posterior)	Restricción del uso de Bluetooth En algunos dispositivos Xiaomi y HUAWEI con Android 12, Kaspersky Endpoint Security para Android no solicita al usuario el permiso **Dispositivos Bluetooth cercanos**. Este problema es causado por características específicas del firmware MIUI en Xiaomi y del firmware EMUI en HUAWEI. A pesar de la ausencia de la solicitud de este permiso, todas las funciones relacionadas con el uso de Bluetooth funcionan correctamente en estos dispositivos.
Ignorar la optimización de la batería (para Android 12 o posterior)	Control de apps
	Protección web
	Antirrobo
Notificaciones (para Android 13)	Notifica al usuario sobre problemas de seguridad y eventos de la app

Permiso	Función de la aplicación
Permitir la ejecución en segundo plano (para Android 12 o versiones posteriores)	Asegura el funcionamiento continuo de la app. Si no se concede permiso, es posible que la app se descargue de la memoria y no pueda reiniciar.
Administrador del dispositivo (obligatorio)	Antirrobo: bloqueo del dispositivo (solo para Android 5 a 6)
	Antirrobo: tomar una foto de identificación con la cámara frontal
	Antirrobo: hacer sonar la alarma
	Antirrobo: reinicio completo
	Protección con contraseña
	Protección de eliminación de aplicaciones
	Instalación de certificado de seguridad
	Control de apps
	Administración de Knox (solo para dispositivos Samsung)
	Configuración de Wi-Fi
	Configuración de Exchange ActiveSync
	Restricción del uso de la cámara, Bluetooth y Wi-Fi
Cámara	Antirrobo: tomar una foto de identificación con la cámara frontal En los dispositivos con Android 11 o posterior, el usuario debe otorgar el permiso "Mientras se usa la aplicación" cuando se lo pida.
Localización	Antirrobo: localización del dispositivo En los dispositivos con Android 10 o posterior, el usuario debe conceder el permiso "Todo el tiempo" cuando se solicite.
	Comandos: obtener historial de ubicaciones
Accesibilidad	Antirrobo: bloqueo del dispositivo (solo para Android 7 y versiones posteriores)
	Protección web
	Control de apps
	Protección de eliminación de aplicaciones (solo para Android 7 y versiones posteriores)
	Visualización de advertencias de Kaspersky Endpoint Security para Android (solo para Android 10 o versiones posteriores)
	Restringir el uso de la cámara (solo para Android 11 o posterior)
Mostrar ventanas emergentes (para algunos dispositivos Xiaomi)	Protección web
Mostrar ventanas emergentes mientras se ejecuta en segundo plano (para algunos dispositivos Xiaomi)	Protección web
Ejecutar en segundo plano (para dispositivos Xiaomi con firmware MIUI en Android 11 o anterior)	Control de apps
	Protección web
	Antirrobo

Iniciar y detener Kaspersky Endpoint Security para Android

Kaspersky Endpoint Security para Android se inicia al iniciarse el sistema operativo y protege el dispositivo móvil durante la sesión completa. El usuario puede detener la aplicación al deshabilitar todos los componentes de Kaspersky Endpoint Security para Android. Puede usar directivas a fin de configurar los permisos del usuario para administrar componentes de la aplicación.

En ciertos dispositivos (por ejemplo, HUAWEI, Meizu y Xiaomi), debe agregar manualmente Kaspersky Endpoint Security para Android a la lista de aplicaciones que se inician al iniciarse el sistema operativo (**Seguridad** → **Permisos** → **Ejecución automática**). Si la aplicación no se agrega a la lista, Kaspersky Endpoint Security para Android deja de realizar todas sus funciones después de que el dispositivo móvil se reinicia.

También debe deshabilitar el modo de Ahorro de batería para Kaspersky Endpoint Security para Android. Esto es necesario para que la aplicación se ejecute en segundo plano, por ejemplo, al ejecutar un análisis de malware programado o sincronizar el dispositivo con Kaspersky Security Center. Este problema se puede atribuir a las funciones específicas del software integrado de estos dispositivos.

Activar Kaspersky Endpoint Security para Android

En Kaspersky Security Center, la licencia puede cubrir varios grupos de funciones. Para garantizar que la aplicación Kaspersky Endpoint Security para Android sea totalmente funcional, la licencia de Kaspersky Security Center adquirida por la organización debe admitir la funcionalidad de Administración de dispositivos móviles.

Para obtener información detallada sobre las opciones de licencia, consulte la sección Acerca de la licencia.

La activación de la aplicación Kaspersky Endpoint Security para Android en un dispositivo móvil se realiza proporcionando información de licencia válida a la aplicación. La información de la licencia se envía al dispositivo junto con la configuración de la directiva al sincronizar el dispositivo con Kaspersky Security Center.

Si la activación de la aplicación móvil no se completa en 30 días a partir del momento en que se instala en el dispositivo móvil, la aplicación cambia automáticamente al modo de funcionalidad limitada. En este modo, la mayoría de los componentes de la aplicación no son operativos. En modo de funcionalidad limitada, la aplicación deja de realizar la sincronización automática con Kaspersky Security Center. Por lo tanto, si no se activa la aplicación 30 días después de la instalación, el usuario deberá sincronizar manualmente el dispositivo con Kaspersky Security Center.

Si Kaspersky Security Center no está implementado en su organización o no está accesible a los dispositivos móviles, los usuarios pueden activar la aplicación móvil en sus dispositivos de forma manual.

Para activar la aplicación móvil:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Haga clic en el botón **License**.

4. En la ventana que se abre, utilice la lista desplegable para seleccionar la clave de licencia requerida del almacenamiento de claves del Servidor de administración.

   Los detalles de la clave de licencia se muestran en los campos a continuación.

   > Puede reemplazar la clave de activación existente en el dispositivo móvil si es diferente de la seleccionada en la lista desplegable anterior. Para hacerlo, seleccione la casilla **Replace with selected key if the key on devices is different**.

5. Haga clic en el botón **Save** para guardar los cambios que realizó.

La aplicación se activará después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Actualizar Kaspersky Endpoint Security para Android

Kaspersky Endpoint Security para Android se puede actualizar de las siguientes maneras:

- Mediante el sitio web de Kaspersky. El usuario del dispositivo móvil descarga la nueva versión de la aplicación desde el sitio web de Kaspersky y la instala en el dispositivo.
- Mediante HUAWEI AppGallery, Samsung Galaxy Store, RuStore o Xiaomi GetApps. El usuario del dispositivo móvil descarga la nueva versión de la aplicación desde una tienda de aplicaciones y la instala en el dispositivo siguiendo el procedimiento de actualización estándar para la plataforma Android.

  > Para actualizar la aplicación a través de Samsung Galaxy Store, el usuario del dispositivo debe tener una cuenta de Samsung.

- Mediante Kaspersky Security Center. Puede actualizar remotamente la versión de la aplicación en el dispositivo mediante Kaspersky Security Center.

Puede seleccionar el método de actualización de la aplicación más conveniente para su organización. Puede usar solo un método de actualización.

Actualización de la aplicación desde el sitio web de Kaspersky

Para actualizar la aplicación desde el sitio web de Kaspersky:

1. Vaya al sitio web de Kaspersky.
2. Busque Kaspersky Security para dispositivos móviles en el sitio web.
3. Toque **Mostrar descargas**.
4. Seleccione una versión de la aplicación y toque **Descargar**.
5. Abra el archivo APK descargado y siga las instrucciones en pantalla.

Kaspersky Endpoint Security para Android se actualizó.

Después de descargar la aplicación, Kaspersky Endpoint Security para Android comprueba los términos y condiciones del Contrato de licencia de usuario final (EULA). Si se actualizaron los términos del EULA, la aplicación envía una solicitud a Kaspersky Security Center. Si el administrador acepta el EULA en Kaspersky Next Expert View (on-premise), Kaspersky Endpoint Security para Android omite el paso de aceptación durante la instalación de la aplicación.

Actualización de la aplicación mediante Kaspersky Security Center

Kaspersky Endpoint Security para Android se puede actualizar utilizando Kaspersky Security Center después de que se aplica una directiva de grupo. En la configuración de la directiva de grupo, puede seleccionar el paquete de instalación independiente de la versión de Kaspersky Endpoint Security para Android que cumpla con los requisitos de seguridad corporativos.

Puede actualizar a través de Kaspersky Security Center si Kaspersky Endpoint Security para Android se instaló mediante un paquete de instalación en Kaspersky Security Center o mediante un paquete de instalación independiente. Si se instaló desde Google Play, no puede actualizar la aplicación a través de Kaspersky Security Center.

Para actualizar Kaspersky Endpoint Security para Android mediante un paquete de instalación independiente, se debe permitir la instalación de aplicaciones desde fuentes desconocidas en el dispositivo móvil del usuario. Para obtener información sobre la instalación de aplicaciones sin Google Play, consulte la Ayuda de Android.

Para actualizar la versión de la aplicación:

1. Agregue un nuevo paquete de instalación de Kaspersky Endpoint Security para Android.
2. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
3. En la ventana de propiedades de la directiva, seleccione **Application settings**.
4. Seleccione **Android** y vaya a la sección **KES for Android settings**.
5. En la tarjeta **App update**, haga clic en **Settings**.

   Se abre la ventana **App update**.
6. Habilite la configuración con el interruptor **App update**.
7. Haga clic en **Select**.

   Se abre la ventana **Select installation package**.
8. En la lista de paquetes de instalación independientes de Kaspersky Endpoint Security para Android, seleccione el paquete cuya versión cumpla con los requisitos de seguridad corporativos.

   No se puede revertir a una versión anterior de la aplicación Kaspersky Endpoint Security para Android.
9. Haga clic en **Select**.

10. Haga clic en **Aceptar**.

11. Haga clic en el botón **Save** para guardar los cambios que realizó.

    La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center. Se le solicita al usuario del dispositivo móvil que instale la versión nueva de la aplicación. Después de que el usuario confirma la instalación, la versión nueva de la aplicación se instala en el dispositivo móvil.

La función de actualizaciones (incluido el suministro de actualizaciones de las firmas antimalware y de la base de código) y la función de KSN pueden dejar de estar disponibles en el software en el territorio de EE. UU.

Eliminar Kaspersky Endpoint Security para Android

Kaspersky Endpoint Security para Android se puede eliminar de los modos siguientes:

1. Eliminación de la aplicación por parte del usuario

   El usuario elimina Kaspersky Endpoint Security para Android manualmente con la interfaz de la aplicación. Para que los usuarios puedan eliminar la aplicación, la eliminación de la aplicación debe estar permitida en la tarjeta **Configure access to app settings** de la sección **KES for Android settings** en la configuración de la directiva.

2. Eliminación de la aplicación por parte del administrador (solo dispositivos corporativos)

   El administrador elimina la aplicación de forma remota mediante Kaspersky Next Expert View (local). La aplicación se puede eliminar desde un dispositivo independiente o desde varios dispositivos a la vez.

Permitir a los usuarios eliminar Kaspersky Endpoint Security para Android

Para proteger la aplicación contra la eliminación en dispositivos con Android 7 o posterior, Kaspersky Endpoint Security para Android debe estar configurado como función de accesibilidad. Cuando el Asistente de configuración inicial se está ejecutando, Kaspersky Endpoint Security para Android le pide al usuario que conceda a la aplicación todos los permisos requeridos. El usuario puede omitir estos pasos o desactivar estos permisos en la configuración del dispositivo más adelante. En ese caso, la aplicación no estará protegida de la eliminación.

Para permitir la eliminación de la aplicación en una directiva de grupo:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **Android** y vaya a la sección **KES for Android settings**.

4. En la tarjeta **Configure access to app settings**, haga clic en **Settings**.

   Se abre la ventana **Configure access to app settings**.

5. Seleccione la casilla **Allow removing the app from device**.

6. Haga clic en **Aceptar**.

7. Haga clic en el botón **Save** para guardar los cambios que realizó.

Como resultado, los usuarios podrán eliminar la aplicación de los dispositivos móviles después de la sincronización con el Servidor de administración. El botón de eliminación de la aplicación pasa a estar disponible en la configuración de Kaspersky Endpoint Security para Android.

Para eliminar una aplicación de un dispositivo, siga estos pasos:

1. En la ventana principal de Kaspersky Endpoint Security para Android, toque **Settings** → **App settings** → **Additional** → **Remove app**.

> En los dispositivos corporativos, solo el administrador puede eliminar Kaspersky Endpoint Security para Android.

2. Confirme la eliminación de Kaspersky Endpoint Security para Android.

Kaspersky Endpoint Security para Android se eliminará del dispositivo.

Eliminación de Kaspersky Endpoint Security para Android por parte del usuario

> En los dispositivos corporativos, solo el administrador puede eliminar Kaspersky Endpoint Security para Android.

Para eliminar de forma independiente Kaspersky Endpoint Security para Android desde un dispositivo móvil, el usuario debe seguir este procedimiento:

1. En la ventana principal de Kaspersky Endpoint Security para Android, toque **Settings** → **App settings** → **Additional** → **Remove app**.

> Si el botón **Remove app** no se muestra, esto significa que el administrador activó la protección contra la eliminación de Kaspersky Endpoint Security para Android o que el dispositivo opera en modo de propietario del dispositivo.

2. Confirme la eliminación de Kaspersky Endpoint Security para Android.

Kaspersky Endpoint Security para Android se eliminará del dispositivo.

> Le recomendamos que elimine Kaspersky Endpoint Security para Android solo con la configuración de la aplicación, como se describe en las instrucciones anteriores. Otros métodos de desinstalación pueden resultar en la eliminación incompleta de contenedores corporativos y causar otro comportamiento impredecible.

Eliminación remota de Kaspersky Endpoint Security para Android en dispositivos corporativos

Puede eliminar la aplicación Kaspersky Endpoint Security para Android de los dispositivos corporativos de forma remota enviando un comando **Reset to factory settings**.

Al ejecutar el comando **Reset to factory settings**, se borran todos los datos del dispositivo y se revierte la configuración del dispositivo a sus valores de fábrica. Android Enterprise recomienda este método de eliminación de aplicaciones para garantizar que los datos se eliminen de un dispositivo corporativo.

Para eliminar la aplicación,

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.
2. En la lista de dispositivos que se abre, seleccione un dispositivo al que desee enviar un comando.

   Puede seleccionar varios dispositivos.
3. Haga clic en **Send command**.
4. En la ventana **Send command** que se abre, en el campo **Command**, seleccione el comando **Reset to factory settings**.
5. Haga clic en **Send**.

   Puede ver y cancelar comandos en el **Command history**.

   El comando se envía a los dispositivos seleccionados. Kaspersky Endpoint Security para Android se elimina de estos dispositivos.
6. En la lista de dispositivos, seleccione el dispositivo y luego haga clic en **Delete**.

   El dispositivo se elimina de la lista de dispositivos administrados en Kaspersky Next Expert View (on-premise).

   Si el dispositivo no se elimina de Kaspersky Next Expert View (on-premise), puede haber problemas con la instalación de aplicaciones de Kaspersky en este dispositivo.

Administración de dispositivos móviles en Kaspersky Next Expert View (on-premise)

Para realizar una configuración centralizada de dispositivos móviles, debe configurar las directivas. Una directiva es un conjunto de configuraciones de seguridad para administrar dispositivos móviles de sistemas operativos y modos de funcionamiento específicos dentro de un grupo de administración y para administrar las aplicaciones móviles instaladas en los dispositivos.

En esta sección se describe cómo crear grupos de administración, configurar directivas para dispositivos móviles y conectar dispositivos móviles a Kaspersky Security Center para administrarlos posteriormente.

Creación de grupos de administración

Para aplicar una directiva a un grupo de dispositivos, es aconsejable crear un grupo independiente para estos dispositivos antes de instalar las aplicaciones de administración de dispositivos móviles.

Un *grupo de administración* es un conjunto lógico de dispositivos administrados que se combinaron en función de un rasgo específico para que se los pueda administrar como una única unidad dentro de Kaspersky Security Center.

Todos los dispositivos administrados que pertenecen a un grupo de administración están configurados para lo siguiente:

- Use la misma configuración, que puede especificar en Directivas.
- Usar un modo común de funcionamiento de las aplicaciones, mediante la creación de tareas de grupo con parámetros específicos. Puede usar tareas de grupo para, por ejemplo, crear e instalar un paquete de instalación común, actualizar las bases de datos y los módulos de una aplicación, realizar análisis a pedido y activar la protección en tiempo real.

Un dispositivo administrado puede pertenecer a un solo grupo de administración.

Los grupos y los servidores de administración se pueden organizar en jerarquías sin límites de anidamiento. Cada nivel de una jerarquía puede incluir servidores de administración secundarios y virtuales, grupos y dispositivos administrados. También puede mover dispositivo de un grupo a otro.

Inmediatamente después de la instalación de Kaspersky Security Center, la jerarquía de los grupos de administración contiene solo un grupo de administración llamado Dispositivos administrados. Al crear una jerarquía de grupos de administración, puede agregar dispositivos al grupo Dispositivos administrados y agregar grupos anidados.

Para crear un grupo de administración, haga lo siguiente:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** > **Hierarchy of groups**.
2. En la estructura del grupo de administración, seleccione el grupo de administración al que pertenecerá el nuevo grupo de administración.
3. Haga clic en **Agregar**.
4. En la ventana **Name of the new administration group** que se abre, ingrese un nombre para el grupo y, a continuación, haga clic en el botón **Agregar**.

   Aparece un nuevo grupo de administración con el nombre especificado en la jerarquía de grupos de administración.

Para crear automáticamente una estructura de grupos de administración, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** > **Hierarchy of groups**.

2. Haga clic en **Import**.

Se inicia el Asistente de nueva estructura de grupos de administración. Siga las instrucciones del asistente.

Después de crear un grupo de administración, se recomienda configurar la opción de asignar automáticamente los dispositivos en los cuales desea instalar las aplicaciones en este grupo. Luego, configure los parámetros que son comunes para todos los dispositivos mediante una directiva de específica.

Configurar directivas

En esta sección se describe cómo administrar directivas en Kaspersky Next Expert View (on-premise).

Crear una directiva

Kaspersky Next Expert View (on-premise) le permite crear directivas para establecer la configuración de seguridad de un grupo de dispositivos móviles Android, iOS y Aurora. Los valores de los ajustes de seguridad configurados en las directivas se guardan en el Servidor de administración, se distribuyen a los dispositivos móviles durante la sincronización y se guardan en los dispositivos como la configuración actual.

Puede crear directivas mediante el Asistente de directivas móviles.

Para crear una directiva:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**.

2. En la estructura del grupo de administración, seleccione el grupo de administración para el que desea crear una directiva.

   De manera predeterminada, la nueva directiva se aplicará al grupo de **Mobile devices**.

3. Haga clic en **Agregar** para iniciar el Asistente de directivas móviles.

4. En la ventana **Select application**, seleccione la opción **Kaspersky Mobile Devices Protection and Management** y luego haga clic en **Siguiente**.

   Se abre el Asistente de directivas móviles. Haga clic en **Start** y luego avance por el asistente con los botones **Back** y **Next**.

Paso 1. Licencia

En este paso, seleccione una licencia.

La licencia que seleccione determina los ajustes de seguridad que puede configurar en una directiva. De manera predeterminada, se preselecciona la licencia que admite la funcionalidad MDM básico en Kaspersky Next Expert View (on-premise). Puede seleccionar una licencia diferente manualmente.

Después de actualizar la licencia en la directiva principal, se debe volver a guardar la directiva secundaria para aplicar los cambios.

Paso 2. Sistemas operativos y modos de funcionamiento del dispositivo

En este paso, seleccione los sistemas operativos a los que se aplicará la directiva y especifique los modos de funcionamiento del dispositivo

- **Android**
  - **Personal device** (protección y administración básicas de un dispositivo Android personal).
  - **Device with corporate container** (entorno corporativo aislado en un dispositivo Android).
  - **Corporate device** (un conjunto ampliado de configuraciones para administrar un dispositivo Android corporativo).

    Para obtener información detallada, consulte la sección Acerca de los modos de funcionamiento del dispositivo Android.
- **iOS**
  - **Basic protection** (protección contra amenazas web y detección de liberación en dispositivos iOS).
  - **Basic control** (administración básica de un dispositivo iOS personal).
  - **Supervised** (un conjunto ampliado de configuraciones para administrar un dispositivo iOS).

    Para obtener información detallada, consulte la sección Acerca de los modos de funcionamiento del dispositivo iOS.

    Para conectar y administrar dispositivos iOS en los modos de funcionamiento supervisado y de control básico, debe tener un Servidor de MDM para iOS instalado en el grupo de administración seleccionado. Para obtener información detallada sobre la instalación del Servidor de MDM para iOS, consulte la sección Implementar el Servidor de MDM para iOS.

    Para el modo de funcionamiento de protección básica, puede crear un grupo de administración independiente sin el Servidor de MDM para iOS y distribuir una directiva.

    Para los modos de funcionamiento de control básico o supervisado, puede crear grupos de administración con diferentes Servidores de MDM para iOS y distribuir diferentes directivas respectivamente.

    Además, puede combinar dispositivos en los modos de funcionamiento supervisado y de control básico en un grupo de administración y distribuir una directiva para el modo de funcionamiento supervisado. En este caso, la configuración admitida por el modo de funcionamiento correspondiente se aplicará a los dispositivos.

- **Aurora**
  - **Protection** (protección de dispositivos Aurora contra amenazas).

    Para conectar dispositivos Aurora, debe tener Kaspersky Endpoint Security for Aurora preinstalado en los dispositivos que se conectarán.

*En la pestaña **General** de la ventana Nueva directiva:*

1. En el campo **Name**, especifique el nombre de la nueva directiva. Si especifica el nombre de una directiva existente, se le agregará un (1) al final de manera automática.
2. En el bloque de configuración **Policy status**, seleccione el estado de la directiva:
   - **Active**. El asistente guarda la directiva creada en el Servidor de administración. En la siguiente sincronización de los dispositivos móviles con el Servidor de administración, la directiva se usará como directiva activa en los dispositivos.
   - **Inactive**. El asistente guarda la directiva creada en el Servidor de administración como directiva de respaldo. Esta directiva se puede activar en el futuro, después de un evento específico. Si es necesario, una directiva inactiva puede pasarse al estado activo.

     Se pueden crear varias directivas para una aplicación del grupo, pero solo una de ellas puede estar activa. Cuando se crea una nueva directiva activa, la anterior automáticamente deja de estar en efecto.
3. En el bloque de configuración **Settings inheritance**, seleccione las opciones de herencia:
   - **Inherit settings from parent policy**

     Si habilita esta opción en una directiva secundaria y un administrador bloquea algunas configuraciones en la directiva primaria, no podrá cambiar esas configuraciones en la directiva secundaria.

     Si deshabilita esta opción, podrá cambiar todas las configuraciones del grupo secundario, incluso si algunas están bloqueadas en la directiva principal.
   - **Force inheritance of settings in child policies**

     Si habilita esta opción en una directiva principal, se habilita la opción **Inherit settings from parent policy** para cada directiva secundaria. En este caso, no puede deshabilitar esta opción para ninguna directiva secundaria. Todas las configuraciones que están bloqueadas en la directiva principal se heredan a la fuerza en los grupos secundarios y no puede cambiar estas configuraciones en los grupos secundarios.

   De manera predeterminada, la opción **Inherit settings from parent policy** está habilitada y la opción **Force inheritance of settings in child policies** está deshabilitada.

   Para obtener más información sobre la herencia de directivas, consulte la Ayuda de Kaspersky Security Center.

La herencia de la configuración de la directiva solo funciona si se seleccionan modos de funcionamiento del dispositivo idénticos para la directiva principal y secundaria o si los modos de funcionamiento del dispositivo seleccionados para la directiva secundaria proporcionan más configuraciones de seguridad. Por ejemplo, una directiva secundaria para dispositivos Android con un contenedor corporativo puede heredar la configuración de una directiva principal para dispositivos personales, pero no puede heredar la configuración de una directiva principal para dispositivos corporativos.
Si crea una directiva secundaria que no es compatible con la directiva principal, debe eliminarla y crear una nueva directiva secundaria para administrar dispositivos.

4. Haga clic en **Guardar**.

Se crea la nueva directiva para dispositivos móviles. Para obtener más información sobre cómo configurar la configuración de la directiva, consulte la sección Configuración y administración.

Modificar una directiva

Kaspersky Next Expert View (on-premise) le permite modificar directivas.

Para modificar una directiva:

1. Realice una de las siguientes acciones para abrir la ventana de propiedades de la directiva:

   - En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas que se abre, haga clic en el nombre de la directiva que desee modificar.

   - En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**. Seleccione el dispositivo móvil al que se aplica la directiva que desee modificar y, luego, seleccione la directiva en la pestaña **Active policies and policy profiles**.

2. En la ventana de propiedades de la directiva, vaya a la pestaña **Application settings** y defina la configuración de la directiva.

Además, puede definir la configuración general, la herencia de la configuración, las notificaciones y el registro de eventos y los perfiles de la directiva, y ver el historial de revisión. Para obtener más información, consulte la Ayuda de Kaspersky Security Center.

3. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana de propiedades de la directiva.

Se modifica la directiva. Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Copiar una directiva

Kaspersky Next Expert View (on-premise) le permite crear una copia de una directiva.

Para crear una copia de una directiva, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**.
2. En la lista de directivas que se abre, seleccione la casilla junto al nombre de la directiva que desee copiar y, a continuación, haga clic en **Copiar**.
3. En el árbol de grupos de administración que se abre, seleccione el grupo de destino donde desea que se cree la directiva.

   Para crear un grupo de administración nuevo, seleccione un grupo existente y, a continuación, haga clic en **Add child group**.
4. Haga clic en **Copiar**.
5. Haga clic en **Aceptar** para confirmar la operación.

Se creará una copia de la directiva en el grupo objetivo con el mismo nombre. El estado de cada directiva copiada o movida en el grupo objetivo será *Inactiva*. Puede cambiar el estado a *Activa* en cualquier momento.

Si en el grupo objetivo ya existe una directiva con un nombre idéntico al de la directiva recién creada o movida, se agrega el sufijo (<siguiente número de secuencia>) al nombre de la directiva que se creó o movió recientemente, por ejemplo: (1).

Movimiento de una directiva a otro grupo de administración

Kaspersky Next Expert View (on-premise) le permite mover una directiva a otro grupo de administración.

Para mover una directiva a otro grupo de administración, siga los siguientes pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**.
2. En la lista de directivas que se abre, seleccione la casilla junto al nombre de la directiva que desee mover a otro grupo de administración y, a continuación, haga clic en **Mover**.
3. En el árbol emergente de grupos de administración, seleccione el grupo objetivo al que desee mover la directiva.

   Para crear un grupo de administración nuevo, seleccione un grupo existente y, a continuación, haga clic en **Add child group**.
4. Haga clic en **Mover**.
5. Haga clic en **Aceptar** para confirmar la operación.

El resultado depende de las propiedades de herencia de la directiva:

- Si la directiva no se hereda en el grupo de origen, se moverá al grupo objetivo.
- Si la directiva se hereda en el grupo de origen, no se moverá. En su lugar, se creará una copia de la directiva en el grupo objetivo.

El estado de cada directiva copiada o movida en el grupo objetivo será *Inactiva*. Puede cambiar el estado a *Activa* en cualquier momento.

Si en el grupo objetivo ya existe una directiva con un nombre idéntico al de la directiva recién creada o movida, se agrega el sufijo (<siguiente número de secuencia>) al nombre de la directiva que se creó o movió recientemente, por ejemplo: (1).

Ver la lista de directivas

Kaspersky Next Expert View (on-premise) le permite ver la lista de directivas creadas, sus estados y propiedades.

Para ver la lista de directivas, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**.

2. Se abrirá la lista de directivas con una breve información sobre estas. En esta página, puede crear, modificar, copiar, mover y eliminar las directivas.

Visualización de los resultados de la distribución de directivas

Kaspersky Next Expert View (on-premise) le permite ver el gráfico de distribución de una directiva y la información sobre todos los dispositivos que se rigen por esa directiva.

Para ver los resultados de la distribución de una directiva, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**.

2. En la lista de directivas que se abre, seleccione la casilla junto al nombre de la directiva cuyos resultados de distribución desea ver y, a continuación, haga clic en **Distribution**.

Se abre la página de resultados de distribución de la directiva. Esta página contiene el resumen de la directiva, un gráfico de distribución de la directiva y una tabla con información sobre todos los dispositivos incluidos en esa directiva. Para abrir la ventana de propiedades de la directiva, haga clic en el botón **Configure policy**.

Administrar revisiones de directivas

Kaspersky Next Expert View (on-premise) le permite ver qué modificaciones se realizaron en una directiva durante un período determinado, así como guardar información sobre estas modificaciones en un archivo.

Para ver una revisión de una directiva:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**.

2. En la lista de directivas que se abre, haga clic en la directiva cuya revisión desea ver y luego vaya a la sección **Revision history**.

3. En la lista de revisiones de la directiva, haga clic en el número de revisión que desee ver.

Si el tamaño de una revisión es superior a 10 MB, no podrá verla con Kaspersky Next Expert View (on-premise). Se le pedirá que guarde la revisión seleccionada en un archivo JSON.

Si el tamaño de la revisión no supera los 10 MB, se muestra un informe en formato HTML con la configuración de la revisión de la directiva seleccionada. Dado que el informe se muestra en una ventana emergente, asegúrese de que las ventanas emergentes estén permitidas en su navegador.

Para guardar una revisión de la directiva en un archivo JSON, en la lista de revisiones de la directiva, seleccione la revisión que desea guardar y, a continuación, haga clic en **Save to file**.

La revisión se guardará en un archivo JSON.

Para obtener información detallada sobre cómo administrar las revisiones de las directivas, consulte la Ayuda de Kaspersky Security Center.

Restringir los permisos para configurar directivas

Los administradores de Kaspersky Security Center pueden configurar los permisos de acceso de los usuarios de Kaspersky Next Expert View (on-premise) para diferentes funciones de la solución MDM básico en Kaspersky Next Expert View (on-premise), según las tareas laborales de los usuarios.

En la interfaz de Kaspersky Next Expert View (on-premise), puede configurar los derechos de acceso en las pestañas **Seguridad** y **User roles** de la ventana de propiedades del Servidor de administración. La pestaña **User roles** le permite agregar roles de usuario estándar con un conjunto predefinido de derechos. La sección **Seguridad** le permite configurar derechos para un mismo usuario o un grupo de usuarios, o asignar funciones a un usuario o a un grupo de usuarios. Los derechos de usuario para cada aplicación se configuran en función de alcances funcionales.

Para cada área funcional, el administrador puede asignar los siguientes permisos:

- **Permitir modificación**. El usuario de Kaspersky Next Expert View (on-premise) puede cambiar la configuración de las directivas en la ventana de propiedades.
- **Bloquear modificación**. El usuario de Kaspersky Next Expert View (on-premise) no puede cambiar la configuración de las directivas en la ventana de propiedades. Las fichas de la directiva que pertenecen al alcance funcional para el cual se ha asignado este derecho no se muestran en la interfaz.

Para obtener más información sobre la administración de derechos y roles de usuario en Kaspersky Next Expert View (on-premise), consulte la ayuda de Kaspersky Security Center.

Configurar el control de acceso basado en roles

Kaspersky Next Expert View (on-premise) proporciona herramientas para el acceso basado en roles a las funciones de MDM básico en Kaspersky Next Expert View (on-premise).

Puede configurar los derechos de acceso a las funciones de la aplicación para MDM básico en Kaspersky Next Expert View (on-premise) de una de las siguientes formas:

- Configure los derechos de cada usuario o grupo de usuarios individualmente;
- Cree roles de usuarios estándares con un conjunto predefinido de derechos y asignar esos roles a los usuarios en función del ámbito de sus actividades.

Aplicar roles de usuario es una manera de simplificar y agilizar la tarea rutinaria de configurar derechos de acceso a las funciones de la aplicación. Cada rol tiene asignados permisos de acceso que responden a las tareas y obligaciones con las que deben cumplir los usuarios.

Los roles de usuario pueden llevar nombres que identifiquen sus propósitos. Puede crear un número ilimitado de roles en la aplicación. Puede utilizar roles de usuario predefinidos, que ya vienen configurados con un conjunto de derechos, o puede crear roles nuevos y configurar los derechos necesarios a mano.

Para obtener información detallada sobre cómo configurar el acceso del usuario en Kaspersky Security Center, consulte la Ayuda de Kaspersky Security Center.

Algunos de los roles de usuario predefinidos no están autorizados para funcionar con dispositivos móviles. Los roles de usuario predefinidos que están disponibles para las funciones del MDM básico en Kaspersky Next Expert View (on-premise) se enumeran en la siguiente tabla.

Roles de usuario predefinidos para el MDM básico en Kaspersky Next Expert View (on-premise)

Rol	Leer	Escribir	Administración de claves de licencia: cree directivas y modifique la configuración de claves de licencia	Administración de vulnerabilidades y parches: consulte los EULA no aceptados y acepte EULA
Administrador de Kaspersky Endpoint Security	+	+	-	-
Operador de Kaspersky Endpoint Security	+	-	-	-
Administrador principal	+	+	-	-
Operador principal	+	-	-	-
Administrador de Administración de dispositivos móviles	+	+	+	+
Operador de Administración de dispositivos móviles	+	-	-	-

Para obtener información detallada sobre los roles de usuario predefinidos, consulte la Ayuda de Kaspersky Security Center.

Derechos de acceso a las funciones de MDM básico en Kaspersky Next Expert View (on-premise)

Área funcional	Derecho
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (on-premise) > Configuración de la aplicación	• **Lectura:** obtenga acceso de lectura a todas las configuraciones en la sección de la directiva correspondiente • **Escritura:** obtenga acceso de escritura a todas las configuraciones en la sección de la directiva correspondiente Tenga en cuenta que para ajustar la configuración de Protección web y Control web, el administrador debe tener los derechos de **Lectura** y **Escritura** para las áreas funcionales **Protección web** y **Controles de seguridad**.
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (on-premise) > Controles de seguridad	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (on-premise) > Contenedor corporativo	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (on-premise) > Configuración del dispositivo	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (on-premise) > Configuración de las aplicaciones de administración de dispositivos de Kaspersky	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (on-premise) > Protección	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (on-premise) > Restricciones	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (on-premise) > Configuración de Samsung Knox	

Derecho	Acción del usuario: derecho necesario para realizar la acción
Administración de dispositivos móviles > **General** > **Lectura**	• Ver la sección **Móvil** en Kaspersky Next Expert View (on-premise)
Administración de dispositivos móviles > **General** > **Escritura**	• Realizar cualquier acción con los certificados (excepto ver los certificados) También se debe otorgar el derecho **Administrar certificados**. • Ajustar la configuración de Firebase Cloud Messaging
Administración de dispositivos móviles > **General** > **Conectar nuevos dispositivos**	• Conectar nuevos dispositivos móviles y Servidores de MDM para iOS • Eliminar dispositivos
Administración de dispositivos móviles > **General** > **Administrar certificados**	• Realizar cualquier acción con certificados • Configurar reglas de emisión de certificados También se debe otorgar el derecho de **Escritura**.
Administración de dispositivos móviles > **General** > **Enviar solo comandos de información a dispositivos móviles**	• Enviar y cancelar el comando **Sincronizar dispositivo**
Administración de dispositivos móviles > **General** > **Enviar comandos a dispositivos móviles**	• Enviar y cancelar cualquier comando
Administración de dispositivos móviles > General > Iniciar sesiones de RDP	• Establecer conexiones remotas a dispositivos

Configuración de perfiles de directivas

Los perfiles de directivas facilitan la administración de varias versiones de una misma directiva dentro de un grupo de administración. Puede crear una sola directiva y agregar perfiles que contengan únicamente la configuración que desea personalizar, lo que elimina la necesidad de crear varias directivas similares desde cero.

Cada perfil es un subconjunto específico de la configuración de la directiva. La directiva proporciona la configuración principal para los dispositivos administrados, mientras que cada perfil contiene únicamente la configuración que difiere de la directiva principal.

Los perfiles se distribuyen a los dispositivos administrados junto con la directiva y se aplican cuando se cumplen sus condiciones de activación. Cuando se activa un perfil, su configuración anula la configuración correspondiente de la directiva principal. Por ejemplo, una directiva puede impedir que los usuarios instalen aplicaciones en los dispositivos administrados en general, mientras que un perfil de esa directiva permite que los usuarios instalen aplicaciones de un grupo específico de dispositivos o usuarios.

El uso de perfiles de directivas permite administrar diferentes configuraciones de dispositivos y mantener una sola directiva.

Puede modificar las condiciones específicas que deben afectar la activación del perfil de la directiva que está creando. Para dispositivos móviles, puede modificar las siguientes condiciones:

- **Rules for specific device owner**

  Activación del perfil en el dispositivo según su propietario.

  - **Device owner**
  - **Device owner is included in an internal security group**

- **Rules for role assignment**

  Activación del perfil en el dispositivo según el rol del propietario.

  - **Activate policy profile by specific role of device owner**

- **Rules for tag usage**

  Activación del perfil en el dispositivo en función de las etiquetas asignadas al dispositivo.

  - **Lista de etiquetas**
  - **Apply to devices without the specified tags**

- **Rules for Active Directory usage**

  Activación del perfil de directiva en el dispositivo según la asignación del dispositivo en una unidad organizativa de Active Directory o la membresía de ese dispositivo (o el propietario del dispositivo) en un grupo de seguridad de Active Directory. El alcance de la configuración depende de la directiva utilizada actualmente.

  - **Device owner's membership in an Active Directory security group**
  - **Device membership in Active Directory security group**
  - **Device allocation in Active Directory organizational unit**

Para obtener información detallada sobre cómo configurar reglas de activación, crear, eliminar o copiar perfiles de directivas, consulte la Ayuda de Kaspersky Security Center.

Eliminar una directiva

Kaspersky Next Expert View (on-premise) le permite eliminar directivas.

Puede eliminar solo directivas que no se hereden en el grupo de administración actual. Si se hereda una directiva, solo puede eliminarla en el grupo de nivel superior para el que se creó.

Si elimina una directiva principal, sus directivas secundarias permanecerán y estarán disponibles para su edición.

Para eliminar una directiva:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**.
2. En la lista de directivas que se abre, seleccione la casilla junto al nombre de la directiva que desee eliminar y, a continuación, haga clic en **Eliminar**.
3. En la ventana que se abre, haga clic en **Aceptar** para confirmar la operación.

La directiva se elimina. Antes de que se aplique la nueva directiva, los dispositivos móviles que pertenecen al grupo de administración no dejan de trabajar con la configuración especificada en la directiva que se eliminó.

Conexión de dispositivos móviles a Kaspersky Next Expert View (on-premise)

Para administrar dispositivos móviles y las aplicaciones de administración de dispositivos móviles instaladas en ellos, debe conectar estos dispositivos a Kaspersky Security Center.

Antes de conectarlos, asegúrese de que la licencia compatible con la solución de Administración de dispositivos móviles esté configurada en la sección **Claves de licencia** de las propiedades del Servidor de administración.

Para conectar un dispositivo móvil a Kaspersky Security Center, siga los siguientes pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.
2. En la lista de dispositivos móviles que se abre, haga clic en **Add**.

   El Asistente para conectar un nuevo dispositivo móvil empieza a ejecutarse. Haga clic en **Start** y luego avance por el asistente con los botones **Back** y **Next**.

Welcome

En la pantalla de bienvenida, puede leer un resumen de los pasos del asistente de conexión de dispositivos móviles.

Paso 1. Policy

En este paso, seleccione una directiva para los dispositivos que se conectarán Los dispositivos funcionan de acuerdo con la configuración de seguridad especificada en la directiva.

- **Use an existing policy**

  Para esta opción, especifique el grupo de administración de la directiva que desea elegir. Se mostrarán el nombre de la directiva, los sistemas operativos y los modos de funcionamiento de los dispositivos administrados por esta directiva.

  Si es necesario, haga clic en **Go to policy** para ver las propiedades de la directiva que seleccionó.

- **Create a new policy**

  Para esta opción, haga clic en el botón **Create policy** que aparece. Será redirigido al Asistente de directivas móviles. Después de crear una directiva con las propiedades requeridas, puede volver al asistente de conexión de dispositivos móviles.

Paso 2. Operating systems

En este paso, seleccione los sistemas operativos de los dispositivos que se conectarán. La configuración de la directiva determina los sistemas operativos disponibles: Android, iOS o Aurora.

- **Android**

  Después de seleccionar este sistema operativo, se mostrará la **Installation settings** de Kaspersky Endpoint Security para Android. Para modificarlos, haga clic en **Edit settings**.

  a. Seleccione la **Installation source** de Kaspersky Endpoint Security para Android:

  - **Kaspersky website**

    Elija este método para dispositivos móviles que pueden acceder a Internet para descargar el archivo de instalación APK desde el sitio web de Kaspersky. Luego, la aplicación se actualizará desde el sitio web de Kaspersky o desde HUAWEI AppGallery, Samsung Galaxy Store, RuStore o Xiaomi GetApps.

    Esta fuente de instalación funciona para todos los modos de funcionamiento.

  - **RuStore**

    El usuario recibirá un vínculo a RuStore. La aplicación puede instalarse desde RuStore si se sigue el procedimiento de instalación estándar en la plataforma Android.

    El vínculo incluye los siguientes datos:

    - Configuración de sincronización de Kaspersky Security Center.
    - Detalles para la recepción automática del certificado móvil en la primera sincronización.
    - Indicación de si se aceptaron el Contrato de licencia de usuario final de Kaspersky Endpoint Security para Android y las declaraciones adicionales. Si el administrador acepta los acuerdos en Kaspersky Next Expert View (on-premise), Kaspersky Endpoint Security para Android omite el paso de aceptación durante la instalación de la aplicación.

    Esta fuente de instalación funciona solo para dispositivos personales y dispositivos con un contenedor corporativo.

  - **Installation package**

    El paquete de instalación de Kaspersky Endpoint Security para Android se descargará del servidor de Kaspersky Security Center y se actualizará a través de Kaspersky Security Center mediante la configuración de la directiva. Puede elegir este método si los dispositivos móviles de su empresa no tienen acceso a Internet.

    Para esta fuente de instalación, antes de conectar dispositivos móviles, cree el paquete de instalación de Kaspersky Endpoint Security para Android.

Esta fuente de instalación funciona para todos los modos de funcionamiento.

- Para seleccionar un paquete de instalación, haga clic en **Select installation package** y luego seleccione el paquete de instalación de la lista que se abre.
- Si no hay paquetes de instalación disponibles, se le ofrecerá crear uno. Haga clic en **Create installation package** y, a continuación, siga los pasos del Asistente de nuevo paquete, como se describe en la Ayuda de Kaspersky Security Center para crear un paquete de instalación a partir de un archivo o crear un paquete de instalación independiente. Una vez creado el paquete de instalación, puede volver al Asistente de conexión de dispositivos móviles.

Las actualizaciones automáticas a través de la tienda no están disponibles con este método de instalación. Puede actualizar la aplicación manualmente en la sección **App update** de la configuración de la directiva.
Se utiliza el último paquete de instalación cargado en Kaspersky Security Center para instalar la aplicación en los dispositivos.

Para dispositivos corporativos, asegúrese de que la casilla **Allow using HTTP to download the app** esté seleccionada para garantizar que se descargue Kaspersky Endpoint Security para Android. De lo contrario, la aplicación se descargará a través de HTTPS solo si una autoridad certificadora de confianza emitió el certificado del Servidor web de Kaspersky Security Center.

Para obtener más información sobre los métodos de instalación, consulte la sección Instalar Kaspersky Endpoint Security para Android.

b. Seleccione la **Installation network** para Kaspersky Endpoint Security para Android (solo dispositivos corporativos):

- **Prompt the user to select a Wi-Fi network on device**

  Si selecciona esta opción, se le pedirá al usuario que se conecte a cualquier red Wi-Fi disponible para descargar la aplicación.

- **Only use the specified Wi-Fi network** (Android 9 o posterior)

  Para elegir una red de instalación, haga clic en **Select network**.

  En la ventana que se abre, defina los siguientes ajustes:

  - **Service set identifier (SSID)**

    Especifica el nombre de una red inalámbrica con un punto de acceso (SSID). El nombre de la red inalámbrica no puede superar los 32 caracteres.

  - **Hidden network**

    Especifica si la red seleccionada transmite su SSID.

  - **Network protection**

    Especifica un tipo de seguridad de red inalámbrica. Valores posibles:

    - **NONE**

      Si se selecciona, la red no está protegida.

- **WPA**

  Si se selecciona, la red está protegida mediante el protocolo de seguridad WPA. Esta opción requiere el ingreso de una contraseña para acceder a la red.

- **WEP**

  Si se selecciona, la red está protegida con el protocolo WEP. Esta opción requiere el ingreso de una contraseña para acceder a la red y solo se aplica a dispositivos con Android 9 o versiones anteriores.

- **Password**

  Especifica la contraseña para acceder a una red inalámbrica protegida con un protocolo WPA o WEP. La contraseña se enviará al usuario en un código QR.

  No envíe la contraseña para una red Wi-Fi confidencial que no debe ser de público acceso. La contraseña se envía al usuario sin cifrar junto con otros datos de configuración del dispositivo.

- **Use proxy server**

  Especifica el uso de un servidor proxy. Si se selecciona esta opción, debe proporcionar la dirección y el puerto del servidor proxy. También puede especificar una lista de direcciones para los que se omitirá el proxy.

- **Proxy server address**

  Especifica la dirección IP o el nombre del símbolo (dirección web) del servidor proxy. El número máximo de caracteres es 256.

- **Proxy server port**

  Especifica el número de puerto del servidor proxy. El valor debe estar en el intervalo entre 0 y 65536.

- **PAC file URL**

  Una URL a un archivo de configuración automática de proxy (PAC) para la red Wi-Fi.

- **Do not use proxy server for the following addresses**

  Especifica las direcciones para las cuales el servidor proxy no se debe utilizar.

  Puede ingresar la dirección en formato `example.com`. Si ingresa `example.com`, el servidor proxy no se utilizará para las direcciones `pictures.example.com`, `example.com/movies`, etc. El protocolo (por ejemplo, `http://`) se puede omitir.

No utilice una contraseña para una red Wi-Fi confidencial que no debe ser de público acceso. La contraseña no cifrada se envía al usuario en un código QR junto con otros datos de configuración del dispositivo.

- **Try to use mobile network** (Android 8 o posterior)

  Si elige esta opción, el dispositivo intentará usar datos móviles para descargar la aplicación. Si el dispositivo no tiene una tarjeta SIM o la red móvil no está disponible, se le pedirá al usuario que seleccione cualquier red Wi-Fi disponible.

c. Seleccione la casilla **Enable all system apps** (solo dispositivos corporativos) si desea que las aplicaciones

del sistema se mantengan activas en el dispositivo. Si es necesario, se pueden deshabilitar más adelante en la sección Control de aplicaciones.

- **iOS**

  Para conectar y administrar dispositivos iOS en los modos de funcionamiento supervisado y de control básico, debe tener un Servidor de MDM para iOS instalado en el grupo de administración seleccionado. Para obtener información detallada sobre la instalación del Servidor de MDM para iOS, consulte la sección Implementar el Servidor de MDM para iOS.

  La *aplicación Kaspersky Protection para iOS* se instalará en los dispositivos iOS personales en el modo de funcionamiento de protección básica.

  Se instalará un *perfil de administración* en los dispositivos que operan en los modos de control básico y supervisado.

  En los dispositivos que ejecutan iOS 12.1 o posterior, debe confirmar manualmente la instalación de un perfil de administración en un dispositivo móvil. También debe conceder el permiso para la administración remota del dispositivo.

- **Aurora**

  Para conectar dispositivos Aurora, debe tener Kaspersky Endpoint Security for Aurora preinstalado en los dispositivos que se conectarán.

Paso 3. Accept agreements

En este paso, seleccione quién debe aceptar el Contrato de licencia de usuario final (EULA) y la Política de privacidad

- **Administrator**

  El administrador acepta los acuerdos en el siguiente paso del asistente. En este caso, la aplicación omite el paso de aceptación durante la instalación de la aplicación.

- **Users**

  Los usuarios aceptan los acuerdos en los dispositivos móviles.

Este paso solo se aplica a los sistemas operativos iOS y Android. Si conectará dispositivos Aurora, los acuerdos solo son aceptados por los usuarios en sus dispositivos móviles.

Tenga en cuenta que al administrador se le ofrecerá aceptar el EULA solo después de que los usuarios acepten la misma versión del EULA en los dispositivos por primera vez. Después de la conexión y la primera sincronización de los dispositivos con Kaspersky Security Center, el administrador podrá aceptar esta versión del EULA en la posterior conexión de dispositivos.

La lista de contratos aceptados está disponible en la sección **Contrato de licencia de usuario final** de las propiedades del Servidor de administración.

Paso 4. End User License Agreement and Privacy Policy

En este paso, si se selecciona **Administrator** como el destinatario de los contratos en el paso anterior del asistente, se le ofrecerá leer la Política de privacidad, el EULA y todos los documentos asociados. Debe aceptar los términos y condiciones del EULA y la Política de privacidad antes de instalar las aplicaciones de administración de dispositivos móviles.

Paso 5. Users

En este paso, elija uno o más usuarios de los dispositivos que se conectarán. Estos usuarios recibirán los detalles de instalación de la aplicación para conectar sus dispositivos a Kaspersky Security Center. Si un usuario no está en la lista, puede agregar una nueva cuenta de usuario sin salir del asistente.

- Para elegir un usuario existente, seleccione las casillas de verificación junto a los nombres de usuario correspondientes.
- Para agregar un nuevo usuario, haga clic en **Add user**.

  a. Especifique las credenciales de usuario en el bloque de configuración **Credentials**.

  - **User name**
  - **Password**

    La contraseña debe cumplir con los siguientes requisitos de complejidad:

    - La contraseña debe contener entre 8 y 16 caracteres.
    - Debe contener los caracteres de al menos tres de estos grupos: letras mayúsculas (AZ), letras minúsculas (az), dígitos (0-9), caracteres especiales (@ # $% ^ & * - _! + = [] { } |: ',.? / \ `~" ();).

  b. Si es necesario, especifique los detalles opcionales en el grupo de configuración **Optional information**.

  - **Full user name**
  - **Description**
  - **Email address**
  - **Phone number**

  c. Haga clic en **OK** para guardar los cambios.

  El nuevo usuario se agregará y se mostrará en la lista de usuarios.

- Para modificar los detalles del usuario, haga clic en **Edit user**.

  Los campos que puede modificar dependen del subtipo de usuario: *interno* o *dominio*.

No puede especificar otro usuario como propietario del dispositivo ni eliminar el usuario asignado después de que el dispositivo se haya conectado. Sin embargo, si no asignó ningún usuario al conectar el dispositivo, puede asignar el usuario más tarde mediante la entrega de un certificado para dispositivos móviles.

Paso 6. Send connection details

En este paso, seleccione cómo enviar los códigos QR y los vínculos para instalar las aplicaciones de administración móvil o los perfiles de administración. Puede seleccionar una de las siguientes opciones:

- **Send a message to users' email addresses**

  Seleccione esta opción para enviar los detalles de la conexión por correo electrónico a los usuarios seleccionados. Para instalar la aplicación o un perfil de administración, el usuario debe escanear el código QR con la cámara del dispositivo móvil o abrir el vínculo al paquete de instalación.

  Estas direcciones de correo electrónico deben especificarse en la configuración de la cuenta de usuario en Kaspersky Security Center.

  Si desea enviar los detalles de la conexión a una dirección de correo electrónico que no está especificada en la configuración de la cuenta de usuario en Kaspersky Security Center, seleccione la casilla **Send a copy of the message to an alternate email address** y luego especifique la dirección de correo electrónico requerida.

- **Show the details after completing the wizard**

  Elija esta opción para analizar el código QR con la cámara del dispositivo móvil o haga clic en el vínculo del asistente.

Paso 7. Confirm

En este paso, verifique los detalles de conexión del dispositivo móvil especificados en los pasos anteriores y luego haga clic en **Finish** para confirmar la operación.

Si selecciona una gran cantidad de usuarios o grupos de usuarios, la creación de códigos QR y vínculos de conexión puede demorar varios minutos.

Finish

En la pantalla **Finish**:

- Si elige la opción **Send a message to users' email addresses**, los usuarios especificados recibirán los correos electrónicos con códigos QR y vínculos para conectar dispositivos móviles al Servidor de administración.
- Si elige la opción **Show the details after completing the wizard**, los detalles de la conexión estarán disponibles en la pantalla **Finish**. Puede ver los detalles que se muestran o hacer clic en **Download list** para recibir un archivo con información resumida. Los detalles de la conexión se muestran solo una vez y no se puede acceder a ellos nuevamente después de cerrar la pantalla **Finish**.

Haga clic en **Cerrar** para salir del asistente.

Tan pronto como los usuarios instalan las aplicaciones de administración móvil, sus dispositivos se conectan al Servidor de administración y se muestran en la pestaña **Dispositivos** de Kaspersky Next Expert View (on-premise).

Ahora puede ajustar la configuración de los dispositivos y las aplicaciones de administración de dispositivos móviles mediante directivas. También podrá enviar comandos a dispositivos móviles para la protección de datos en caso de robo o pérdida de los dispositivos.

Conexión directa de dispositivos Android a Kaspersky Security Center

Los dispositivos Android pueden conectarse directamente al puerto 13292 del Servidor de administración.

Según el método utilizado para la autenticación, son posibles dos opciones de conexión.

Conectar dispositivos con un certificado cliente (certificado de usuario)

Al conectar un dispositivo con un certificado de usuario, ese dispositivo se asocia a la cuenta de usuario a la cual el certificado correspondiente se asignó a través de herramientas del Servidor de administración.

En este caso, se utilizará la autenticación SSL bidireccional (autenticación mutua). Tanto el Servidor de administración como el dispositivo serán autenticados con certificados.

Conectar dispositivos sin un certificado cliente (certificado de usuario)

Al conectar un dispositivo sin un certificado de usuario, ese dispositivo no se asocia a ninguna de las cuentas de usuario en el Servidor de administración. Pero cuando el dispositivo reciba un certificado, este dispositivo se vinculará al usuario al que las herramientas del Servidor de administración le hayan asignado el certificado correspondiente.

Al conectar ese dispositivo al Servidor de administración, la Autenticación SSL unidireccional se aplicará, lo que significa que solo el Servidor de administración se autentica con el certificado. Después de que el dispositivo reciba el certificado de usuario, el tipo de autenticación cambiará a la autenticación SSL bidireccional (autenticación SSL de 2 modos, autenticación mutua).

Traslado de dispositivos móviles no asignados a grupos de administración

Cuando los dispositivos móviles están conectados a Kaspersky Security Center, se muestran en la página **Asset management → Unassigned devices** de Kaspersky Next Expert View (on-premise). Para administrar los dispositivos recién conectados, puede crear una regla para asignarlos automáticamente a grupos de administración o moverlos a un grupo de administración de forma manual.

Para mover un dispositivo móvil no asignados a un grupo de administración, siga los siguientes pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management → Unassigned devices**.
2. Seleccione el dispositivo que desee mover a un grupo de administración y, a continuación, haga clic en **Move to group**.
3. En el árbol emergente de grupos de administración, seleccione el grupo objetivo al que desee mover el dispositivo.

   Para crear un grupo de administración nuevo, seleccione un grupo existente y, a continuación, haga clic en **Add child group**.
4. Haga clic en **Mover**.

El dispositivo se moverá al grupo de administración especificado y se le aplicará la directiva correspondiente.

Acciones en dispositivos móviles para conectarse al Servidor de administración

Según el modo en el que operará su dispositivo, es posible que deba realizar acciones adicionales para proteger su dispositivo y conectarlo al Servidor de administración.

Instalar un certificado de dispositivos móviles

Si recibió una contraseña de certificado, debe usarla para instalar el certificado de dispositivos móviles en su dispositivo.

Para instalar el certificado de dispositivos móviles, siga estos pasos:

1. Recuerde o anote la contraseña que recibió de su administrador por correo electrónico.
2. Realice una de las siguientes acciones:
   - En un dispositivo Android, ingrese la contraseña del certificado cuando se lo solicite Kaspersky Endpoint Security para Android.
   - En un dispositivo iOS, ingrese la contraseña del certificado durante la instalación del perfil de administración.

El certificado móvil se instalará en su dispositivo.

Preconfigurar dispositivos Android corporativos

Para conectar un dispositivo Android corporativo al Servidor de administración, debe preconfigurar el dispositivo según la versión del sistema operativo y la disponibilidad de un escáner de códigos QR.

Instalar Kaspersky Endpoint Security for Aurora

El código QR que recibió de su administrador contiene la configuración utilizada para conectar su dispositivo al Servidor de administración. Antes de conectar el dispositivo, debe instalar Kaspersky Endpoint Security for Aurora. Para obtener más información sobre la instalación de Kaspersky Endpoint Security en dispositivos Aurora, consulte la Ayuda de Kaspersky Endpoint Security for Aurora.

Configuración de los ajustes de sincronización

Para administrar dispositivos móviles y recibir informes o estadísticas desde dispositivos móviles de usuarios, deberá ajustar la configuración de sincronización. La sincronización se realiza mediante el protocolo HTTPS. La sincronización del dispositivo móvil con el Servidor de administración se puede realizar de las siguientes formas:

- **Mediante programación**. Puede configurar la programación de sincronización en la configuración de la directiva. Las modificaciones en la configuración de la directiva, los comandos y las tareas se realizarán cuando el dispositivo se sincronice con Kaspersky Security Center según la programación, es decir con un retraso.

  Debido a las limitaciones de Doze, cuando selecciona un período de sincronización corto, los dispositivos pueden sincronizarse con el Servidor de administración con menos frecuencia de lo esperado.

  El uso de períodos cortos de sincronización reduce la duración de la batería del dispositivo.

- **Forzada**. La sincronización se realiza mediante notificaciones push de FCM (Firebase Cloud Messaging). La sincronización forzada se realiza principalmente para enviar comandos a un dispositivo móvil en tiempo y forma. Esto puede ser útil cuando un dispositivo móvil está en modo de ahorro de batería, ya que en este caso la aplicación puede realizar tareas más tarde de lo especificado. Si desea usar la sincronización forzada, asegúrese de que los ajustes de FCM estén configurados en Kaspersky Security Center.

  Utilice el comando **Synchronize device** para forzar la sincronización de un dispositivo Android o un dispositivo MDM con iOS.

  > El botón **Force synchronization** y la casilla **Do not disconnect from the Administration Server** en la ventana de propiedades del dispositivo no son compatibles con dispositivos móviles.

Para ajustar la configuración de sincronización para dispositivos Android, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **Android** y vaya a la sección **KES for Android settings**.
4. En la tarjeta **Scheduled synchronization**, haga clic en **Settings**.

   Se abrirá la ventana **Scheduled synchronization**.
5. Habilite la sincronización con el interruptor **Scheduled synchronization**.
6. En la lista desplegable **Synchronization period**, seleccione el período entre las sincronizaciones de dispositivos con Kaspersky Security Center. El valor predeterminado es 3 horas.

7. Para deshabilitar la sincronización de dispositivos con Kaspersky Security Center en itinerancia, seleccione la casilla **Do not synchronize while roaming**.

   El usuario del dispositivo puede seguir realizando la sincronización manualmente en la configuración de la aplicación (**Configuración** → **Configuración de la aplicación** → **Sincronización** → **Sincronizar**).

8. Haga clic en **Aceptar**.

9. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center. Puede sincronizar manualmente el dispositivo móvil con un comando especial.

Para ajustar la configuración de sincronización para dispositivos iOS que operan en modo de protección básica:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **iOS** y vaya a la sección **KP for iOS settings**.

4. En la tarjeta **Scheduled synchronization**, haga clic en **Settings**.

   Se abrirá la ventana **Scheduled synchronization**.

5. Habilite la sincronización con el interruptor **Scheduled synchronization**.

6. En la lista desplegable **Synchronization period**, seleccione el período entre las sincronizaciones de dispositivos con Kaspersky Security Center. El valor predeterminado es 6 horas.

7. Haga clic en **Aceptar**.

8. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

En algunos dispositivos iOS, la sincronización en segundo plano puede realizarse más tarde de lo esperado si el usuario sale de Kaspersky Protection para iOS deslizando el dedo hacia arriba en el Selector de aplicaciones. Para forzar la sincronización, el usuario debe volver a abrir la aplicación. Para obtener más información sobre las restricciones y recomendaciones relacionadas con la optimización de la ejecución de tareas en segundo plano, consulte la sección Problemas conocidos de Kaspersky Protection para iOS.

Para obtener más información sobre cómo configurar los ajustes de sincronización de los dispositivos iOS en los modos de funcionamiento de control básico y supervisado, consulte la sección Visualización de la lista de Servidores de MDM para iOS instalados y configuración de sus ajustes.

Administrar los certificados de dispositivos móviles

Kaspersky Next Expert View (on-premise) le permite emitir, renovar o eliminar certificados móviles, de correo o de VPN de dispositivos móviles.

Esta sección contiene información sobre cómo administrar certificados para dispositivos móviles y configurar sus reglas de emisión.

Reemitir el certificado del Servidor de administración móvil

Debe especificar un certificado de reserva del Servidor de administración móvil para cumplir con los requisitos de seguridad de su organización y mantener una conexión continua entre los dispositivos administrados y el Servidor de administración. Se vuelve a emitir un certificado móvil emitido por Kaspersky Security Center de manera predeterminada.

Le recomendamos que especifique un certificado de reserva al instalar el Servidor de administración o, a más tardar, 30 días antes de la caducidad del certificado existente. La hora exacta de caducidad está disponible en el campo **Expires** de la configuración del certificado (en el menú principal, seleccione → **General** → **Certificates**).

El período máximo de validez de cualquier certificado del Servidor de administración es de 397 días.

El certificado de reserva se entrega al dispositivo durante la sincronización y se convierte en el certificado principal inmediatamente después de que caduca el certificado existente. Si el certificado caduca y no se especificó ningún certificado de reserva, se perderá la conexión entre el Servidor de administración y Kaspersky Endpoint Security en los dispositivos administrados. En este caso, para volver a conectar los dispositivos, debe especificar un nuevo certificado y reinstalar Kaspersky Endpoint Security en cada uno de los dispositivos administrados.

Para volver a emitir el certificado del Servidor de administración con activación retrasada (para usar un certificado como certificado de reserva), siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), haga clic en el nombre del Servidor de administración.

2. En la ventana de propiedades del Servidor de administración que se abre, seleccione **General** → **Certificates**.

3. Si planea continuar usando el certificado emitido por Kaspersky Security Center, siga estos pasos:

   a. Haga clic en **Reissue**.

   b. En la ventana que se abre:

      1. En la sección **Connection address**, seleccione **Use old connection address** o **Change connection address to** si se usará una nueva dirección de conexión.

      2. En la sección **Activate new certificate**, seleccione **After this period expires, days** y especifique el número de días antes de que el certificado se active.

         Recomendamos especificar un período de activación del certificado de al menos 30 días para que todos los dispositivos tengan tiempo de recibir el certificado. Tenga en cuenta que el período especificado debe ser mayor que el período para sincronizar dispositivos con el Servidor de administración. Para obtener más información sobre cómo configurar la sincronización de dispositivos con el Servidor de administración, consulte la sección Configuración de la sincronización.

      3. Haga clic en **Aceptar**.

   Como alternativa, si planea usar su propio certificado personalizado:

   a. Compruebe si su certificado cumple con los requisitos de Kaspersky Security Center. Si es necesario, modifique el certificado.

   b. Seleccione la opción **Other certificate** y haga clic en el botón **Manage certificate**.

   c. En la ventana que se abre, haga clic en **Browse**.

   d. En la ventana que se abre, seleccione el tipo de certificado y luego especifique la ubicación y la configuración del certificado:

      - Si selecciona **PKCS #12**, haga clic en el botón **Browse** ubicado junto al campo **Certificate** y busque el archivo del certificado en su disco duro. Si el archivo del certificado está protegido con contraseña, ingrese la contraseña en el campo **Password**.

      - Si selecciona **X.509**, haga clic en el botón **Browse** ubicado junto al campo **Private key** y busque la clave privada en su disco duro. Si la clave privada está protegida con contraseña, ingrese la contraseña en el campo **Password**. Luego haga clic en el botón **Browse** al lado del campo **Certificate** y especifique la clave pública en su disco duro.

   e. En la sección **Activate new certificate**, seleccione **After this period expires, days** y especifique el número de días antes de que el certificado se active.

   f. Haga clic en **Guardar**.

   g. Haga clic en **Aceptar**.

   h. Haga clic en el botón **Guardar** para guardar los cambios que realizó.

El certificado se vuelve a emitir como certificado de reserva.

Para volver a emitir inmediatamente el certificado del Servidor de administración (no se recomienda si tiene dispositivos móviles administrados), siga estos pasos:

No seleccione **Immediately** si tiene dispositivos móviles administrados. Si selecciona esta opción, la conexión con todos los dispositivos administrados se perderá, ya que el nuevo certificado no se entregará a los dispositivos y el certificado anterior ya no será válido.

1. En la ventana principal de Kaspersky Next Expert View (on-premise), haga clic en el nombre del Servidor de administración.
2. En la ventana de propiedades del Servidor de administración que se abre, seleccione **General** → **Certificates**.
3. Si planea continuar usando el certificado emitido por Kaspersky Security Center, siga estos pasos:
   a. Haga clic en **Reissue**.
   b. En la ventana que se abre:
      1. En la sección **Connection address**, seleccione **Use old connection address** o **Change connection address to** si se usará una nueva dirección de conexión.
      2. En la sección **Activate new certificate**, seleccione **Immediately**.
      3. Haga clic en **Aceptar**.

   Como alternativa, si planea usar su propio certificado personalizado:

   a. Compruebe si su certificado cumple con los requisitos de Kaspersky Security Center. Si es necesario, modifique el certificado.
   b. Seleccione la opción **Other certificate** y haga clic en el botón **Manage certificate**.
   c. En la ventana que se abre, haga clic en **Browse**.
   d. En la ventana que se abre, seleccione el tipo de certificado y luego especifique la ubicación y la configuración del certificado:
      - Si selecciona **PKCS #12**, haga clic en el botón **Browse** ubicado junto al campo **Certificate** y busque el archivo del certificado en su disco duro. Si el archivo del certificado está protegido con contraseña, ingrese la contraseña en el campo **Password**.
      - Si selecciona **X.509**, haga clic en el botón **Browse** ubicado junto al campo **Private key** y busque la clave privada en su disco duro. Si la clave privada está protegida con contraseña, ingrese la contraseña en el campo **Password**. Luego haga clic en el botón **Browse** al lado del campo **Certificate** y especifique la clave pública en su disco duro.
   e. En la sección **Activate new certificate**, seleccione **Immediately**.
   f. Haga clic en **Guardar**.
   g. Haga clic en **Aceptar**.
   h. Haga clic en el botón **Guardar** para guardar los cambios que realizó.

El certificado se vuelve a emitir como el certificado principal del Servidor de administración.

Para obtener información detallada sobre los certificados, consulte la Ayuda de Kaspersky Security Center.

Configuración de las reglas de emisión de certificados

Kaspersky Next Expert View (on-premise) le permite configurar cómo se emiten, renuevan y protegen los certificados para dispositivos móviles.

Para configurar las reglas de emisión de certificados:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Certificates**.

2. En la lista de certificados que se abre, haga clic en **Issuance rules**.

   - En la sección **PKI settings**:

     a. En el bloque de configuración **Integration with PKI**, habilite el interruptor **Integrate issuance of certificates with Microsoft Certification Authority (CA) via PKI** para emitir certificados automáticamente después de la integración.

     Haga clic en **Select device** y, a continuación, especifique un dispositivo con el Agente de red instalado que se conectará a la CA de Microsoft.

     Para obtener información detallada sobre la PKI, consulte la sección Integración con la infraestructura de clave pública.

     b. En el bloque de configuración **Domain account for transmitting requests to issue certificates**, especifique el **PKI account name** (el nombre de la cuenta de usuario que se usará para la integración de PKI en el formato `userPrincipalName@DNSDomainName`) y la **Password** (la contraseña de dominio para la cuenta).

     c. Haga clic en **Guardar** para aplicar los cambios.

   - En la sección **Mobile certificates**, puede hacer lo siguiente:

     a. En el bloque de configuración **Validity**, en el campo **Certificate validity period (days)**, especifique la vida útil del certificado en días. La validez predeterminada de un certificado es de 365 días. Cuando caduque este período, el dispositivo móvil no podrá conectarse al Servidor de administración.

     b. En el bloque de configuración **Renewal**, en el campo **Renew certificate before it expires in (days)**, especifique el número de días que quedan hasta la caducidad del certificado actual cuando el Servidor de administración debe emitir un nuevo certificado. Por ejemplo, si el valor del campo es 4, el Servidor de administración emite un nuevo certificado cuatro días antes de que caduque el certificado actual. El valor predeterminado es 30.

     Seleccione la casilla **Renew certificate automatically** para renovar los certificados automáticamente. Si esta opción está deshabilitada, los certificados se deben renovar manualmente a medida que caducan. Esta casilla está marcada por defecto.

c. En el bloque de configuración **Password protection**, seleccione la casilla **Prompt for password during certificate installation** para solicitar al usuario una contraseña cuando el certificado se instale en un dispositivo móvil. La contraseña se usa solo una vez, durante la instalación del certificado en el dispositivo móvil. El Servidor de administración generará automáticamente la contraseña y se la enviará al usuario por correo electrónico. Puede especificar la longitud de la contraseña en el campo **Password length**.

> La protección con contraseña solo está disponible para certificados de celular.

d. Haga clic en **Guardar** para aplicar los cambios.

- En las secciones **Mail certificates** y **VPN certificates**, si la integración de PKI está configurada:

a. En el bloque de configuración **Renewal**, en el campo **Renew certificate before it expires in (days)**, especifique el número de días que quedan hasta la caducidad del certificado actual cuando el Servidor de administración debe emitir un nuevo certificado. Por ejemplo, si el valor del campo es 4, el Servidor de administración emite un nuevo certificado cuatro días antes de que caduque el certificado actual.

Seleccione la casilla **Renew certificate automatically** para renovar los certificados automáticamente. Si esta opción está deshabilitada, los certificados se deben renovar manualmente a medida que caducan. Esta casilla está marcada por defecto.

b. En el bloque **PKI settings**, especifique el **Certificate template name in PKI** (la plantilla de certificado que se utilizará para emitir certificados a los usuarios del dominio).

El servicio Agente de red para Windows instalado en un dispositivo que se conecta a la CA se ejecuta con la cuenta de usuario especificada. Este servicio es responsable de emitir los certificados de dominio de los usuarios. El servicio inicia cuando se carga la lista de plantillas de certificados haciendo clic en el botón **Refresh list** o cuando se genera un certificado.

> Al conectar el dispositivo móvil de un usuario que no es del dominio (con Android o iOS) a Kaspersky Security Center, el intento de emitir un certificado puede fallar.

c. En los bloques de configuración **Automatic issuance of mail certificate on device connection** y **Automatic issuance of VPN certificate on device connection**, seleccione las casillas **Issue for devices managed by Kaspersky Endpoint Security for Android** o **Issue for iOS MDM devices** para habilitar la emisión automática de un correo o certificado de VPN cuando los dispositivos se conectan a Kaspersky Security Center.

Si seleccionó la casilla **Issue for iOS MDM devices**, seleccione el alias del certificado en la lista desplegable. El alias del certificado es un nombre que identifica al certificado. Puede configurar el uso posterior del alias seleccionado para la emisión del certificado en las siguientes secciones de la directiva:

- Para certificados de correo: en las propiedades de la Cuenta de correo electrónico para dispositivos MDM con iOS y en las propiedades de la Cuenta Exchange ActiveSync para dispositivos MDM iOS.
- Para certificados VPN: en las propiedades de la Red VPN para dispositivos MDM con iOS y en las propiedades de la Red Wi-Fi para dispositivos MDM con iOS.

También puede cambiar el alias para certificados de correo electrónico y VPN individuales o múltiples; para ello, haga clic en **Modify alias** en la lista de certificados (**Asset management** → **Mobile** → **Certificates**).

d. Haga clic en **Guardar** para aplicar los cambios.

Kaspersky Security Center utilizará la configuración especificada para emitir, renovar y proteger a los

certificados de los dispositivos móviles.

Emitir certificados de dispositivos móviles

Puede emitir certificados móviles, de correo o VPN para los dispositivos móviles.

Para emitir un certificado, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Certificates**.

2. En la lista de certificados que se abre, haga clic en **Add**.

   Se inicia el Asistente de emisión de certificados. Haga clic en **Start** y luego avance por el asistente con los botones **Back** y **Next**.

Welcome

En la pantalla de bienvenida, puede leer un resumen de los pasos del Asistente de emisión de certificados.

> Tenga en cuenta que la numeración y el conjunto de pasos pueden variar según el tipo de certificado, el sistema operativo y la configuración de emisión definida en la sección **Issuance rules**.

Paso 1. Certificate type

En este paso, elija el certificado que se emitirá.

- **Mail certificate** (para configurar el correo electrónico corporativo en los dispositivos).
- **VPN certificate** (para configurar el acceso a redes privadas y recursos web corporativos en los dispositivos).
- **Mobile certificate** (para identificar dispositivos móviles en el Servidor de administración).

Paso 2. Operating system

En este paso, seleccione el sistema operativo de los dispositivos para los que se emitirá el certificado.

- **Android**
- **iOS**

Paso 3. Connection method

> Este paso solo se muestra si seleccionó **Mail certificate** o **VPN certificate** como el tipo de certificado y **Android** como el sistema operativo de los dispositivos para los cuales se emitirá el certificado.

En este paso, seleccione el método para conectar los dispositivos al Servidor de administración.

- **Connect using mobile certificate authentication**

  Seleccione esta opción si desea que el certificado móvil se utilice para identificar al usuario cuando se conecta al Servidor de administración.

- **Connect without mobile certificate authentication**

  Seleccione esta opción si desea instalar un certificado en un dispositivo sin autenticación de certificado.

  > Si hay un certificado para dispositivos móviles en el dispositivo, siempre se usará para la autenticación.

Paso 4. Users

En este paso, seleccione uno o más usuarios que recibirán los detalles para instalar certificados. Si un usuario no está en la lista, puede agregar una nueva cuenta de usuario sin salir del asistente.

- Para elegir un usuario existente, seleccione las casillas de verificación junto a los nombres de usuario correspondientes.
- Para agregar un nuevo usuario, haga clic en **Add user**.

  a. Especifique las credenciales de usuario en el bloque de configuración **Credentials**.

  - **User name**
  - **Password**

    La contraseña debe cumplir con los siguientes requisitos de complejidad:

    - La contraseña debe contener entre 8 y 16 caracteres.
    - Debe contener los caracteres de al menos tres de estos grupos: letras mayúsculas (AZ), letras minúsculas (az), dígitos (0-9), caracteres especiales (@ # $% ^ & * - _! + = [] { } |: ',.? / \ `~" ();).

  b. Si es necesario, especifique los detalles opcionales en el grupo de configuración **Optional information**.

  - **Full user name**
  - **Description**
  - **Email address**
  - **Phone number**

  c. Haga clic en **OK** para guardar los cambios.

  El nuevo usuario se agregará y se mostrará en la lista de usuarios.

- Para modificar los detalles del usuario, haga clic en **Edit user**.

Los campos que puede modificar dependen del subtipo de usuario: *interno* o *dominio*.

Paso 5. Certificate alias and source

En este paso, elija el alias del certificado y la fuente para importar el certificado.

- **Certificate alias**

  Un *alias de certificado* es un nombre que identifica el certificado. Puede usar el alias seleccionado más adelante para configurar los ajustes de la directiva: Cuenta de correo electrónico para dispositivos MDM con iOS; Cuenta de Exchange ActiveSync para dispositivos MDM con iOS; Red VPN para dispositivos MDM con iOS; Red Wi-Fi para dispositivos MDM con iOS.

  > Esta opción está disponible solo si seleccionó **Mail certificate** o **VPN certificate** como el tipo de certificado.

- **Integrate issuance with Microsoft CA via PKI**

  Para esta opción, especifique una de las plantillas disponibles importadas de la CA de Microsoft en el campo **PKI template**.

  > Esta opción solo está disponible si la integración con PKI está habilitada en las Reglas de emisión.

- **Upload file**

  Para esta opción, especifique el **Certificate format**:

  - Para el formato PKCS # 12, en el campo **Certificate file**, haga clic en **Seleccionar** y, a continuación, especifique un archivo P12 o PFX.

  - Para el formato X.509, en el campo **Private key file**, haga clic en **Seleccionar** y, a continuación, especifique un archivo PRK o PEM.

    En el campo **Certificate file**, haga clic en **Seleccionar** y, a continuación, especifique un archivo CER, CRT o CERT.

    Después de especificar los archivos, también puede ingresar la **Certificate password**.

Paso 6. Authentication method

> Este paso solo se muestra si seleccionó **Mobile certificate** como tipo de certificado o si seleccionó **Mail certificate** o **VPN certificate** para dispositivos Android y especificó la opción **Conectar sin autenticación de certificado móvil** como método de conexión.

En este paso, elija el método de autenticación de usuario para recibir el certificado.

- **Domain or internal user credentials**. Los usuarios accederán al certificado con las credenciales de usuario internas o de dominio. En dispositivos móviles, los usuarios deberán especificar el nombre de usuario en uno de los siguientes formatos:
  - `userPrincipalName@DNSDomainName`
  - `sAMAccountName`
  - `sAMADomain\sAMAccountName`
- **Password**. Los usuarios accederán al certificado con una contraseña enviada por correo electrónico o que se muestra después de completar el asistente.

En el bloque de configuración **Certificate use on device**, haga clic en la casilla **Allow using one certificate multiple times on the same device (only for devices with Kaspersky Endpoint Security for Android installed)** si desea permitir el uso de un certificado para dispositivos móviles varias veces en el mismo dispositivo.

> Esta opción solo está disponible si **Android** se elige como el sistema operativo de los dispositivos para los que se emitirá el certificado.

Paso 7. Send certificate details

En este paso, elija cómo enviar los detalles de instalación del certificado Puede seleccionar una de las siguientes opciones:

- **Send a message to users' email addresses**

  Elija esta opción para enviar los detalles de la instalación del certificado por correo electrónico a los usuarios seleccionados. Estas direcciones de correo electrónico deben especificarse en la configuración de la cuenta de usuario en Kaspersky Security Center.

  Si desea enviar los detalles de la instalación del certificado a una dirección de correo electrónico que no está especificada en la configuración de la cuenta de usuario en Kaspersky Security Center, seleccione la casilla **Send a copy of the message to an alternate email address** y luego especifique la dirección de correo electrónico requerida.

- **Show the details after completing the wizard**

  Elija esta opción para mostrar los detalles de la instalación del certificado en el paso final del asistente de emisión de certificados.

Paso 8. Confirm

En este paso, verifique los detalles de emisión del certificado especificados en los pasos anteriores y luego haga clic en **Confirmar y emitir certificado** para confirmar la operación.

Finish

En la pantalla Finalizar:

- Si elige la opción **Send a message to users' email addresses**, los usuarios especificados recibirán los correos electrónicos con los detalles de instalación del certificado.
- Si elige la opción **Show the details after completing the wizard**, los detalles de la instalación del certificado se muestran en la pantalla Finalizar. Puede ver los detalles que se muestran o hacer clic en **Download list** para recibir un archivo con información resumida.

Haga clic en **Cerrar** para salir del asistente.

Después de completar el asistente de emisión de certificados, los certificados se crean y se agregan a la lista de certificados de usuario. Puede eliminar o volver a emitir certificados, así como ver sus propiedades.

Renovar certificados de dispositivos móviles

Si uno de los certificados está a punto de caducar, puede renovarlo mediante Kaspersky Next Expert View (on-premise).

Si sigue los pasos a continuación, puede renovar un certificado móvil o un certificado de correo o VPN emitido a través de PKI.

Para renovar un certificado, haga lo siguiente:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Certificates**.
2. En la lista de certificados que se abre, seleccione el certificado que desea renovar y luego haga clic en **Renew**.

El estado del certificado cambia a **Certificate renewed**.

Eliminar certificados de dispositivos móviles

Puede eliminar los certificados de dispositivos móviles mediante Kaspersky Next Expert View (on-premise).

Tenga en cuenta que, si elimina un certificado para dispositivos móviles, el dispositivo ya no podrá sincronizarse con el Servidor de administración y no podrá administrarse a través de Kaspersky Security Center.

Cuando elimina un certificado, solo se elimina de Kaspersky Next Expert View (on-premise) y ya no se renueva, pero permanece en el dispositivo. Para eliminar un certificado de dispositivos MDM con iOS, dispositivos corporativos o dispositivos con contenedor corporativo, debe ejecutar el comando Eliminar datos corporativos. En dispositivos Android personales, los usuarios deben eliminar el certificado manualmente.

Cuando elimina un certificado para dispositivos móviles del dispositivo MDM con iOS, el dispositivo no se elimina de Kaspersky Next Expert View (on-premise), pero pierde la capacidad de sincronizarse con el Servidor de MDM para iOS y se le asigna el estado "Inactivo". En este caso, debe eliminar este dispositivo de la lista de dispositivos administrados en Kaspersky Next Expert View (on-premise) y luego volver a conectarlo mediante el Asistente de conexión de dispositivos móviles.

Para eliminar un certificado de Kaspersky Next Expert View (on-premise):

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Certificates**.

2. En la lista de certificados que se abre, seleccione el certificado que desea eliminar y luego haga clic en **Eliminar**.

El certificado se elimina y se quita de la lista de certificados.

Integración con la Infraestructura de Clave Pública (PKI)

Puede integrar la emisión de certificados con la entidad de certificación (CA) de Microsoft a través de una infraestructura de claves pública (PKI). La integración con una PKI está destinada principalmente a simplificar la emisión de certificados de usuario de dominio por parte del Servidor de administración. Una vez que se completa la integración, los certificados se emiten automáticamente.

Puede realizar la integración con una PKI con los ajustes indicados y designar la PKI como origen de certificados para tipos específicos de certificados. La configuración de integración de PKI especificada en las **Issuance rules** le permite establecer la plantilla predeterminada individual para todos los tipos de certificados.

Particularidades del uso de la integración PKI para la emisión de certificados:

- La integración de PKI está desactivada de forma predeterminada. Puede habilitarlo utilizando el interruptor **Integrate issuance of certificates with Microsoft Certification Authority (CA) via PKI**. Para obtener información detallada sobre cómo habilitar una PKI y configurar sus ajustes, consulte la sección Configurar reglas de emisión de certificados.

- La emisión de certificados se realiza mediante el Agente de red de Windows, que permite la integración entre el Servidor de administración y la CA de Microsoft. Como puede haber varios dispositivos con el Agente de red instalado, puede elegir el dispositivo que se conectará a la CA de Microsoft en las **Issuance rules**. Este dispositivo deberá tener un certificado de agente de inscripción (EA) instalado en el repositorio de certificados de la cuenta usada para la integración con la PKI. Este certificado es emitido por el administrador de la entidad de certificación (CA) del dominio.

- La cuenta con la que se realiza la integración con la PKI debe ser de un usuario de dominio y debe contar con el derecho *Iniciar sesión como servicio*.

- Kaspersky Security Center solo puede funcionar con una integración con PKI (CA de Microsoft) a la vez.

Para obtener información detallada sobre cómo configurar la integración con una PKI para emitir certificados, consulte la sección Configuración de reglas de emisión de certificados.

Configuración de la integración con PKI a través del Agente de red de Windows

Las estaciones de trabajo de dominio basadas en Windows no admiten la integración nativa con PKI. Por lo tanto, para habilitar la integración entre el Servidor de administración y la CA de Microsoft, debe configurar un host de Windows intermedio con el Agente de red instalado que dirigirá las solicitudes de dominio a la CA.

Para configurar Microsoft Active Directory y la CA para la integración de PKI, siga estos pasos:

1. Cree una cuenta de dominio bajo la cual se realizará la integración con PKI. Esta cuenta se utilizará para transmitir solicitudes a la CA de Microsoft a fin de emitir certificados.

   a. Ejecute secpol.msc.

   b. En la ventana que se abre, haga clic en **Directivas locales** → **Asignación de derechos de usuario** → **Permitir registro como servicio** para proporcionar el permiso *Iniciar sesión como servicio* a la cuenta de dominio.

2. Otorgue permiso a la cuenta de dominio para trabajar con la CA.

   a. En el lado del servidor que tiene la CA, abra el complemento de la CA certsrv.msc.

   b. Seleccione la CA y, a continuación, haga clic en **Propiedades**.

   c. En la pestaña **Seguridad**, haga clic en **Agregar** y luego especifique la cuenta de dominio creada anteriormente.

   d. Proporcione el permiso **Emitir y administrar certificados** para la cuenta de dominio.

   e. Aplique los cambios.

3. Agregue la plantilla de certificado del **Agente de inscripción** a la lista de certificados que se emitirán:

   a. En el complemento de la CA, haga clic con el botón derecho en **Plantillas de certificado** → **Nueva** → **Plantilla de certificado para emitir**.

   b. Seleccione la plantilla del **Agente de inscripción** y, a continuación, haga clic en **Aceptar**.

   c. Asegúrese de que el usuario del dominio tenga acceso a la plantilla de certificado:

      a. En el complemento certsrv.msc, haga clic en **Plantillas de certificado** → **Administrar**.

      b. En la ventana que se abre, haga clic en **Propiedades** → **Seguridad**.

      c. En la ventana que se abre, compruebe si el usuario tiene derecho de *lectura e inscripción*.

Para configurar la integración de PKI mediante un host de Windows intermedio con el Agente de red instalado, siga estos pasos:

1. Prepare un servidor que actuará como intermediario entre Kaspersky Security Center Linux y la CA.

   Debe ser un servidor de Windows en el mismo dominio que la CA.

2. Otorgue a la cuenta de dominio creada anteriormente el permiso para acceder a un servidor de Windows intermedio.

3. Inicie sesión en el servidor con la cuenta de dominio para crear un perfil de usuario permanente e instalar el certificado del Agente de inscripción:

   a. Inicie sesión en el host de Windows donde se implementará el Agente de red.

   b. Ejecute certmgr.msc como administrador.

c. Haga clic en **Personal** → **Todas las tareas** → **Solicitar nuevo certificado...** para iniciar el Asistente de inscripción de certificados.

Siga los pasos del asistente con la configuración predeterminada.

d. En el paso **Solicitar certificados**, seleccione el tipo de certificado **Agente de inscripción** y, a continuación, haga clic en **Inscribir**.

Una vez que el estado de la inscripción se establezca en "Realizada con éxito", haga clic en **Finalizar**.

> Si se producen errores, espere a que se apliquen las directivas en el host o verifique que los derechos de usuario en la configuración de Permisos para controladores de dominio estén configurados correctamente.

4. Proporcione el permiso *Iniciar sesión como servicio* a la cuenta de dominio en el host de Windows.

a. Ejecute secpol.msc.

b. En la ventana que se abre, haga clic en **Directivas locales** → **Asignación de derechos de usuario** → **Permitir registro como servicio**.

5. Instale el Agente de red Windows. Para obtener información detallada sobre la instalación, consulte la Ayuda de Kaspersky Security Center.

- Instale el Agente de red con los valores predeterminados, excepto la dirección del Servidor de administración. Asegúrese de que el puerto 13000 esté abierto en el host que tiene Kaspersky Security Center instalado.
- Asegúrese de que la conexión con el host de Windows esté establecida (en Kaspersky Next Expert View (on-premise), haga clic en **Asset management** → **Unassigned devices**).
- Espere 15 minutos hasta que se establezca la primera sincronización programada del Agente de red con Kaspersky Security Center.

Ver la lista de certificados de dispositivos móviles

Kaspersky Next Expert View (on-premise) le permite ver los certificados para dispositivos móviles creados y sus propiedades.

Para ver la lista de todos los certificados y sus propiedades, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Certificates**.
2. En la ventana que se abre, puede ver la lista de todos los certificados creados y sus propiedades en la tabla.

Para ver las propiedades de un certificado individual, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Certificates**.
2. En la lista de certificados que se abre, seleccione el certificado cuyas propiedades quiera ver.

3. En la ventana **Certificate details**, vea las propiedades del certificado:

   - **User name**
   - **Status**
   - **Type**
   - **Protocol**
   - **Source**
   - **Expiration date**
   - **Issue date**
   - **Latest status update**
   - **Alias**
   - **Automatic renewal enabled**
   - **Thumbprint**

Para ver los certificados instalados en un dispositivo MDM con iOS, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.
2. En la lista de dispositivos móviles que se abre, seleccione el dispositivo cuyos certificados desea ver.
3. En la ventana de propiedades del dispositivo que se abre, seleccione la sección **Certificates**.

   Se muestra la lista de certificados instalados en el dispositivo y sus propiedades.

   - **Certificate name**
   - **User certificate**
   - **Certificate thumbprint**

Configuración y administración

Esta sección está destinada a los especialistas que administran MDM básico en Kaspersky Next Expert View (on-premise), así como a los especialistas que brindan soporte técnico a las organizaciones que lo utilizan.

Control

Esta sección contiene información sobre cómo supervisar dispositivos móviles de forma remota en Kaspersky Next Expert View (on-premise).

Configuración de restricciones

Esta sección proporciona instrucciones sobre cómo configurar el acceso del usuario a las funciones de dispositivos móviles.

Configuración de restricciones para dispositivos Android personales

Estas configuraciones se aplican a dispositivos personales y dispositivos con un contenedor corporativo.

Para mantener un dispositivo Android seguro, Kaspersky Mobile Devices Protection and Management le permite configurar el acceso de los usuarios a las siguientes funciones de los dispositivos móviles:

- Wi-Fi
- Cámara
- Bluetooth

De forma predeterminada, el usuario puede usar el Wi-Fi, la cámara y el Bluetooth en el dispositivo sin restricciones.

Para configurar las restricciones de utilización de Wi-Fi, de la cámara y de Bluetooth en el dispositivo:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **Android** y vaya a la sección **Restrictions**.
4. En la tarjeta **Device feature restrictions**, haga clic en **Settings**.

   Se abre la ventana **Device feature restrictions**.
5. Habilite la configuración con el interruptor **Device feature restrictions**.
6. Configurar el uso de Wi-Fi, cámara y Bluetooth:
   - Para deshabilitar el módulo Wi-Fi en el dispositivo móvil del usuario, active la casilla **Prohibit use of Wi-Fi**.

     En dispositivos personales y dispositivos con un contenedor corporativo que ejecuta Android 10 o versiones posteriores, no se admite la prohibición del uso de redes Wi-Fi.
   - Para deshabilitar la cámara en el dispositivo móvil del usuario, active la casilla **Prohibit use of camera**.

     Cuando el uso de la cámara está prohibido, la aplicación muestra una notificación al abrirla y la cierra poco después. En dispositivos Asus y OnePlus, la notificación se muestra en pantalla completa. El usuario del dispositivo puede tocar el botón **Cerrar** para salir de la aplicación.

En dispositivos con Android 11 o versiones posteriores, Kaspersky Endpoint Security para Android debe estar configurado como una función de Accesibilidad. Kaspersky Endpoint Security para Android solicita al usuario que configure la app como una función de Accesibilidad a través del Asistente de configuración inicial. El usuario puede omitir este paso o desactivar este servicio más adelante en los ajustes del dispositivo. Si este es el caso, no podrá restringir el uso de la cámara.

- Para deshabilitar el Bluetooth en el dispositivo móvil del usuario, active la casilla **Prohibit use of Bluetooth**.

  En Android 12 o versiones posteriores, puede desactivarse el uso de Bluetooth solo si el usuario del dispositivo otorgó el permiso **Dispositivos cercanos**. El usuario puede otorgar este permiso durante el Asistente de configuración inicial o posteriormente.

  En dispositivos personales con Android 13 o una versión posterior, el uso de Bluetooth no se puede deshabilitar.

7. Haga clic en **Aceptar**.
8. Haga clic en el botón **Save** para guardar los cambios que realizó.

   La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

También puede restringir funciones adicionales del sistema operativo en dispositivos corporativos.

Configuración de restricciones para dispositivos MDM con iOS

Para garantizar conformidad con los requisitos de seguridad corporativa, configure restricciones al funcionamiento de los dispositivos MDM con iOS.

Las funciones permitidas en la sección **Restrictions** de la directiva pero prohibidas en los perfiles de configuración instalados en los dispositivos no están disponibles en los dispositivos.

Configuración de restricciones para las funciones

Para configurar restricciones de funciones de dispositivos iOS con MDM:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **iOS** y vaya a la sección **Restrictions**.
4. En la tarjeta **Device feature restrictions**, haga clic en **Settings**.

   Se abre la ventana **Device feature restrictions**.
5. Habilite la configuración con el interruptor **Device feature restrictions**.

6. Habilite las restricciones de funciones del dispositivo MDM con iOS usando los interruptores en las pestañas correspondientes y seleccione las restricciones requeridas.

Lista de restricciones de funciones del dispositivo

- Restricciones en la pestaña **General**:
  - En la sección **Device settings**:
    - **Prohibit voice dial on a locked device**

      Uso de la función de marcación por voz en un dispositivo móvil bloqueado.

      Si la casilla está desactivada, el usuario puede utilizar comandos de voz para marcar números de teléfono en un dispositivo móvil bloqueado.

      Si la casilla está marcada, el usuario no puede utilizar comandos de voz para marcar números de teléfono en un dispositivo móvil bloqueado.

      Esta casilla está desactivada por defecto.

    - **Limit ad tracking**

      Uso de la tecnología IFA (Identifier for advertisers) para llevar un seguimiento de sitios web visitados y aplicaciones iniciadas en el dispositivo MDM de iOS. IFA permite configurar el seguimiento de anuncios en el dispositivo móvil de acuerdo con los intereses del usuario.

      Si la casilla está seleccionada, la tecnología IFA se deshabilita en el dispositivo del usuario.

      Si la casilla está desactivada, la tecnología se activa IFA en el dispositivo móvil y realiza un seguimiento de los sitios web visitados y aplicaciones iniciadas para mostrar anuncios personalizados.

      Esta casilla está desactivada por defecto.

    - **Prohibit Handoff**

      Uso de la función Handoff en el dispositivo móvil del usuario. Handoff le permite empezar a trabajar con datos en un dispositivo Apple, luego cambiar a otro dispositivo Apple y continuar trabajando con esos datos.

      Si la casilla no está marcada, Handoff está disponible para el usuario.

      Si la casilla está marcada, Handoff no está disponible.

      Esta casilla está desactivada por defecto.

    - **Prohibit editing device name**

      Habilidad de modificar el nombre del dispositivo móvil.

      Si la casilla no está marcada, el usuario puede editar el nombre del dispositivo móvil.

      Si la casilla está marcada, el nombre del dispositivo no se puede editar.

      Esta casilla está desactivada por defecto.

    - **Prohibit modifying restrictions**

      Habilidad de ajustar la configuración de restricciones en el dispositivo móvil. El usuario puede usar las restricciones para configurar las funciones del control parental en el dispositivo móvil. El usuario puede restringir funciones del dispositivo (por ejemplo, bloquear el uso de la cámara), el acceso a contenido multimedia (por ejemplo, configurar restricciones de edad para la visualización de películas), el uso de aplicaciones (por ejemplo, bloquear el uso de iTunes Store) y configurar otras restricciones.

      Si la casilla no está marcada, el usuario puede ajustar la configuración de restricciones en el dispositivo móvil.

      Si la casilla está marcada, no es posible configurar restricciones en el dispositivo móvil.

Esta casilla está desactivada por defecto.

- **Prohibit Spotlight suggestions**

  Uso de los resultados de búsqueda en Internet de Spotlight en las sugerencias de Siri. Al usar las sugerencias de Spotlight, las consultas de búsqueda y sus datos de usuario asociados se envían a Apple.

  Si la casilla no está marcada, el usuario puede permitir que se muestren los resultados de la búsqueda en Internet de Spotlight en las sugerencias de Siri.

  Si la casilla está marcada, los resultados de la búsqueda en Internet de Spotlight no están disponibles en las sugerencias de Siri. Los datos de usuario no se envían a Apple.

  El usuario puede habilitar los resultados de búsqueda en Internet de Spotlight en las sugerencias de Siri incluso si la casilla está marcada. Esto se debe a un problema reconocido por Apple.

  Esta casilla está desactivada por defecto.

- En la sección **Data loss protection**:

  - **Prohibit screenshots and screen recording**

    Capacidad de tomar una captura de pantalla o vídeo desde la pantalla del dispositivo de MDM de iOS.

    Si la casilla está desactivada, el usuario puede realizar y guardar capturas de pantalla o vídeos desde la pantalla del dispositivo móvil.

    Si la casilla está marcada, el usuario no puede realizar ni guardar capturas de pantalla o vídeos desde la pantalla del dispositivo móvil.

    Esta casilla está desactivada por defecto.

  - **Prohibit non-managed apps from using documents from managed apps**

    Posibilidad de utilizar aplicaciones no gestionadas (personales) del dispositivo MDM de iOS para abrir los documentos creados utilizando aplicaciones y cuentas gestionadas (corporativas). Las aplicaciones no gestionadas son aplicaciones instaladas, configuradas y gestionadas por el usuario del dispositivo móvil.

    Si la casilla está desactivada, el usuario puede usar aplicaciones no administradas para abrir documentos creados en aplicaciones corporativas administradas.

    Si la casilla está marcada, el usuario no puede usar aplicaciones no administradas para abrir documentos creados con aplicaciones administradas. Por ejemplo, esta configuración impide que un archivo adjunto de correo electrónico confidencial de una cuenta de correo electrónico administrada se abra en las aplicaciones personales del usuario.

    Esta casilla está desactivada por defecto.

  - **Prohibit managed apps from using documents from non-managed apps**

    Posibilidad de utilizar aplicaciones gestionadas (corporativas) en el dispositivo MDM de iOS para abrir documentos creados utilizando aplicaciones no gestionadas (personales) y cuentas del usuario. Las aplicaciones no gestionadas son aplicaciones instaladas, configuradas y gestionadas por el usuario del dispositivo móvil.

    Si la casilla está desactivada, el usuario puede usar aplicaciones administradas para abrir documentos creados con aplicaciones no administradas.

    Si la casilla está marcada, el usuario no puede usar aplicaciones administradas para abrir documentos creados con aplicaciones no administradas. Por ejemplo, esta configuración evita que un documento de una cuenta personal de iCloud se abra en una app corporativa.

Esta casilla está desactivada por defecto.

- **Restringir copiar y pegar entre apps administradas y no administradas**

  Restringe la funcionalidad de copiar y pegar cuando se selecciona al menos una de las siguientes casillas:

  - **Prohibit non-managed apps from using documents from managed apps**
  - **Prohibit managed apps from using documents from non-managed apps**

  Si la casilla está marcada, el usuario del dispositivo no puede usar el portapapeles.

  Si la casilla no está marcada, el usuario del dispositivo puede usar el portapapeles.

  Esta casilla está desactivada por defecto.

  Cuando se selecciona esta casilla, varias combinaciones de las restricciones **Prohibit non-managed apps from using documents from managed apps** y **Prohibit managed apps from using documents from non-managed apps** tienen efectos diferentes en términos de la capacidad del usuario para usar el portapapeles.

Prohibit non-managed apps from using documents from managed apps	Prohibit managed apps from using documents from non-managed apps	Restricción de las funciones
Habilitado	Habilitado	El usuario no puede copiar y pegar datos.
Habilitado	Deshabilitado	El usuario puede copiar datos de aplicaciones administradas y pegar datos en aplicaciones no administradas. El usuario no puede copiar datos de aplicaciones no administradas y pegar datos en aplicaciones administradas.
Deshabilitado	Habilitado	El usuario puede copiar datos de aplicaciones no administradas y pegar datos en aplicaciones administradas. El usuario no puede copiar datos de aplicaciones administradas y pegar datos en aplicaciones no administradas.
Deshabilitado	Deshabilitado	El usuario puede copiar datos de aplicaciones administradas y pegar datos en aplicaciones no administradas. El usuario puede copiar datos de aplicaciones no administradas y pegar datos en aplicaciones administradas.

- **Disable encryption of backup copies**

  Cifrado de las copias de seguridad de los datos del dispositivo de MDM de iOS en la aplicación iTunes instalada en el equipo del usuario.

  Si la casilla está desactivada, cuando se crea una copia de seguridad de los datos del dispositivo móvil en la aplicación iTunes, los datos se cifran y se protegen automáticamente con una contraseña. En este caso, el usuario no puede cifrar copias de seguridad de los datos del dispositivo en la app iTunes.

  Si la casilla está marcada, el usuario puede elegir si desea utilizar el cifrado de copias de seguridad en la aplicación iTunes.

  Esta casilla está desactivada por defecto.

- **Prohibit reset to factory settings**

  Habilidad para eliminar todos los datos del dispositivo y restablecer los ajustes de fábrica.

  Si la casilla no está marcada, el usuario puede borrar todos los datos del dispositivo y restablecer la los ajustes de fábrica.

  Si la casilla está marcada, la opción para restablecer los ajustes de fábrica no está disponible.

Esta casilla está desactivada por defecto.

- **Prohibit modifying account settings**

  Opción que permite al usuario añadir nuevas cuentas (como cuentas de correo electrónico) y editar la configuración de la cuenta en el dispositivo MDM de iOS.

  Si la casilla de verificación no está seleccionada, el usuario del dispositivo móvil puede agregar nuevas cuentas y editar la configuración de las cuentas existentes.

  Si la casilla de verificación está seleccionada, no se permite al usuario del dispositivo móvil agregar nuevas cuentas ni editar la configuración de las cuentas existentes.

  Esta casilla está desactivada por defecto.

- En la sección **Security and privacy**:

  - **Prohibit sending diagnostic and personal data to Apple**

    Recepción automática de datos e información de diagnóstico sobre el uso del dispositivo MDM de iOS y la transmisión de un informe con estos datos a Apple para su análisis.

    Si la casilla está desactivada, después de mostrarse una advertencia, el usuario puede permitir la transmisión de informes con datos e información de diagnóstico sobre el uso del dispositivo móvil a Apple.

    Si la casilla está marcada, se bloquea la transmisión de informes con datos de diagnóstico e información sobre el uso del dispositivo móvil a Apple.

    Esta casilla está desactivada por defecto.

  - **Prohibit changing password**

    Habilidad de configurar, cambiar o eliminar la opción Desbloquear contraseña del dispositivo móvil.

    Si la casilla no está marcada, el usuario puede configurar, cambiar o eliminar la contraseña usada para desbloquear el dispositivo móvil.

    Si la casilla está marcada, la administración de Desbloquear contraseña del dispositivo no está disponible.

    Esta casilla está desactivada por defecto.

  - **Prohibit modifying Touch ID and Face ID settings**

    Habilidad de agregar y eliminar huellas digitales de Touch ID y datos de Face ID.

    Si la casilla no está marcada, el usuario puede agregar y eliminar huellas dactilares de Touch ID o datos de Face ID.

    Si la casilla está marcada, la administración de la huella digital de Touch ID o de datos correspondientes a Face ID no está disponible.

    Esta casilla está desactivada por defecto.

  - **Prohibit device unlock using Touch ID and Face ID**

    Touch ID y Face ID hacen posible utilizar una huella dactilar o reconocimiento facial como contraseña para desbloquear el dispositivo MDM de iOS. Touch ID y Face ID también se pueden usar para autenticar compras mediante Apple Pay, iTunes Store, App Store y Book Store, así como para iniciar sesión en aplicaciones.

    Si la casilla de verificación está desactivada, el usuario puede utilizar una huella dactilar o reconocimiento facial en lugar de ingresar una contraseña para desbloquear el dispositivo móvil.

    Si se selecciona esta casilla de verificación, el usuario puede usar Touch ID o Face ID para desbloquear el dispositivo móvil.

Esta casilla está desactivada por defecto.

- **Prompt for password for each purchase on iTunes Store**

  Uso de la contraseña de restricción para comprar contenido multimedia en iTunes Store.

  Si la casilla está marcada, antes de hacer la primera compra mediante iTunes Store, el usuario tiene que especificar una contraseña de restricción en la configuración de la restricción de compras y utilizarla posteriormente para evitar compras accidentales o no autorizadas. Una vez verificada la cuenta al realizar una compra, la contraseña de restricciones no se pedirá de nuevo durante los próximos 15 minutos.

  Si la casilla está desmarcada, no se requiere que el usuario ingrese la contraseña de restricción antes de realizar compras en iTunes Store.

  Esta casilla está desactivada por defecto.

- **Prompt for password on first connection via AirPlay**

  Usar una contraseña al conectar el dispositivo móvil MDM de iOS a los dispositivos compatibles con AirPlay. La contraseña se utiliza para la transmisión segura de contenido multimedia.

  Si la casilla de verificación está seleccionada, antes de la primera conexión del dispositivo móvil a los dispositivos compatibles con AirPlay, el usuario tiene que especificar la contraseña en la configuración de seguridad de AirPlay e ingresarla posteriormente.

  Si la casilla está desactivada, el usuario puede decidir si utilizar una contraseña al conectar el dispositivo móvil a los dispositivos compatibles con AirPlay.

  Esta casilla está desactivada por defecto.

- **Prohibit installing configuration profiles**

  Uso de perfiles de configuración adicionales en el dispositivo con MDM de iOS.

  Si la casilla no está marcada, el usuario puede instalar perfiles de configuración adicionales en el dispositivo móvil.

  Si la casilla está marcada, el usuario no puede instalar perfiles de configuración adicionales en el dispositivo móvil.

  Esta casilla está desactivada por defecto.

- **Prohibit non-Configurator hosts**

  Protección del dispositivo de MDM de iOS contra conexiones de terceros. Una conexión de terceros es una conexión a otros dispositivos o la sincronización con servicios de Apple, como iTunes.

  Si la casilla está desactivada, el usuario puede sincronizar el dispositivo MDM de iOS con otros dispositivos y servicios de Apple.

  Si la casilla está marcada, en el dispositivo móvil del usuario se bloquearán los hosts no especificados en el configurador.

  Esta casilla está desactivada por defecto.

- **Prohibit modifying settings for sending diagnostic data**

  Recepción automática de datos e información de diagnóstico sobre el uso del dispositivo MDM de iOS y la transmisión de un informe con estos datos a Apple para su análisis.

  Si la casilla no está marcada, el usuario puede configurar el envío de informes que contienen información de diagnóstico y datos de uso del dispositivo móvil a Apple.

  Si la casilla está marcada, la configuración para el envío de informes que contienen información de diagnóstico no está disponible.

  Esta casilla está desactivada por defecto.

- En la sección **iCloud**:
  - **Prohibit backup in iCloud**

    Copia de seguridad automática de datos desde el dispositivo con MDM de iOS a iCloud. Las copias de los datos que ya están almacenados en iCloud no se crean durante el proceso de respaldo. Tampoco se crean copias de contenido multimedia que se recibió al sincronizar el dispositivo con una computadora y que no se compraron en iTunes Store.

    Si la casilla está desactivada, el usuario puede guardar las copias de seguridad de los datos del dispositivo móvil en iCloud. Las copias de seguridad de los datos se guardan en iCloud a diario cuando el dispositivo está habilitado, bloqueado y conectado a una fuente de alimentación.

    Si la casilla está marcada, el usuario no puede guardar las copias de seguridad de los datos del dispositivo móvil en iCloud.

    Esta casilla está desactivada por defecto.

  - **Prohibit storing documents and data in iCloud**

    Copia de seguridad automática de documentos en iCloud. Los documentos de iCloud se pueden abrir y editar en otros dispositivos en los que está configurado el servicio de iCloud.

    Si la casilla no está marcada, el usuario puede guardar documentos en iCloud, abrirlos y editarlos en otros dispositivos en aplicaciones compatibles con iCloud (por ejemplo, TextEdit).

    Si la casilla está marcada, no se permite al usuario guardar documentos en iCloud.

    Esta casilla está desactivada por defecto.

  - **Prohibit iCloud Keychain**

    Sincronización automática de las credenciales de las cuentas de un usuario de un dispositivo MDM de iOS con otros dispositivos Apple del usuario. Los datos sincronizados se guardan en el llavero de iCloud. Los datos del llavero de iCloud están cifrados. El llavero de iCloud permite guardar los siguientes datos en iCloud:

    - Cuentas de sitios web
    - Números y fechas de caducidad de tarjeta de crédito
    - Contraseñas de redes inalámbricas

    Si la casilla está desactivada, el usuario puede sincronizar datos de las cuentas con otros dispositivos de Apple del usuario.

    Si la casilla está marcada, no se permite al usuario utilizar el Llavero de iCloud en el dispositivo móvil.

    Esta casilla está desactivada por defecto.

  - **Prohibit managed apps from storing data in iCloud**

    Creación de una copia de seguridad de los datos de aplicaciones administradas en iCloud.

    Si la casilla no está marcada, el usuario puede almacenar los datos de aplicaciones administradas en iCloud.

    Si la casilla está marcada, el usuario no puede almacenar datos corporativos en iCloud.

    Esta casilla está desactivada por defecto.

  - **Prohibit backup of enterprise books**

    Copia de seguridad de libros de la empresa con iCloud o iTunes. Puede proporcionar acceso a libros de la empresa si los coloca en el servidor web corporativo.

Si la casilla no está marcada, la copia de seguridad de los libros de la empresa con iCloud o iTunes está disponible para el usuario.

Si la casilla está marcada, la copia de seguridad de los libros de la empresa no está disponible.

Esta casilla está desactivada por defecto.

- **Prohibit synchronizing notes and highlights in enterprise books**

  Habilidad de sincronizar notas, favoritos y fragmentos destacados en los libros de la empresa con iCloud.

  Si la casilla no está marcada, el usuario puede sincronizar notas, favoritos y fragmentos destacados en los libros de empresa. Los cambios estarán disponibles en todos los dispositivos de Apple que usen iCloud del usuario.

  Si la casilla está marcada, las notas, los favoritos y los fragmentos destacados solo estarán disponibles en este dispositivo móvil.

  Esta casilla está desactivada por defecto.

- **Prohibit iCloud photo sharing**

  Uso de la función Compartir fotos de iCloud en el dispositivo MDM de iOS para conceder acceso a otros usuarios a las fotos y los vídeos en el servidor de iCloud. Los otros usuarios deben tener configurada la función Compartir fotos de iCloud.

  Si la casilla está desactivada, la función de compartir fotos en iCloud estará disponible para el usuario. Los usuarios de otros dispositivos pueden ver las fotos y los videos del usuario, dejar comentarios y agregar sus propias fotos y videos. El usuario también puede acceder a los datos de otros usuarios en el servidor de iCloud.

  Si la casilla está marcada, la función de compartir fotos en iCloud no estará disponible para el usuario. El usuario no puede conceder a otros usuarios acceso a sus fotos y vídeos en el servidor de iCloud, ni acceder a los datos de otros usuarios en dicho servidor.

  Esta casilla está desactivada por defecto.

- **Prohibit iCloud Media Library**

  Uso de la función Biblioteca multimedia de iCloud para cargar de forma automática las fotos y los videos del dispositivo móvil MDM con iOS a otros dispositivos Apple del usuario.

  Si la casilla no está marcada, la función Biblioteca multimedia de iCloud está disponible para el usuario cuando trabaja con la aplicación Fotos.

  Si la casilla está marcada, la función Biblioteca multimedia de iCloud no está disponible para el usuario. Las fotos y los videos del usuario guardados en la Biblioteca multimedia de iCloud se eliminan del servidor iCloud.

  Esta casilla está desactivada por defecto.

- En la sección **Certificates**:

  - **Prohibit users from accepting untrusted TLS certificates**

    Uso de certificados TLS no fiables para proporcionar un canal de comunicaciones cifrado entre las aplicaciones del dispositivo MDM de iOS (Mail, Contactos, Calendario o Safari) y los recursos corporativos.

    Si la casilla está desactivada, el usuario puede permitir el uso de un certificado TLS no confiable después de mostrarse una advertencia.

    Si la casilla está marcada, se bloquea el uso de certificados TLS no fiables.

    Esta casilla está desactivada por defecto.

- **Prohibit automatic updates of trusted certificates**

  Actualizaciones automáticas de certificados de confianza en el dispositivo MDM de iOS.

  Si la casilla está desactivada, los cambios hechos en la configuración de confianza de un certificado no se aplican automáticamente.

  Si la casilla está marcada, los cambios en la configuración de la confianza de un certificado no se aplican automáticamente. Después de que se le muestre una advertencia, el usuario puede optar por aplicar cambios a la configuración de confianza del certificado.

  Esta casilla está desactivada por defecto.

- Restricciones en la pestaña **Apps**:

  - En la sección **General**:

    - **Prohibit use of camera**

      Uso de la cámara en el dispositivo móvil del usuario.

      Si la casilla está desactivada, se permite al usuario utilizar la cámara del dispositivo.

      Si la casilla de verificación está seleccionada, se deshabilita el uso de la cámara del dispositivo. El usuario no puede tomar fotos, grabar videos ni usar la app FaceTime. El ícono de la cámara en la pantalla de inicio del dispositivo está oculto.

      Esta casilla está desactivada por defecto.

    - **Prohibit FaceTime**

    - **Prohibit iMessage**

      Uso del servicio iMessage en el dispositivo móvil del usuario.

      Si la casilla no está marcada, el usuario puede enviar y recibir mensajes con iMessage.

      Si la casilla está marcada, el servicio iMessage no está disponible en el dispositivo móvil. El usuario no puede enviar ni recibir mensajes a través de iMessage.

      Esta casilla está desactivada por defecto.

    - **Prohibit Book Store**

      Acceso a Books Store desde la aplicación Apple Books en el dispositivo móvil del usuario.

      Si la casilla está desactivada, el usuario puede visitar Book Store desde la aplicación Apple Books instalada en el dispositivo.

      Si la casilla está marcada, el usuario no puede visitar Books Store desde la aplicación Apple Books.

      Esta casilla está desactivada por defecto.

    - **Prohibit installation of apps from Apple Configurator and iTunes**

      El usuario puede instalar aplicaciones de manera independiente en un dispositivo MDM de iOS.

      Si la casilla está desactivada, el usuario puede instalar o actualizar apps de forma independiente en un dispositivo móvil desde App Store mediante iTunes o Apple Configurator.

      Si la casilla está marcada, el usuario no puede instalar o actualizar apps de desde App Store mediante iTunes o Apple Configurator en un dispositivo móvil. La instalación y las actualizaciones solo están disponibles para aplicaciones corporativas. El icono de la App Store está oculto en la pantalla principal del dispositivo MDM de iOS.

      Esta casilla está desactivada por defecto.

- **Prohibit installation of apps from the App Store**

  Habilidad de instalar independientemente aplicaciones en un dispositivo móvil desde App Store. La casilla está disponible si la casilla **Prohibit installation of apps from Apple Configurator and iTunes** no está marcada.

  Si la casilla no está marcada, el usuario puede instalar y actualizar aplicaciones independientemente desde App Store.

  Si la casilla está marcada, el usuario no puede instalar ni actualizar aplicaciones desde App Store en el dispositivo móvil. El icono de la App Store está oculto en la pantalla principal del dispositivo MDM de iOS.

  Esta casilla está desactivada por defecto.

- **Prohibit automatic app downloads**

  Uso de descargas automáticas de aplicaciones en el dispositivo móvil del usuario. La casilla está disponible si la casilla **Prohibit installation of apps from Apple Configurator and iTunes** no está marcada.

  Si la casilla no está marcada, las descargas automáticas de aplicaciones están disponibles para el usuario. Después de que esta función se habilita, las aplicaciones que el usuario descargó desde App Store se descargan automáticamente en los otros dispositivos Apple del usuario.

  Si la casilla está marcada, las descargas automáticas de aplicaciones están deshabilitadas y no disponibles.

  Esta casilla está desactivada por defecto.

- **Prohibit in-app purchases**

  Uso del sistema de compras en las apps en el dispositivo móvil.

  Si la casilla está desactivada, el usuario puede hacer compras en las aplicaciones instaladas en el dispositivo móvil.

  Si la casilla está marcada, el usuario no puede hacer compras en las aplicaciones instaladas en el dispositivo móvil.

  Esta casilla está desactivada por defecto.

- **Prohibit trusting new enterprise developers**

  Habilidad de configurar la confianza de las aplicaciones corporativas en un dispositivo móvil. Puede desarrollar aplicaciones corporativas y distribuirlas entre empleados para el uso interno. Para trabajar con una aplicación corporativa, el usuario del dispositivo móvil debe hacerlo con una aplicación de confianza.

  Si la casilla no está marcada, el usuario puede configurar la confianza en las aplicaciones corporativas.

  Si la casilla está marcada, el usuario no puede configurar el nivel de confianza para aplicaciones corporativas al instalar una aplicación manualmente.

  Esta casilla está desactivada por defecto.

- **Prohibit removing apps**

  Esta opción permite eliminar apps del dispositivo móvil.

  Si la casilla está desactivada, el usuario puede eliminar del dispositivo las aplicaciones instaladas mediante App Store o iTunes.

  Si la casilla está marcada, el usuario no puede eliminar del dispositivo móvil las apps instaladas mediante App Store o iTunes.

  Esta casilla está desactivada por defecto.

- En la sección **AirPrint**:
  - **Prohibit AirPrint**

    Seleccione o desmarque esta casilla para especificar si el usuario del dispositivo puede usar AirPrint.

    La casilla está desactivada de manera predeterminada.

  - **Prohibit storing AirPrint credentials**

    Seleccione o desmarque esta casilla para especificar si el usuario del dispositivo puede almacenar un llavero con el nombre de usuario y la contraseña para AirPrint.

    La restricción es compatible con dispositivos con iOS 11 y versiones posteriores.

    La casilla está desactivada de manera predeterminada.

  - **Prohibit iBeacon discovery of AirPrint printers**

    Seleccione o desmarque esta casilla para especificar si la detección de impresoras AirPrint por iBeacon está habilitada. Deshabilitar la detección de impresoras AirPrint por iBeacon evita que balizas Bluetooth de AirPrint falsas obtengan información sobre el tráfico de la red.

    La restricción es compatible con dispositivos con iOS 11 y versiones posteriores.

    La casilla está desactivada de manera predeterminada.

  - **Force AirPrint to use a trusted TLS certificate**

    Seleccione o desmarque esta casilla para especificar si se requiere un certificado de confianza para la comunicación de impresión TLS.

    La restricción es compatible con dispositivos con iOS 11 y versiones posteriores.

    La casilla está desactivada de manera predeterminada.

- En la sección **AirDrop**:
  - **Prohibit AirDrop**

    Usar la función AirDrop para transmitir datos del usuario del dispositivo de MDM de iOS a otros dispositivos de Apple.

    Si la casilla no está marcada, el usuario puede utilizar AirDrop para transmitir datos a otros dispositivos de Apple.

    Si la casilla está marcada, el usuario no puede transmitir datos a otros dispositivos de Apple utilizando AirDrop.

    Esta casilla está desactivada por defecto.

  - **Treat AirDrop as a managed app**

    Uso de AirDrop como aplicación administrada para transferir datos desde el dispositivo móvil a otros dispositivos Apple. Esta restricción requiere que seleccione la casilla **Prohibit non-managed apps from using documents from managed apps**. Las aplicaciones no gestionadas son aplicaciones instaladas, configuradas y gestionadas por el usuario del dispositivo móvil.

    Si la casilla no está marcada, AirDrop se trata como una aplicación no administrada.

    Si la casilla está marcada, AirDrop se trata como una aplicación administrada.

    Esta casilla está desactivada por defecto.

- En la sección **Apple Music**:
  - **Prohibit Apple Music**

    Escuchar música en el dispositivo móvil del usuario con el servicio Apple Music.

    Si la casilla no está marcada, el usuario puede escuchar música en el dispositivo móvil en la aplicación Música.

    Si la casilla está marcada, el servicio Apple Music no está disponible para el usuario.

    Esta casilla está desactivada por defecto.

  - **Prohibit Radio in Apple Music**

    Escuchar la radio usando el servicio Apple Music en el dispositivo móvil del usuario.

    Si la casilla no está marcada, el usuario puede escuchar radio en la aplicación Música en el dispositivo móvil.

    Si la casilla está marcada, el usuario no puede escuchar la radio.

    Esta casilla está desactivada por defecto.

- En la sección **Apple Watch**:
  - **Disable Apple Watch wrist detection**

    Bloqueo automático de Apple Watch cuando el usuario se quita el reloj de la mano.

    Si la casilla no está marcada, Apple Watch se bloquea cuando el usuario se quita el reloj de la mano. Para desbloquearlo, el usuario debe escribir una contraseña en el dispositivo móvil.

    Si la casilla está marcada, Apple Watch no se puede bloquear después de que el usuario se quita el reloj.

    Esta casilla está desactivada por defecto.

  - **Prohibit pairing with Apple Watch**

    Sincronización de Apple Watch con un dispositivo móvil supervisado.

    Si la casilla no está marcada, el usuario del dispositivo móvil supervisado puede sincronizarlo con Apple Watch.

    Si la casilla está marcada, la sincronización con Apple Watch no está disponible.

    Esta casilla está desactivada por defecto.

- En la sección **Siri**:
  - **Prohibit Siri**

    > En desuso en iOS 26.4 y versiones posteriores.

    Uso de la app Siri en el dispositivo móvil del usuario.

    Si la casilla está desactivada, el usuario puede utilizar comandos de voz de Siri en el dispositivo móvil.

    Si la casilla está marcada, el usuario puede utilizar comandos de voz de Siri en un dispositivo móvil.

    Esta casilla está desactivada por defecto.

- **Prohibit when device is locked**

  > En desuso en iOS 26.4 y versiones posteriores.

  Uso de comandos de voz de Siri cuando el dispositivo móvil del usuario está bloqueado. El dispositivo móvil del usuario debe estar protegido con contraseña.

  Si la casilla de verificación no está seleccionada, el usuario puede utilizar comandos de voz de Siri en un dispositivo móvil bloqueado.

  Si la casilla de verificación está seleccionada, el usuario no puede utilizar comandos de voz de Siri en un dispositivo bloqueado.

  Esta casilla está desactivada por defecto.

- **Prohibit use of profanity filter**

  > En desuso en iOS 26.4 y versiones posteriores.

  Esta opción deshabilita el filtro de lenguaje obsceno mientras se utiliza la aplicación Siri en el dispositivo móvil.

  Si la casilla está desactivada, se filtra el lenguaje obsceno mientras el usuario utiliza la aplicación Siri.

  Si la casilla está marcada, no se filtra el lenguaje obsceno mientras el usuario utiliza la aplicación Siri.

  Esta casilla está desactivada por defecto.

- **Prohibit Siri from using internet search**

  > En desuso en iOS 26.4 y versiones posteriores.

  Esta opción prohíbe a Siri usar la búsqueda en Internet con comandos de voz en el dispositivo con MDM de iOS.

  Si la casilla está desactivada, Siri puede buscar en Internet respuestas a las preguntas del usuario.

  Si la casilla está marcada, Siri no puede buscar información en Internet.

  Esta casilla está desactivada por defecto.

- En la sección **Find My**:

  - **Prohibit locating devices in Find My**

    Seleccione o desmarque esta casilla para especificar si el usuario del dispositivo puede buscar dispositivos en la aplicación Encontrar.

    La restricción es compatible con dispositivos con iOS 13 y versiones posteriores.

    La casilla está desactivada de manera predeterminada.

  - **Prohibit locating friends in Find My**

    Seleccione o desmarque esta casilla para especificar si el usuario del dispositivo puede buscar amigos en la aplicación Encontrar.

La restricción es compatible con dispositivos con iOS 13 y versiones posteriores.

La casilla está desactivada de manera predeterminada.

- En la sección **Classroom**:
  - **Prohibit screen viewing via Classroom**

    Habilidad de un instructor de ver las pantallas del iPad de los estudiantes con la aplicación Aula.

    Si la casilla no está marcada, el instructor puede ver las pantallas del iPad de los estudiantes en la aplicación Aula.

    Si la casilla está marcada, el instructor no puede ver las pantallas del iPad de los estudiantes en la aplicación Aula.

    Esta casilla está desactivada por defecto.

- Restricciones en la pestaña **Storage**:
  - En la sección **General**:
    - **Prohibit access to USB devices in Files**

      Si la casilla no está marcada, el usuario puede acceder a los dispositivos USB conectados en la aplicación Archivos.

      Si la casilla está marcada, se bloquea el acceso a los dispositivos USB conectados en la aplicación Archivos.

      La configuración está disponible solo para los dispositivos móviles con la versión de iOS 13.1 o posteriores.

      Esta casilla está desactivada por defecto.

    - **Disable access to USB devices when the device is locked**

      Especifica si el modo USB restringido está habilitado cuando el dispositivo está bloqueado.

      Si la casilla está marcada, cuando se bloquea el dispositivo, las conexiones a las unidades USB están limitadas por el modo USB restringido.

      Si la casilla no está marcada, el dispositivo puede conectarse a unidades USB cuando está bloqueado.

      La configuración está disponible para los dispositivos móviles con la versión de iOS 11.4.1 o posteriores.

      Esta casilla está desactivada por defecto.

- Restricciones en la pestaña **Network**:
  - En la sección **General**:
    - **Prohibit use of NFC**

      Si la casilla no está marcada, el uso de NFC está permitido.

      Si la casilla está marcada, el uso de NFC está deshabilitado.

      La configuración está disponible solo para los dispositivos móviles con la versión de iOS 14.2 o posteriores.

      Esta casilla está desactivada por defecto.

    - **Prohibit creating VPN configurations**

Si la casilla no está marcada, el usuario puede crear una configuración de VPN en el dispositivo administrado.

Si la casilla está marcada, el usuario no puede crear una configuración de VPN en el dispositivo administrado.

La configuración está disponible solo para los dispositivos móviles con la versión de iOS 11 o posteriores.

Esta casilla está desactivada por defecto.

- **Prohibit modifying eSIM settings**

  Seleccione o desmarque esta casilla para especificar si el usuario del dispositivo puede cambiar la configuración relacionada con el plan del operador.

  La restricción es compatible con dispositivos con iOS 11 y versiones posteriores.

  La casilla está desactivada de manera predeterminada.

- En la sección **Wi-Fi**:

  - **Force Wi-Fi on**

    Especifica si la conexión Wi-Fi del dispositivo administrado debe estar siempre activada. El dispositivo puede conectarse a cualquier red Wi-Fi.

    Si se selecciona la casilla, la conexión Wi-Fi en el dispositivo está siempre encendida, incluso en modo avión. El usuario no puede deshabilitar el Wi-Fi en la configuración del dispositivo.

    Si la casilla está desactivada, el usuario puede deshabilitar el Wi-Fi en la configuración del dispositivo.

    La configuración está disponible solo para los dispositivos móviles con la versión de iOS 13 o posteriores.

    Esta casilla está desactivada por defecto.

  - **Force connection to allowed Wi-Fi networks only**

    Especifica si el dispositivo puede conectarse solo a redes Wi-Fi permitidas. Esta opción está disponible si agrega al menos una red Wi-Fi a la lista de redes Wi-Fi en la sección Wi-Fi.

    Si la casilla está marcada, el dispositivo se conecta solo a las redes Wi-Fi permitidas. El usuario no puede deshabilitar el Wi-Fi en la configuración del dispositivo.

    Si la casilla está desactivada, el usuario puede conectarse a cualquier red Wi-Fi.

    La configuración está disponible solo para los dispositivos móviles con la versión de iOS 14.5 o posteriores.

    Esta casilla está desactivada por defecto.

  - **Prohibit modifying Personal Hotspot settings**

    Si la casilla no está marcada, el usuario del dispositivo puede modificar la configuración del Hotspot personal.

    Si la casilla está marcada, el usuario del dispositivo no puede modificar la configuración del Hotspot personal.

    La configuración está disponible solo para los dispositivos móviles con la versión de iOS 12.2 o posteriores.

    Esta casilla está desactivada por defecto.

- En la sección **Bluetooth**:
  - **Prohibit modifying Bluetooth settings**

    Si la casilla no está marcada, el usuario puede modificar la configuración de Bluetooth en el dispositivo móvil.

    Si la casilla está marcada, no se puede modificar la configuración de Bluetooth en el dispositivo móvil.

    La configuración está disponible solo para los dispositivos móviles con la versión de iOS 11 o posteriores.

    Esta casilla está desactivada por defecto.

- En la sección **Cellular**:
  - **Prohibit automatic sync while roaming**

    Prohibir la sincronización automática de los datos del usuario cuando el dispositivo MDM de iOS está en itinerancia.

    Si la casilla de verificación no está seleccionada, el usuario puede habilitar la sincronización automática de los datos cuando el dispositivo está en itinerancia. Habilitar la sincronización automática durante el roaming puede resultar en costos inesperados del servicio móvil.

    Si la casilla está marcada, no se permite al usuario utilizar la sincronización automática de datos cuando el dispositivo está en itinerancia.

    Esta casilla está desactivada por defecto.

  - **Prohibit modifying cellular settings**

    Habilidad de configurar la transferencia de datos de la red móvil por parte de aplicaciones instaladas en un dispositivo móvil.

    Si la casilla no está marcada, el usuario puede configurar la transferencia de datos a través de una red móvil.

    Si la casilla está marcada, la configuración de la transferencia de datos de la red móvil por parte de aplicaciones no se puede modificar.

    Esta casilla está desactivada por defecto.

- Restricciones en la pestaña **Additional settings**:
  - En la sección **Display**:
    - **Prohibit changing wallpaper**

      Habilidad de seleccionar la imagen que se mostrará en la pantalla bloqueada o la pantalla de inicio.

      Si la casilla está marcada, el usuario puede seleccionar el fondo de pantalla del dispositivo móvil.

      Si esta casilla está marcada, la selección del fondo de pantalla no está disponible.

      Esta casilla está desactivada por defecto.

  - En la sección **Text**:
    - **Prohibit spellcheck**

      > En desuso en iOS 26.4 y versiones posteriores.

Uso del corrector ortográfico al escribir texto en un dispositivo móvil. La función de corrector ortográfico subraya las palabras escritas incorrectamente y sugiere correcciones.

Si la casilla no está marcada, el usuario puede habilitar y usar la función de corrector ortográfico.

Si la casilla está marcada, el corrector ortográfico no está disponible al escribir texto.

Esta casilla está desactivada por defecto.

- **Prohibit auto-correction**

  > En desuso en iOS 26.4 y versiones posteriores.

  Uso de la función de autocorrección al escribir texto.

  Si la casilla no está marcada, el usuario puede habilitar y usar la función de autocorrección.

  Si la casilla está marcada, la autocorrección no está disponible al escribir texto.

  Esta casilla está desactivada por defecto.

- **Prohibit dictionary search**

  > En desuso en iOS 26.4 y versiones posteriores.

  Uso de un diccionario para obtener definiciones de palabras en el dispositivo móvil. Solo un teclado de software tiene la función de diccionario.

  Si la casilla no está marcada, el usuario puede resaltar cualquier palabra en la pantalla del dispositivo móvil y obtener la definición de esa palabra.

  Si esta casilla está marcada, la búsqueda en el diccionario no está disponible.

  Esta casilla está desactivada por defecto.

- En la sección **Keyboard**:

  - **Prohibit predictive text**

    > En desuso en iOS 26.4 y versiones posteriores.

    Uso de la función de ingreso predictivo de texto. La función de ingreso predictivo de texto muestra opciones para completar palabras y sugerencias según los diccionarios disponibles.

    Si la casilla no está marcada, el usuario puede habilitar y usar la función de ingreso predictivo de texto.

    Si la casilla está marcada, la función de ingreso predictivo de texto no está disponible. En este caso, no se muestran sugerencias al escribir texto.

    Esta casilla está desactivada por defecto.

  - **Prohibit keyboard shortcuts**

    > En desuso en iOS 26.4 y versiones posteriores.

    Uso de accesos directos del teclado para el acceso rápido a funciones del dispositivo móvil.

Si la casilla no está marcada, el usuario puede habilitar la función de acceso directo del teclado y usarla al trabajar con el dispositivo móvil.

Si la casilla está marcada, la función de acceso directo del teclado no está disponible.

Esta casilla está desactivada por defecto.

- En la sección **Notifications**:
  - **Prohibit Wallet on-screen notifications when screen is locked**

    Uso de notificaciones de Wallet en la pantalla de bloqueo del dispositivo MDM de iOS.

    Si la casilla está desactivada, las notificaciones de Wallet aparecen en la pantalla de bloqueo del dispositivo móvil.

    Si la casilla está marcada, las notificaciones de Wallet no aparecen en la pantalla de bloqueo del dispositivo móvil. Para trabajar con Wallet, el usuario debe desbloquear el dispositivo.

    Esta casilla está desactivada por defecto.

  - **Hide Control Center when screen is locked**

    Posibilidad de ir al Centro de control del dispositivo de MDM de iOS cuando el dispositivo está bloqueado.

    Si la casilla está desactivada, el usuario puede ir al centro de control cuando el dispositivo está bloqueado.

    Si la casilla está marcada, el usuario no puede ir al centro de control cuando el dispositivo está bloqueado.

    Esta casilla está desactivada por defecto.

  - **Hide Notification Center when screen is locked**

    Posibilidad de ir al Centro de notificaciones del dispositivo MDM de iOS cuando el dispositivo está bloqueado.

    Si la casilla no está marcada, el usuario puede ir al centro de notificaciones deslizando hacia abajo la pantalla de bloqueo.

    Si la casilla está marcada, el usuario no puede ir al centro de notificaciones cuando el dispositivo está bloqueado.

    Esta casilla está desactivada por defecto.

  - **Hide Today View when screen is locked**

    Mostrar información de la vista Hoy en la pantalla de un dispositivo MDM de iOS bloqueado. La sección Hoy del centro de notificaciones muestra la siguiente información:

    - Eventos de calendario
    - Recordatorios
    - Precios de las acciones
    - Clima

    Si la casilla está desactivada, el usuario puede ver notificaciones en la vista Hoy en un dispositivo móvil bloqueado.

    Si la casilla está desactivada, la vista Hoy no aparece en el dispositivo móvil bloqueado.

    Esta casilla está desactivada por defecto.

- **Prohibit modifying notification settings**

  Habilidad de configurar la visualización de notificaciones en el dispositivo móvil.

  Si la casilla no está marcada, el usuario puede ajustar la configuración para ver notificaciones en el dispositivo móvil.

  Si la casilla está marcada, la visualización de notificaciones no se puede configurar.

  Esta casilla está desactivada por defecto.

- Restricciones en la pestaña **OS update**:

  - En la sección **General**:

    - **Delay software updates (days)**

      Permite demorar las actualizaciones del sistema operativo en el dispositivo.

      Si la casilla está marcada, el usuario no puede acceder a las actualizaciones durante el período especificado. La demora predeterminada es 30 días. Puede especificar otro período en el campo **Number of days from 1 to 90**.

      Si la casilla está desactivada, el usuario puede actualizar el software tan pronto como haya actualizaciones disponibles.

      La configuración está disponible solo para los dispositivos móviles con la versión de iOS 11.3 o posteriores.

      Esta casilla está desactivada por defecto.

7. Haga clic en **Aceptar**.
8. Haga clic en el botón **Save** para guardar los cambios que realizó.

Como resultado, las restricciones de las funciones se configurarán en el dispositivo móvil del usuario después de que se aplique la directiva.

Configurar restricciones de aplicaciones

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **iOS** y vaya a la sección **Restrictions**.
4. En la tarjeta **App restrictions**, haga clic en **Settings**.

   Se abre la ventana **App restrictions**.
5. Habilite la configuración con el interruptor **App restrictions**.
6. Configure las restricciones de aplicaciones del dispositivo MDM con iOS.

   Lista de restricciones de aplicaciones

   Restricciones en la sección **Safari**:

   - **Allow use of Safari**

     Uso del navegador Safari en el dispositivo MDM con iOS.

Si la casilla está marcada, el usuario puede utilizar el navegador Safari.

Si la casilla no está marcada, el usuario no puede utilizar el navegador Safari. El ícono de Safari está oculto en la pantalla de inicio del dispositivo MDM con iOS.

Esta casilla está marcada por defecto.

- **Allow AutoFill**

  Guardar y autorrellenar información ingresada por el usuario en formularios web en el navegador Safari.

  Si esta casilla está marcada, se guardan los datos del usuario ingresados en los formularios web. Posteriormente se insertan automáticamente en formularios web.

  Si esta casilla no está marcada, los datos del usuario no se insertan en los formularios web.

  Esta casilla está marcada por defecto.

- **Warn the user when visiting a dangerous website**

  Una opción que habilita una advertencia para el usuario que aparece antes de visitar un sitio web que Kaspersky Mobile Devices Protection and Management clasificó como peligroso.

  Si la casilla está marcada, Kaspersky Mobile Devices Protection and Management advierte al usuario sobre su intento de visitar un sitio web peligroso.

  Si la casilla no está marcada, Kaspersky Mobile Devices Protection and Management no advierte al usuario sobre su intento de visitar un sitio web peligroso.

  Esta casilla está desactivada por defecto.

- **Allow JavaScript**

  Uso de JavaScript en el navegador Safari.

  Si la casilla está marcada, el navegador Safari utiliza JavaScript al abrir páginas web.

  Si la casilla no está marcada, el navegador Safari no utiliza JavaScript al abrir páginas web.

  Esta casilla está marcada por defecto.

- **Block pop-up windows**

  Bloqueo de ventanas emergentes en el navegador Safari.

  Si la casilla está marcada, Kaspersky Mobile Devices Protection and Management bloquea las ventanas emergentes en el navegador Safari.

  Si la casilla no está marcada, Kaspersky Mobile Devices Protection and Management no bloquea las ventanas emergentes en el navegador Safari.

  Esta casilla está desactivada por defecto.

- **Cookie settings**

  Seleccione las condiciones para aceptar cookies:

  - **Allow cookies and website tracking**. El navegador Safari acepta cookies y permite rastrear la actividad del usuario.
  - **Allow cookies and block website tracking**. El navegador Safari acepta cookies y bloquea el seguimiento de la actividad del usuario.
  - **Block cookies and website tracking**. El navegador Safari bloquea las cookies y el seguimiento de la actividad del usuario.

  El valor predeterminado es **Allow cookies and website tracking**.

Restricciones en la sección **Game Center**:

- **Allow use of Game Center**

  Acceso al servicio de juegos Game Center desde la aplicación Game Center en el dispositivo móvil MDM con iOS.

  Si la casilla está marcada, el usuario puede visitar el servicio de juegos Game Center desde la aplicación Game Center en el dispositivo móvil.

  Si la casilla no está marcada, el usuario no puede visitar el servicio de juegos Game Center desde la aplicación Game Center en el dispositivo móvil. El ícono de Game Center está oculto en la pantalla de inicio del dispositivo MDM con iOS.

  Esta casilla está marcada por defecto.

- **Allow adding friends in Game Center**

  Una opción que permite agregar usuarios al servicio de juegos Game Center en el dispositivo móvil MDM con iOS.

  Si la casilla está marcada, el usuario puede agregar usuarios al servicio de juegos Game Center en el dispositivo móvil.

  Si la casilla no está marcada, el usuario no puede agregar usuarios al servicio de juegos Game Center en el dispositivo móvil.

  Esta casilla está marcada por defecto.

- **Allow multiplayer games in Game Center**

  Uso del servicio de juegos Game Center en el modo multijugador en el dispositivo MDM con iOS.

  Si la casilla está marcada, el usuario puede participar en juegos multijugador en el servicio de juegos Game Center en el dispositivo móvil.

  Si la casilla no está marcada, el usuario no puede participar en juegos multijugador en el servicio de juegos Game Center en el dispositivo móvil.

  > Si la casilla no está marcada, los usuarios aún pueden jugar juntos a través de SharePlay o un servicio de terceros.

  Esta casilla está marcada por defecto.

Restricciones en la sección **Additional settings**:

- **Allow use of iTunes Store**

  Acceso al servicio multimedia iTunes Store desde la aplicación iTunes en un dispositivo MDM con iOS.

  Si la casilla está marcada, el usuario puede ver, comprar y descargar contenido multimedia de iTunes Store utilizando la aplicación iTunes en el dispositivo móvil.

  Si la casilla no está marcada, el usuario no puede ver, comprar ni descargar contenido multimedia de iTunes Store utilizando la aplicación iTunes en el dispositivo móvil. El ícono de iTunes está oculto en la pantalla de inicio del dispositivo MDM con iOS.

  Esta casilla está marcada por defecto.

- **Allow use of News**

  Visualización de noticias en el dispositivo móvil del usuario con la aplicación News.

  Si la casilla está marcada, el usuario puede ver noticias con la aplicación News.

  Si la casilla no está marcada, la aplicación News no está disponible para el usuario.

Esta casilla está marcada por defecto.

- **Allow use of Podcasts**

  Escuchar podcasts en el dispositivo móvil del usuario con la aplicación Podcasts.

  Si la casilla está marcada, el usuario puede buscar, reproducir y descargar podcasts con la aplicación Podcasts.

  Si la casilla no está seleccionada, no se pueden descargar podcasts al dispositivo móvil.

  Esta casilla está marcada por defecto.

7. Haga clic en **Aceptar**.
8. Haga clic en el botón **Save** para guardar los cambios que realizó.

Como resultado, las restricciones de la aplicación se configurarán en el dispositivo móvil del usuario después de que se aplique la directiva.

Configurar restricciones de contenido

Apple determina las categorías utilizadas para las restricciones de contenido. En algunos casos, cuando se configuran restricciones de contenido, los resultados reales pueden diferir de los resultados esperados.

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **iOS** y vaya a la sección **Restrictions**.
4. En la tarjeta **Content restrictions**, haga clic en **Settings**.

   Se abre la ventana **Content restrictions**.
5. Habilite la configuración con el interruptor de **Content restrictions**.
6. Configure las restricciones de contenido del dispositivo MDM con iOS.

   Lista de restricciones de contenido

   Region

   Selección del país cuyo sistema de clasificación se aplica automáticamente al contenido multimedia en el dispositivo MDM con iOS.

   El valor predeterminado es **Estados Unidos**.

   Ajustes de la sección **Age rating**:

   - **Videos**

     Selección del sistema de clasificación para acceder a películas en el dispositivo MDM con iOS.

     La lista de clasificación depende de la región seleccionada.

     Si se seleccionó la opción **Allow all** el usuario puede ver cualquier película en el dispositivo móvil.

     La opción **Allow all** está seleccionada de manera predeterminada.

- **TV shows**

  Selección del sistema de clasificación para acceder a programas de TV en el dispositivo MDM con iOS.

  La lista de clasificación depende de la región seleccionada.

  Si se seleccionó la opción **Allow all** el usuario puede ver cualquier programación de TV en el dispositivo móvil.

  La opción **Allow all** está seleccionada de manera predeterminada.

- **Apps**

  Seleccionar el sistema de clasificación para acceder a aplicaciones de terceros en el dispositivo MDM con iOS.

  La lista de clasificación depende del sistema de clasificación seleccionado.

  Si se seleccionó la opción **Allow all** el usuario puede utilizar cualquier aplicación de terceros en el dispositivo móvil.

  La opción **Allow all** está seleccionada de manera predeterminada.

  > Las restricciones de la aplicación pueden aplicarse incluso si la opción **Allow all** está seleccionada. Esto se debe a un problema reconocido por Apple.

- **Allow downloading erotica in Apple Books**

  Acceso a contenido para adultos explícito en Book Store en el dispositivo móvil del usuario.

  Si la casilla está marcada, el usuario puede descargar contenido para adultos desde la aplicación Apple Books en el dispositivo MDM con iOS.

  Si la casilla no está marcada, el usuario no puede descargar contenido para adultos desde la aplicación Apple Books en el dispositivo MDM con iOS.

  Esta casilla está marcada por defecto.

- **Allow explicit content**

  Acceso a contenido multimedia explícito desde iTunes Store en el dispositivo MDM con iOS. Se aplican las restricciones de los proveedores de iTunes Store.

  Si la casilla está marcada, el contenido multimedia explícito comprado a través de iTunes Store está disponible en el dispositivo móvil del usuario.

  Si la casilla no está seleccionada, el contenido multimedia explícito comprado a través de iTunes Store queda oculto para el usuario del dispositivo móvil.

  Esta casilla está marcada por defecto.

7. Haga clic en **Aceptar**.

8. Haga clic en el botón **Save** para guardar los cambios que realizó.

Como resultado, las restricciones de contenido se configurarán en el dispositivo móvil del usuario después de que se aplique la directiva.

Configuración del acceso del usuario a sitios web

Esta sección contiene instrucciones sobre cómo configurar el acceso a sitios web en dispositivos iOS y Android.

Configuración de acceso a sitios web en dispositivos Android

Puede usar Control web para configurar el acceso de usuarios de dispositivos Android a sitios web. Control web también admite el filtrado de sitios web según las categorías definidas en el servicio en la nube de Kaspersky Security Network. El filtrado le permite restringir el acceso del usuario a determinadas categorías de sitios web (por ejemplo, "Juegos de azar, loterías, sorteos" o "Comunicación por Internet"). Control web está habilitada de forma predeterminada

En Yandex Browser y Samsung Internet, las URL maliciosas y de phishing pueden permanecer desbloqueadas. Esto se debe a que solo se realiza el análisis del dominio del sitio web. Si se trata de un dominio malicioso o de phishing, Protección web bloquea la amenaza. Si el dominio no está clasificado como malicioso o como phishing, la URL específica no se bloquea.

El Control web en dispositivos Android solo es compatible con Google Chrome, el navegador HUAWEI, Samsung Internet y Yandex Browser.

El Control web requiere lo siguiente para funcionar en un dispositivo administrado:

- Se debe configurar Kaspersky Endpoint Security for Android como un Servicio de accesibilidad.

  En dispositivos corporativos, si Kaspersky Endpoint Security para Android no está habilitado como una función de accesibilidad, Control web solo es compatible con Google Chrome y solo verifica el dominio de un sitio web. Para permitir que otros navegadores (Samsung Internet, Yandex Browser y HUAWEI Browser) admitan Control web, habilite Kaspersky Endpoint Security como una función de accesibilidad. Esto también le permitirá usar la función Pestañas personalizadas.

  Si Kaspersky Endpoint Security para Android no está habilitado como una función de Accesibilidad y hay un proxy habilitado en la tarjeta **Google Chrome settings**, Control web no funcionará.

- Se debe aceptar la Declaración con respecto al procesamiento de datos para el uso de la Protección web (Declaración de Protección web). Kaspersky Endpoint Security usa Kaspersky Security Network (KSN) para analizar sitios web. La Declaración de Protección web contiene los términos del intercambio de datos con KSN.

- En algunos dispositivos, el usuario debe conceder de forma manual los siguientes permisos:

  - **Ejecutar en segundo plano**
  - **Mostrar ventanas emergentes mientras se ejecuta en segundo plano**
  - **Mostrar ventana emergente**
  - **Ignorar la optimización de la batería**

Para ajustar la configuración del acceso de los usuarios de dispositivos a sitios web:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **Android** y vaya a la sección **Security controls**.

4. En la tarjeta **Web Control**, haga clic en **Settings**.

   Se abre la ventana **Web Control**.

5. Seleccione una de las siguientes opciones:

   - Si desea que la aplicación restrinja el acceso del usuario a sitios web en función de su contenido, haga lo siguiente:

     a. En la lista desplegable **Operating mode**, en la lista desplegable, seleccione **Prohibit websites in selected categories**.

     b. En la sección **Categories**, cree una lista de categorías prohibidas; para ello, seleccione las casillas junto a las categorías de sitios web a los que la app bloqueará el acceso.

   - Si desea que la aplicación permita o bloquee el acceso de los usuarios solo a sitios web especificados, haga lo siguiente:

     a. En la lista desplegable **Operating mode**, seleccione **Allow only listed websites** o **Allow all websites except listed ones**.

     b. Haga clic en **Add**.

     c. En la ventana que se abre, cree una lista de sitios web a los que la aplicación permitirá o bloqueará el acceso, según el valor seleccionado en la lista desplegable. Puede añadir sitios web mediante un enlace (URL completa, incluido el protocolo, por ejemplo, `https://example.com`).

     Para asegurarse de que la aplicación permita o bloquee el acceso al sitio web especificado en todas las versiones compatibles de Google Chrome, HUAWEI Browser, Samsung Internet y Yandex Browser, incluya la misma URL dos veces, una vez con el protocolo HTTP (por ejemplo, `http://example.com`) y una vez con el protocolo HTTPS (por ejemplo, `https://example.com`).

     Por ejemplo:

     - `https://example.com`: se permite o bloquea la página principal del sitio web. Solo se puede acceder a esta URL a través del protocolo HTTP.
     - `http://example.com`: se permite o bloquea la página principal del sitio web, pero solo cuando se accede a través del protocolo HTTP. Otros protocolos, como el HTTPS, no se ven afectados.
     - `https://example.com/page/index.html`: solo se permitirá o bloqueará la página index.html del sitio web. El resto del sitio web no se ve afectado por esta entrada.

     La aplicación también admite expresiones regulares. Al escribir la dirección de un sitio web permitido o prohibido, utilice las siguientes plantillas:

     - `https://example\.com/.*`: esta plantilla permite o bloquea todas las páginas secundarias del sitio web, a las que se accede a través del protocolo HTTPS (por ejemplo, `https://example.com/about`).
     - `https?://example\.com/.*`: esta plantilla permite o bloquea todas las páginas secundarias del sitio web, a las que se accede a través de los protocolos HTTP y HTTPS.
     - `https?://.*\.example\.com`: esta plantilla permite o bloquea todas las páginas de subdominios del sitio web (por ejemplo, `https://pictures.example.com`).

- `https?://example\.com/[abc]/.*`: esta plantilla permite o bloquea todas las páginas secundarias del sitio web donde la ruta de la URL comienza con 'a', 'b' o 'c' como primer directorio (por ejemplo, `https://example.com/b/about`).

- `https?://\w{3,5}.example\.com/.*`: esta plantilla permite o bloquea todas las páginas secundarias del sitio web donde el subdominio consta de una palabra con 3 a 5 caracteres (por ejemplo, `http://abde.example.com/about`).

Use la expresión `https?` para seleccionar los protocolos HTTP y HTTPS. Para obtener más información sobre las expresiones regulares, consulte el sitio web de soporte técnico de Oracle.

d. Haga clic en **Agregar**.

- Si desea que la app bloquee el acceso del usuario a todos los sitios web, en la sección **Operating mode**, en la lista desplegable, seleccione **Prohibit all websites**.

6. Si desea que la aplicación verifique la URL completa al abrir un sitio web en Pestañas personalizadas, seleccione la casilla **Check full URL when using Custom Tabs**.

   Pestañas personalizadas es un navegador integrado en la aplicación que permite al usuario ver páginas web sin tener que salir de la aplicación y cambiar a una versión completa del navegador web. Esta opción proporciona un mejor reconocimiento de URL y compara las URL con las reglas de Control web configuradas. Si la casilla está marcada, Kaspersky Endpoint Security para Android abre el sitio web en una versión completa del navegador y verifica toda la dirección web del sitio web. Si la casilla no está marcada, Kaspersky Endpoint Security para Android solo verifica el dominio del sitio web en Pestañas personalizadas.

   La función Pestañas personalizadas es compatible con Google Chrome, el navegador HUAWEI y Samsung Internet.

7. Si desea eliminar las restricciones basadas en el contenido sobre el acceso de los usuarios a los sitios web, deshabilite la configuración con el interruptor **Web Control** y haga clic en **Disable**.

8. Haga clic en **Aceptar**.

9. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Administrar la lista de sitios web

Puede administrar la lista de sitios web con los siguientes botones:

- **Add**: haga clic para agregar un sitio web a la lista ingresando una URL o una expresión regular.

- **Upload**: haga clic para agregar varios sitios web a la lista especificando un archivo TXT que contiene las URL requeridas o las expresiones regulares. El archivo debe estar codificado en UTF-8. Las URL o las expresiones regulares del archivo deben estar separadas por punto y coma o saltos de línea.

- **Edit**: haga clic para cambiar la dirección de un sitio web.

- **Delete**: haga clic para eliminar uno o más sitios web de la lista.

Configuración de acceso a sitios web en dispositivos iOS con MDM

Esta configuración se aplica a los dispositivos supervisados.

Configure los ajustes de Control web para controlar el acceso a sitios web para usuarios de dispositivos MDM con iOS. Control web administra el acceso de los usuarios a sitios web en función de listas de sitios web permitidos y bloqueados. Control web también le permite agregar sitios web favoritos al panel de favoritos de Safari.

De forma predeterminada, el acceso a sitios web no está restringido.

Si una URL redirige a un sitio web diferente, Control web solo verifica el sitio al que redirige.

Para ajustar la configuración de acceso de los usuarios del dispositivo a los sitios web, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **iOS** y vaya a la sección **Security controls**.
4. En la tarjeta **Web Control**, haga clic en **Settings**.

   Se abre la ventana **Web Control**.
5. Habilite la configuración con el interruptor de **Web Control**.
6. En la lista desplegable **Operating mode**, realice una de las siguientes acciones:
   - Si desea crear una lista de sitios web permitidos, seleccione **Allow only listed websites**.
   - Si desea crear una lista de sitios web prohibidos, seleccione **Allow all websites except listed ones**.
7. Realice una de las siguientes acciones:
   - Si desea agregar sitios web manualmente, siga estos pasos:
     a. Haga clic en **Add**.
     b. Agregue sitios web a los que la aplicación permitirá o bloqueará el acceso, según el valor seleccionado en la lista desplegable.

        La dirección del sitio web debe empezar por `http://` o `https://`. Kaspersky Mobile Devices Protection and Management permite o bloquea el acceso a todos los sitios web del dominio. Por ejemplo, si agrega `http://www.example.com` a la lista de sitios web permitidos, se permite el acceso a `http://pictures.example.com` y a `http://example.com/movies`.

        Si desea agregar un sitio web permitido a los marcadores de Safari en dispositivos móviles, seleccione la casilla **Add to bookmarks on device** debajo de la dirección del sitio web.
     c. Haga clic en **Agregar**.

- Si desea cargar un archivo TXT con una lista de sitios web, haga clic en **Cargar**.

  El archivo TXT debe guardarse con la codificación UTF-8 y los saltos de línea LF o CR+RF.

8. Haga clic en **Aceptar**.
9. Haga clic en el botón **Save** para guardar los cambios que realizó.

Como resultado, una vez que se aplique la directiva, Control web se configurará en los dispositivos móviles.

Control de cumplimiento

Esta sección contiene instrucciones sobre cómo supervisar el cumplimiento de los dispositivos con los requisitos corporativos y configurar las reglas de control de cumplimiento.

Control de cumplimiento de dispositivos Android

Puede controlar el cumplimiento de los dispositivos Android con los requisitos de seguridad corporativos. Los requisitos de seguridad corporativos regulan cómo el usuario puede trabajar con el dispositivo. Por ejemplo, la protección en tiempo real debe estar activada en el dispositivo, las bases de datos antimalware deben estar actualizadas y la contraseña del dispositivo debe ser lo suficientemente segura. El Control de cumplimiento se basa en la lista de reglas. Una regla de cumplimiento incluye los componentes siguientes:

- Criterio de control del dispositivo (por ejemplo, ausencia de aplicaciones bloqueadas en el dispositivo).
- Período de tiempo designado para que el usuario solucione el incumplimiento (por ejemplo, 24 horas)
- Respuestas que se realizarán en el dispositivo si el usuario no corrige el problema de incumplimiento dentro del período de tiempo establecido (por ejemplo, bloquear el dispositivo).

  Si el dispositivo está en modo de ahorro de batería, Kaspersky Endpoint Security para Android puede realizar esta tarea más tarde de lo especificado.

Para crear una regla para verificar que los dispositivos cumplan con una directiva, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **Android** y vaya a la sección **Security controls**.
4. En la tarjeta **Compliance Control**, haga clic en **Settings**.

   Se abre la ventana **Compliance Control**.
5. Habilite la configuración con el interruptor **Compliance Control**.

6. En la sección **When non-compliance is detected**:

   - Seleccione la casilla **Notify user** para informar al usuario que el dispositivo no cumple con la directiva.

     Si la casilla está desactivada, no se notifica al usuario sobre el problema de incumplimiento y la respuesta se realiza en el dispositivo tan pronto como expire el tiempo asignado para corregir el incumplimiento.

   - Seleccione la casilla **Notify the administrator through the "Events" section** para informar al administrador que el dispositivo no cumple con la directiva.

7. Haga clic en **Add**.

   Se inicia el Add rule wizard. Este asistente lo ayudará a crear un conjunto de reglas para verificar que el dispositivo cumpla con la directiva. Navegue por el asistente con los botones **Next** y **Back**.

Paso 1. Criterion for non-compliance

Haga clic en **Add criterion** para especificar el criterio de incumplimiento que activa la regla.

Los siguientes criterios están disponibles:

- **Real-time protection is disabled**

  Kaspersky Endpoint Security para Android no está instalado o no se está ejecutando en el dispositivo.

- **Anti-malware databases on device are out of date**

  Las bases de datos antimalware se actualizaron por última vez hace 3 días o más.

- **Forbidden apps are installed**

  La lista de aplicaciones del dispositivo contiene aplicaciones que están configuradas como prohibidas en la configuración **App Control** de la directiva.

- **Apps from forbidden categories are installed**

  La lista de aplicaciones del dispositivo contiene aplicaciones de las categorías que están establecidas como prohibidas en la configuración de **App Control** de la directiva.

- **Not all required apps are installed**

  La lista de aplicaciones del dispositivo no contiene una aplicación que esté establecida como requerida en la configuración de **App Control** de la directiva.

- **Operating system version is outdated**

  La versión de Android en el dispositivo está fuera del rango permitido.

  Para este criterio, especifique las versiones mínima y máxima permitidas de Android en los campos **Minimum version** y **Maximum version**. Si la versión máxima permitida se establece en **Any**, también se permitirán las versiones futuras de Android compatibles con Kaspersky Endpoint Security para Android.

- **Device has not been synchronized for a long time**

  Se comprueba la última sincronización del dispositivo con el Servidor de administración.

  Para este criterio, especifique el período máximo después de la última sincronización en el campo **Period without synchronization**.

- **Device has been rooted**

  El dispositivo está hackeado (se ha obtenido acceso al root en el dispositivo).

- **Unlock password is not compliant with security settings specified in policy**

  La contraseña de desbloqueo del dispositivo no es compatible con la configuración definida en la tarjeta **Screen unlock settings**.

- **Installed version of Kaspersky Endpoint Security for Android is outdated**

  Kaspersky Endpoint Security for Android instalado en el dispositivo es obsoleto.

  Este criterio se aplica solo a una aplicación instalada con un paquete de instalación de Kaspersky Endpoint Security para Android y si la versión mínima permitida de Kaspersky Endpoint Security para Android se especifica en la configuración **App update** de la directiva.

- **SIM card usage is not compliant with security requirements**

  La tarjeta SIM del dispositivo se reemplazó o se quitó en comparación con el estado de verificación anterior, o se insertó una tarjeta SIM adicional.

  Para este criterio, seleccione la condición específica que se debe supervisar:

  - **The SIM card must not be replaced or removed**
  - **The SIM card must not be replaced or removed; additional SIM cards must not be inserted**

- **Device location**

  El dispositivo está fuera de las áreas especificadas de la geocerca.

  > Especificar el área de la geocerca generará un mayor consumo de batería del dispositivo.

  Para este criterio, seleccione la condición específica que se debe supervisar:

  - **The device is within a specified geofence** (las áreas de la geocerca se combinan con el operador lógico OR).
  - **The device is outside specified geofences** (las áreas de la geocerca se combinan mediante el operador lógico AND).

  Para agregar un área de geocerca, siga estos pasos:

  1. Clic en **Add geofences**.

     Se abre la ventana **Add geofences**.

  2. Especifique el **Geofence name**.

  3. Especifique el perímetro de la geocerca ingresando una latitud y una longitud para cada punto.

     > Para cada área de geocerca, puede ingresar manualmente de 3 a 100 pares de coordenadas (latitud, longitud) como números decimales.
     >
     > Un perímetro de geocerca no debe contener líneas que se crucen.

     Si es necesario, puede especificar más de 3 puntos haciendo clic en el botón **Add point**.

     Para eliminar un punto, haga clic en el botón **X**.

Para ver el área de geocerca especificada en el programa Yandex.Maps, haga clic en **View on map**.

4. Haga clic en **Aceptar** para agregar las geocercas especificadas.

- **Kaspersky Endpoint Security for Android has no access to precise or background location**

  Kaspersky Endpoint Security para Android no puede acceder a la ubicación precisa del dispositivo ni utilizar la ubicación del dispositivo en segundo plano.

Paso 2. Responses for non-compliance with security requirements

Añadir las respuestas que se realizarán en el dispositivo si se detecta el criterio de incumplimiento especificado.

Seleccione una de las siguientes opciones:

- **Add instant response**. La respuesta se aplica instantáneamente después de que se detecta el criterio de incumplimiento.

- **Add deferred response**. La respuesta se aplica después de un período de retraso que puede especificar en el campo **Deferral period**.

  Las siguientes respuestas están disponibles:

  - **Block all apps except system apps**

    Se bloquea el inicio de todas las aplicaciones en el dispositivo móvil, excepto las aplicaciones del sistema.

    Tan pronto como el criterio de incumplimiento seleccionado para la regla deje de detectarse en el dispositivo, las aplicaciones se desbloquearán automáticamente.

  - **Lock device**

    El dispositivo móvil está bloqueado. Para obtener acceso a los datos, debe desbloquear el dispositivo ingresando el código de acceso único o usando el comando **Unlock device**.

  - **Wipe corporate data**

    Los datos corporativos se borran del dispositivo. La lista de datos eliminados depende del modo en que funciona el dispositivo:

    - En un dispositivo personal, el perfil de Knox y el certificado de correo se eliminan.

    - En un dispositivo corporativo, el perfil de Knox y los certificados instalados por Kaspersky Endpoint Security para Android (certificados de correo, VPN y perfil SCEP, excepto los certificados móviles) se eliminan.

    - Además, en un dispositivo con contenedor corporativo, el contenedor (su contenido, configuraciones y restricciones) y los certificados instalados en él (certificados de correo, VPN y perfil SCEP, excepto los certificados móviles) se eliminan.

  - **Reset to factory settings**

    Todos los datos se borran del dispositivo y los ajustes se restablecen a los valores de fábrica. Después de que esta respuesta se aplica, el dispositivo deja de ser un dispositivo administrado. Para conectar el dispositivo a Kaspersky Security Center, debe reinstalar Kaspersky Endpoint Security for Android.

    En dispositivos con Android 14 o versiones posteriores, esta respuesta solo se aplica si el dispositivo funciona en modo de dispositivo corporativo.

  - **Lock corporate container**

El contenedor corporativo del dispositivo está bloqueado. Para obtener acceso al contenedor corporativo, debe desbloquearlo.

La respuesta solo se aplica a dispositivos con Android 6 o versiones posteriores.

Una vez que se bloquea el contenedor corporativo de un dispositivo, se borra el historial de contraseñas del contenedor. Significa que el usuario puede especificar una de las contraseñas recientes, independientemente de la configuración de la contraseña del contenedor corporativo.

- **Wipe data of all apps**

  En un dispositivo corporativo, se eliminan los datos de todas las aplicaciones del dispositivo.

  En un dispositivo con contenedor corporativo, se eliminan los datos de todas las aplicaciones del contenedor.

  Como resultado, las aplicaciones vuelven a su estado predeterminado.

  La respuesta solo se aplica a dispositivos con Android 9 o versiones posteriores en los modos de funcionamiento de dispositivo corporativo o dispositivo con contenedor corporativo.

- **Wipe data of a specified app**

  Para esta respuesta, debe especificar el nombre del paquete para la aplicación cuyos datos se eliminarán.
  Cómo obtener el nombre del paquete de una aplicación

  Para obtener el nombre de un paquete de aplicación:

  1. Abrir Google Play.
  2. Busque la aplicación y abra su página.

     La URL de la aplicación termina con el nombre de su paquete (por ejemplo, https://play.google.com/store/apps/details?id= **com.android.chrome**).

  Para obtener el nombre de un paquete de aplicaciones que se agregó a Kaspersky Security Center, siga estos pasos:

  1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Apps & files**.
  2. Seleccione **Android** → **Apps**.

     En la lista de aplicaciones que se abre, los identificadores de aplicaciones se muestran en la columna **Package name**.

  Como resultado, la aplicación se revierte a su estado predeterminado.

  La respuesta solo se aplica a dispositivos con Android 9 o versiones posteriores en los modos de funcionamiento de dispositivo corporativo o dispositivo con contenedor corporativo.

- **Prohibit safe boot**

  El usuario no puede iniciar el dispositivo en modo seguro.

La respuesta solo se aplica a dispositivos corporativos con Android 6 o versiones posteriores.

- **Prohibit use of camera**

  El usuario no puede usar las cámaras del dispositivo.

- **Prohibit use of Bluetooth**

  El usuario no puede encender ni configurar el Bluetooth.

  La respuesta solo se aplica a dispositivos personales con Android 12 o versiones anteriores, dispositivos corporativos o dispositivos con contenedor corporativo.

- **Prohibit use of Wi-Fi**

  El usuario no puede usar ni configurar el Wi-Fi.

  La respuesta solo se aplica a dispositivos personales con Android 9 o versiones anteriores o dispositivos corporativos.

- **Prohibit USB debugging features**

  El usuario no puede usar las funciones de depuración USB y el modo de desarrollador en el dispositivo.

  La respuesta solo se aplica a dispositivos corporativos o dispositivos con contenedor corporativo.

- **Prohibit airplane mode**

  El usuario no puede habilitar el modo avión en el dispositivo.

  La respuesta solo se aplica a dispositivos corporativos con Android 9 o versiones posteriores.

Haga clic en **Add rule** para finalizar el Add rule wizard. La nueva regla y sus detalles aparecen en la lista de reglas de Control de cumplimiento. Para desactivar temporalmente una regla, use el interruptor de alternancia junto a la regla seleccionada.

Para habilitar la eliminación automática de datos de los dispositivos asociados con cuentas deshabilitadas de usuarios de Active Directory, seleccione la casilla **Wipe data from devices with disabled Active Directory user accounts** y seleccione una de las siguientes acciones:

- **Wipe corporate data**
- **Reset to factory settings**

  En dispositivos con Android 14 o versiones posteriores, esta acción solo se aplica si el dispositivo funciona en modo de dispositivo corporativo.

Esta configuración requiere integración con Microsoft Active Directory.

Si usa perfiles de directiva, asegúrese de habilitar la opción de borrar datos para toda la directiva. Cuando se deshabilita una cuenta de usuario en Active Directory, primero se elimina del grupo de usuarios de Active Directory. Como resultado, el perfil de directiva ya no se aplica a esta cuenta de usuario, por lo que los datos no se borran del dispositivo.

Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Control de apps

Esta sección contiene instrucciones sobre cómo configurar el acceso del usuario a aplicaciones en un dispositivo móvil.

Control de apps en dispositivos Android

El componente Control de aplicaciones le permite administrar aplicaciones en dispositivos Android y configurar el uso de estas aplicaciones para mantener seguros los dispositivos.

Puede restringir las actividades del usuario en un dispositivo en el que se hayan instalado aplicaciones prohibidas o no se hayan instalado las aplicaciones necesarias (por ejemplo, bloquear el dispositivo). Puede imponer restricciones usando el componente Control de cumplimiento. Para ello, en la configuración de la regla debe seleccionar el criterio **Forbidden apps are installed**, **Apps from forbidden categories are installed** o **Not all required apps are installed**.

Kaspersky Endpoint Security para Android debe estar configurado como función de Accesibilidad para garantizar el correcto funcionamiento del Control de apps. Kaspersky Endpoint Security para Android solicita al usuario que configure la app como una función de Accesibilidad a través del Asistente de configuración inicial. El usuario puede omitir este paso o desactivar este servicio más adelante en los ajustes del dispositivo. Si el usuario hace esto, Control de aplicaciones no se ejecutará. En los dispositivos corporativos, Control de apps se ejecutará, pero es posible que no funcione correctamente si no se otorga el permiso de Accesibilidad. Aún es necesario otorgar el permiso de Accesibilidad a la app para que funcione correctamente.

En los dispositivos corporativos, tiene un control extendido sobre el dispositivo. Control de apps funciona sin notificar al usuario del dispositivo:

- Las aplicaciones requeridas se instalan automáticamente en segundo plano. Para instalar aplicaciones de forma silenciosa, debe especificar un vínculo al archivo APK de la aplicación requerida en la configuración de la directiva.

- Las aplicaciones prohibidas se pueden eliminar del dispositivo automáticamente. Para eliminar aplicaciones de forma silenciosa, debe seleccionar la casilla **Remove forbidden apps automatically** en la configuración de la directiva.

Para ajustar la configuración de inicio de la aplicación en el dispositivo móvil, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management → Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **Android** y vaya a la sección **Security controls**.

4. En la tarjeta **App Control**, haga clic en **Settings**.

   Se abre la ventana **App Control**.

5. Habilite la configuración con el interruptor **App Control**.

6. Ajuste la configuración en las siguientes pestañas:

   - Si desea configurar las reglas generales de administración de aplicaciones, **vaya a la pestaña App use**.

     1. En la lista desplegable **Operating mode**, seleccione el modo de Control de aplicaciones.

        - Para permitir que el usuario inicie todas las aplicaciones, excepto las especificadas como bloqueadas en la lista de categorías de aplicaciones y aplicaciones, seleccione **Use all apps except forbidden ones**. Kaspersky Endpoint Security para Android ocultará los íconos de las aplicaciones prohibidas. Esta opción se selecciona de forma predeterminada.

        - Para permitir que el usuario pueda iniciar solo las aplicaciones especificadas en la lista de categorías y aplicaciones permitidas, recomendadas o requeridas, seleccione **Use only allowed apps**. Kaspersky Endpoint Security para Android ocultará los íconos de todas las aplicaciones, excepto las especificadas en la lista de aplicaciones permitidas, recomendadas o requeridas y del sistema.

     2. Si desea que Kaspersky Endpoint Security para Android envíe datos sobre aplicaciones prohibidas al registro de eventos sin bloquearlas, seleccione la casilla **Do not block forbidden apps, only add a record to the event log**.

     3. Si desea que Kaspersky Endpoint Security para Android bloquee el inicio de aplicaciones del sistema (como Calendario, Cámara y Configuración) en el dispositivo móvil del usuario, seleccione la casilla **Block system apps**. Esta casilla se muestra en el modo **Use only allowed apps**.

        Recomendamos no bloquear las aplicaciones del sistema, ya que esto podría provocar un mal funcionamiento del dispositivo.

Entre las aplicaciones del sistema, el mecanismo del sistema para solicitar permisos de aplicaciones puede estar bloqueado. Si desea desbloquear este mecanismo, busque su nombre (por ejemplo, `com.google.android.permissioncontroller`) en el registro de eventos y agréguelo a las excepciones.

Antes de eliminar Kaspersky Endpoint Security para Android del dispositivo, desmarque esta casilla o deshabilite Control de aplicaciones.

4. Si desea que Kaspersky Endpoint Security para Android elimine las aplicaciones prohibidas del dispositivo en segundo plano sin notificar al usuario, seleccione la casilla **Remove forbidden apps automatically**. Esta casilla se muestra en las directivas para administrar dispositivos corporativos.

5. Haga clic en **Add** para agregar aplicaciones y categorías para las que desea establecer reglas.

   Se abre la ventana **Add app or category**.

6. En el campo **Object**, seleccione **App** o **App category** y haga lo siguiente:

   - Si seleccionó **App**, seleccione un paquete de instalación o especifique el nombre del paquete y el nombre de la aplicación en los campos correspondientes.
   - Si seleccionó **App category**, seleccione una categoría e ingrese una descripción en los campos correspondientes.
   - Haga clic en **Add**.

   La aplicación o categoría se agrega a la lista.

7. Si desea configurar las excepciones de las aplicaciones prohibidas o permitidas enumeradas, haga clic en **Exceptions**, especifique los nombres de los paquetes en la ventana que se abre y haga clic en **Aceptar**.

8. Si desea recibir informes sobre las aplicaciones instaladas, en la sección **Report on installed apps**, seleccione la casilla **Send data on installed apps**. Luego, puede seleccionar las siguientes casillas:

   - **Send data on built-in apps** para enviar datos sobre aplicaciones del sistema.
   - **Send data on service apps** para enviar datos sobre aplicaciones de servicio que no tienen interfaz de usuario y no se pueden iniciar manualmente.

   Si se configura una aplicación del sistema o una aplicación de servicio en la configuración de Control de aplicaciones, los datos de la aplicación se envían independientemente del estado de las casillas.

   Kaspersky Endpoint Security para Android envía datos al registro de eventos cada vez que se instala o elimina una aplicación del dispositivo.

- Si desea configurar las acciones que se realizarán para las aplicaciones seleccionadas, **vaya a la pestaña App management**.

  1. En la tabla **Actions for apps**, haga clic en **Add**.
  2. En la ventana que se abre, haga lo siguiente:

     a. En la sección **Action**, realice una de las siguientes acciones:

     - **Install**. Se solicita al usuario que instale la aplicación.
     - **Remove**. La aplicación se eliminará del dispositivo del usuario.
     - **Recommend installation**. El usuario recibirá la recomendación de instalar la aplicación.

     b. Complete los siguientes campos:

     Utilice solo fuentes legítimas y de confianza. Al configurar los ajustes en esta sección, usted es el único responsable de los posibles riesgos y consecuencias asociados con el uso de fuentes no confiables.

     - **Package name**
     - **App name**
     - **Link**

       Los vínculos a los paquetes de aplicaciones deben comenzar con http:// o https://.

       Para una instalación silenciosa, especifique un vínculo de descarga directo a un archivo APK que inicie una descarga sin la interacción del usuario. Los vínculos a las páginas de tiendas de aplicaciones no son compatibles con la instalación silenciosa. Puede colocar archivos APK en el Servidor web u otra fuente.

     - **Version**

       Este campo es un parámetro de cadena especificado en el formato de expresiones regulares de Oracle. Para obtener más información sobre las expresiones regulares, consulte el sitio web de soporte técnico de Oracle.

       Los campos **Link** y **Version** no se muestran si selecciona **Remove** en el campo **Action**.

     c. Haga clic en **Add**.

     La acción configurada se agrega a la lista.

7. Haga clic en **Aceptar.**
8. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Niveles de protección de dispositivos móviles

Niveles de protección de dispositivos móviles definidos por Kaspersky Security Center

Kaspersky Next Expert View (on-premise) le permite evaluar rápidamente el nivel de protección actual de los dispositivos móviles administrados en la sección **Asset management** → **Mobile** → **Devices**.

Un dispositivo puede tener uno de los siguientes niveles de protección: **OK**, **Warning** o **Critical**.

Los niveles de protección se asignan y se envían a Kaspersky Security Center, de acuerdo con los siguientes requisitos:

- Se detecta un motivo para asignar un nivel de protección en el dispositivo: el dispositivo obtiene el estado que se muestra en la lista de dispositivos administrados.
- Se detectan varios motivos para asignar niveles de protección en el dispositivo: Kaspersky Mobile Devices Protection and Management asigna el estado más crítico.
- No se detectan motivos para asignar un nivel de protección en el dispositivo: Kaspersky Mobile Devices Protection and Management no envía un estado a Kaspersky Security Center y el estado se establece como *OK*.

Niveles de protección y sus significados

Nivel de protección	Significado
OK	No se requiere intervención de un administrador.
Warning	Se registraron eventos relacionados con amenazas posibles o reales para la seguridad de los dispositivos administrados.
Critical	Se han detectado graves problemas. Se requiere la intervención de un administrador para solucionarlos.

El objetivo del administrador es garantizar que el nivel de protección *OK* exista en todos los dispositivos.

Niveles de protección de dispositivos móviles definidos por Kaspersky Mobile Devices Protection and Management

Kaspersky Mobile Devices Protection and Management define el nivel de protección de los dispositivos móviles según la configuración de la directiva y luego envía los niveles de protección a Kaspersky Security Center durante la sincronización. El administrador puede cambiar el nivel de protección en la directiva, según el nivel de seguridad de la condición (consulte la *tabla Valores predeterminados, motivos y condiciones para asignar un nivel de protección en dispositivos Android*). En este caso, el valor establecido por el administrador anula el valor predeterminado definido por Kaspersky Mobile Devices Protection and Management.

Valores predeterminados, motivos y condiciones para asignar un nivel de protección en dispositivos Android

Condición	Motivo del nivel de protección	Valor predeterminado
Real-time protection is not running	Uno de los siguientes motivos: • No se otorgó el permiso Acceso para administrar todos los archivos. • Kaspersky Security Network está desactivado.	*Critical*

Condición	Motivo del nivel de protección	Valor predeterminado
Web Protection and Web Control are not running	Uno de los siguientes motivos: • No se concedió el permiso Accesibilidad. • El usuario desactivó la Protección web en la configuración de Kaspersky Endpoint Security. • No se concedió el permiso Ignorar optimización de la batería. • La Declaración de Protección web no fue aceptada.	*Warning*
App Control is not running	No se concedió el permiso Accesibilidad.	*Warning*
Device lock is not available	Uno de los siguientes motivos: • No se concedió el permiso Administrador del dispositivo. • No se concedió el permiso Accesibilidad. • La aplicación no está habilitada para superponerse a otras ventanas.	*Warning*
Device location is not available	Uno de los siguientes motivos: • No se ha otorgado el permiso Ubicación. • No se puede determinar la ubicación del dispositivo (cuando se concede el permiso).	*Warning*
Versions of the Kaspersky Security Network Statement do not match	La versión de la Declaración de Kaspersky Security Network que el usuario aceptó en la directiva y la versión de la Declaración de Kaspersky Security Network en el dispositivo no coinciden.	*Warning*
Versions of the Marketing Statement do not match	La versión de la Declaración respecto del procesamiento de datos para fines de marketing que el usuario aceptó en la directiva y la versión de la Declaración respecto del procesamiento de datos para fines de marketing en el dispositivo no coinciden.	*OK*

Inventario de software en dispositivos Android

Puede hacer un inventario de las aplicaciones en los dispositivos Android conectados al Servidor de administración. Kaspersky Endpoint Security para Android recibe información sobre todas las aplicaciones instaladas en los dispositivos móviles. La información obtenida durante el inventario se muestra en las propiedades del dispositivo en la sección **Events**. En esta sección, puede ver información detallada sobre cada aplicación instalada.

Para habilitar el inventario de software:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **Android** y vaya a la sección **Security controls**.
4. En la tarjeta **App Control**, haga clic en **Settings**.

   Se abre la ventana **App Control**.
5. En la sección **Report on installed apps**, seleccione la casilla **Send data on installed apps**.
6. Si desea recibir datos sobre las aplicaciones del sistema, seleccione la casilla **Send data on built-in apps**.
7. Si desea recibir datos sobre aplicaciones de servicio, que no tienen una interfaz y el usuario no puede abrirlas, seleccione la casilla **Send data on service apps**.

8. Haga clic en **Aceptar**.

9. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center. Kaspersky Endpoint Security para Android envía datos al registro de eventos cada vez que se instala o elimina una aplicación del dispositivo.

Protección

Esta sección contiene información sobre cómo administrar de forma remota la protección de dispositivos móviles en Kaspersky Next Expert View (on-premise).

Configuración de la protección antimalware en dispositivos Android

Para la detección oportuna de amenazas, virus y otras aplicaciones maliciosas, puede ajustar la configuración de la protección en tiempo real y los análisis de malware automáticos.

Kaspersky Endpoint Security para Android detecta los siguientes tipos de objetos:

- Virus, gusanos, troyanos y herramientas maliciosas
- Adware
- Aplicaciones legítimas que los intrusos pueden usar para poner en riesgo los dispositivos o los datos de los usuarios

El Antimalware tiene varias limitaciones:

- Debido a limitaciones técnicas, Kaspersky Endpoint Security para Android no puede analizar archivos con un tamaño de 2 GB o más. Durante un análisis, la app omite dichos archivos sin notificarle que se omitieron.
- En dispositivos con Android 11 o versiones posteriores, Kaspersky Endpoint Security para Android no puede analizar las carpetas "Android/datos" ni "Android/obb" y detectar malware en ellas debido a limitaciones técnicas.

Configuración de la protección en tiempo real

Para ajustar la configuración de protección en tiempo real para dispositivos móviles, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **Android** y vaya a la sección **Protection**.

4. En la tarjeta **Real-time protection**, haga clic en **Settings**.

   Se abre la ventana **Real-time protection**.

5. Habilite la configuración con el interruptor **Real-time protection**.

   Si este interruptor está activado, la protección del dispositivo móvil está activada y el usuario no puede desactivarla.

   Si este interruptor está desactivado, la protección del dispositivo móvil está activada, pero el usuario puede desactivarla manualmente.

6. En la lista desplegable **App scan**, seleccione el modo de análisis de la aplicación:

   - **Do not scan apps**
   - **Scan only new apps and files from the Downloads folder**
   - **Scan all apps and monitor actions with files**

7. En la lista desplegable **Action on threat detection**, seleccione una de las siguientes opciones:

   - **Delete**

     Los objetos detectados se eliminarán automáticamente. No se requiere que el usuario realice ninguna acción adicional. Antes de eliminar un objeto, Kaspersky Endpoint Security para Android mostrará una notificación temporal para indicar la detección del objeto.

   - **Skip**

     Si se han omitido objetos detectados, Kaspersky Endpoint Security para Android advierte al usuario sobre problemas en la protección del dispositivo. Para cada amenaza omitida, la app sugiere acciones que el usuario puede realizar para eliminarla. La lista de amenazas omitidas puede cambiar, por ejemplo, si se ha eliminado o movido un archivo. Para recibir una lista actualizada de amenazas, ejecute un análisis completo del dispositivo. Para garantizar la protección fiable de sus datos, elimine todos los objetos detectados.

   - **Delete and save a backup copy of file in quarantine**

8. Para habilitar el análisis adicional de las nuevas aplicaciones antes de su primer uso en el dispositivo del usuario con el servicio en la nube de Kaspersky Security Network, seleccione la casilla **Additional protection by Kaspersky Security Network**.

9. Para bloquear adware y aplicaciones que pueden usar delincuentes para dañar el dispositivo o los datos del usuario, seleccione la casilla **Detect adware, autodialers, and legitimate apps that intruders can use to compromise the user's device and data**.

10. Haga clic en **Aceptar**.

11. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Configurar análisis de malware automáticos

Para configurar una ejecución automática del análisis de malware en el dispositivo móvil, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **Android** y vaya a la sección **Protection**.

4. En la tarjeta **Scan**, haga clic en **Settings**.

   Se abre la ventana **Scan**.

5. Habilite la configuración con el interruptor **Scan**.

6. En la lista **Action on threat detection**, seleccione una de las siguientes opciones:

   - **Delete**

     Los objetos detectados se eliminarán automáticamente. No se requiere que el usuario realice ninguna acción adicional. Antes de eliminar un objeto, Kaspersky Endpoint Security para Android mostrará una notificación temporal para indicar la detección del objeto.

   - **Skip**

     Si se han omitido objetos detectados, Kaspersky Endpoint Security para Android advierte al usuario sobre problemas en la protección del dispositivo. Para cada amenaza omitida, la app sugiere acciones que el usuario puede realizar para eliminarla. La lista de amenazas omitidas puede cambiar, por ejemplo, si se ha eliminado o movido un archivo. Para recibir una lista actualizada de amenazas, ejecute un análisis completo del dispositivo. Para garantizar la protección fiable de sus datos, elimine todos los objetos detectados.

   - **Delete and save a backup copy of file in quarantine**

   - **Ask user**

     Kaspersky Endpoint Security para Android muestra una notificación para que el usuario elija la acción que debe hacerse con el objeto detectado: **Skip** o **Delete**.

     Kaspersky Endpoint Security para Android debe estar configurado como función de accesibilidad para garantizar la visualización de las notificaciones en dispositivos móviles que ejecutan Android 10 o posterior. Kaspersky Endpoint Security para Android solicita al usuario que configure la app como una función de Accesibilidad a través del Asistente de configuración inicial. El usuario puede omitir este paso o desactivar este servicio en la configuración del dispositivo más adelante. En este caso, Kaspersky Endpoint Security para Android muestra una ventana del sistema Android que solicita al usuario elegir la acción que debe realizarse con el objeto detectado: Omitir o Eliminar. Para realizar una acción en varios objetos, debe abrir Kaspersky Endpoint Security.

Si durante un análisis, Kaspersky Endpoint Security para Android detecta aplicaciones maliciosas en los dispositivos de los usuarios, las acciones difieren según el **modo de administración del dispositivo**.

En los dispositivos corporativos, las aplicaciones maliciosas instaladas detectadas por Kaspersky Endpoint Security para Android se eliminan del dispositivo automáticamente si se selecciona la opción **Delete**. Si Kaspersky Endpoint Security para Android detecta aplicaciones maliciosas del sistema, se prohíbe que se muestren y se ejecuten en los dispositivos de los usuarios.

En un contenedor corporativo, las aplicaciones maliciosas instaladas detectadas por Kaspersky Endpoint Security para Android no se eliminan, pero se prohíbe que se muestren y se ejecuten en los dispositivos de los usuarios sin notificar a los usuarios del dispositivo.

Si se selecciona la opción **Ask user**, Kaspersky Endpoint Security para Android solicita a los usuarios que seleccionen una acción para cada aplicación detectada, tanto en dispositivos corporativos como en dispositivos con un contenedor corporativo.

Las aplicaciones malintencionadas instaladas no se pueden poner en cuarentena. En consecuencia, si se selecciona la opción **Delete and save a backup copy of file in quarantine**, se elimina la aplicación maliciosa detectada.

En los dispositivos personales, las aplicaciones maliciosas detectadas no se pueden eliminar automáticamente. En este caso, Kaspersky Endpoint Security para Android solicita al usuario que elimine u omita la aplicación detectada.

7. En el campo **Scheduled scan**, puede configurar lo ajustes para el lanzamiento automático de un análisis completo del sistema de archivos del dispositivo.

8. Si seleccionó un análisis semanal o diario, especifique el día de la semana (para los análisis semanales) y la hora de inicio en los campos **Day** y **Time**.

   Si el dispositivo está en modo de ahorro de batería, la aplicación puede realizar esta tarea más tarde de lo especificado.

9. Haga clic en **Aceptar**.

10. Haga clic en el botón **Save** para guardar los cambios que realizó.

    La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center. Kaspersky Endpoint Security para Android analiza todos los archivos, incluido el contenido de los archivos.

Para mantener actualizada la protección del dispositivo móvil, configure la actualización de la base de datos antimalware.

De manera predeterminada, las actualizaciones de la base de datos antimalware se deshabilitan cuando el dispositivo está en itinerancia. No se realizan actualizaciones programadas de las bases de datos antimalware.

Configurar actualizaciones de la base de datos

Para configurar las actualizaciones de la base de datos antimalware, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **Android** y vaya a la sección **Protection**.

4. En la tarjeta **Database update**, haga clic en **Settings**.

   Se abre la ventana **Database update**.

5. Habilite la configuración con el interruptor **Database update**.

6. En el campo **Scheduled database update**, puede configurar las opciones para actualizaciones automáticas de la base de datos antimalware en el dispositivo del usuario.

7. Si seleccionó una actualización datos semanal o diaria, especifique el día de la semana (para las actualizaciones semanales de la base de datos) y la hora de inicio en los campos **Day** y **Time**.

   Si el dispositivo está en modo de ahorro de batería, la aplicación puede realizar esta tarea más tarde de lo especificado.

8. En la sección **Database update source**, especifique el origen de las actualizaciones desde donde Kaspersky Endpoint Security para Android recibe e instala las actualizaciones de las bases de datos antimalware:

   - **Kaspersky servers**

     Utilización de un servidor de actualización Kaspersky como origen de actualizaciones para descargar las bases de datos de Kaspersky Endpoint Security para Android en los dispositivos móviles de los usuarios. Para actualizar las bases de datos con los servidores de Kaspersky, Kaspersky Endpoint Security para Android transmite datos a Kaspersky (por ejemplo, el ID de la tarea de actualización misma). La lista de datos que se transmite durante las actualizaciones de la base de datos se indica en el Contrato de licencia de usuario final.

   - **Administration Server**

     Utilización del repositorio del servidor de administración de Kaspersky Security Center como origen de actualizaciones para descargar las bases de datos de Kaspersky Endpoint Security para Android en los dispositivos móviles de los usuarios.

   - **Other source**

     Utilización de un servidor de terceros como origen de actualizaciones para descargar las bases de datos de Kaspersky Endpoint Security para Android en los dispositivos móviles de los usuarios. Para iniciar una actualización, debe introducir la dirección de un servidor HTTP en el campo siguiente (por ejemplo, `http://domain.com/`).

9. Si desea que Kaspersky Endpoint Security para Android descargue actualizaciones de la base de datos según el programa de actualización cuando el dispositivo está en itinerancia, seleccione la casilla **Allow database update while roaming** de la sección **Database update while roaming**.

   Aunque la casilla no esté seleccionada, el usuario puede iniciar manualmente una actualización de la base de datos antimalware cuando el dispositivo está en itinerancia.

10. Haga clic en **Aceptar**.

11. Haga clic en el botón **Save** para guardar los cambios que realizó.

    La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Protección de dispositivos Android en Internet

Puede utilizar Protección web para proteger los datos personales de los usuarios de dispositivos móviles en Internet. La Protección web bloquea los sitios web maliciosos que distribuyen códigos maliciosos, además de los sitios web de phishing diseñados para robar sus datos confidenciales y obtener acceso a sus cuentas financieras. Protección Web utiliza el servicio en la nube de Kaspersky Security Network para analizar sitios web antes de abrirlos. La Protección web está habilitada de manera predeterminada.

En Yandex Browser y Samsung Internet, las URL maliciosas y de phishing pueden permanecer desbloqueadas. Esto se debe a que solo se realiza el análisis del dominio del sitio web. Si se trata de un dominio malicioso o de phishing, Protección web bloquea la amenaza. Si el dominio no está clasificado como malicioso o como phishing, la URL específica no se bloquea.

La Protección web en dispositivos Android solo es compatible con Google Chrome, el navegador HUAWEI, Samsung Internet y Yandex Browser.

La Protección web requiere lo siguiente para funcionar en un dispositivo administrado:

- Se debe configurar Kaspersky Endpoint Security for Android como un Servicio de accesibilidad.

  En dispositivos corporativos, si Kaspersky Endpoint Security para Android no está habilitado como una función de accesibilidad, Protección web solo es compatible con Google Chrome y solo verifica el dominio de un sitio web. Para permitir que otros navegadores (Samsung Internet, Yandex Browser y HUAWEI Browser) admitan Protección web, habilite Kaspersky Endpoint Security como una función de accesibilidad.

- Se debe aceptar la Declaración con respecto al procesamiento de datos para el uso de la Protección web (Declaración de Protección web). Kaspersky Endpoint Security usa Kaspersky Security Network (KSN) para analizar sitios web. La Declaración de Protección web contiene los términos del intercambio de datos con KSN.

- En algunos dispositivos, el usuario debe conceder de forma manual los siguientes permisos:

  - **Ejecutar en segundo plano**

  - **Mostrar ventanas emergentes mientras se ejecuta en segundo plano**

- **Mostrar ventana emergente**
- **Ignorar la optimización de la batería**

La Protección web para HUAWEI Browser, Samsung Internet y Yandex Browser no bloquea sitios en un dispositivo móvil si se utiliza un contenedor corporativo y la Protección web está habilitada solo para el contenedor corporativo.

Para activar la Protección web:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **Android** y vaya a la sección **Protection**.
4. En la tarjeta **Web Protection**, habilite la configuración con el interruptor **Web Protection**.
5. Haga clic en **Enable**.

   Si desactiva Protección web, Control web también se desactivará.

   La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Análisis de notificaciones de servicios de mensajería instantánea

Kaspersky Endpoint Security para Android puede detectar URL maliciosas y de phishing en las notificaciones de Telegram, WhatsApp, la aplicación de SMS predeterminada y otras aplicaciones de servicio de mensajería instantánea habituales. Solo se pueden analizar las URL expresadas como texto directamente en el texto de la notificación. Las direcciones URL incrustadas en marcas no se analizan.

Deben cumplirse las siguientes condiciones para habilitar el análisis de notificaciones:

- La Protección web debe estar habilitada.
- La visualización de notificaciones debe estar permitida para los servicios de mensajería instantánea deseados. Kaspersky Endpoint Security para Android analiza únicamente las notificaciones que pueden mostrarse en la pantalla del dispositivo.
- En los dispositivos Google Pixel y Vivo, se debe conceder el permiso "Conversaciones" a Kaspersky Endpoint Security en la configuración de acceso a notificaciones.

Para habilitar el análisis de notificaciones, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **Android** y vaya a la sección **Protection**.
4. En la tarjeta **Web Protection**, seleccione la casilla **Block notifications that contain malicious and phishing URLs**.
5. Para permitir el acceso a las notificaciones en un dispositivo móvil, consulte la sección Protección web.

La aplicación analiza ahora las notificaciones para detectar URL maliciosas y de phishing. Si se encuentra una URL peligrosa, la notificación se bloquea y aparece una pantalla de bloqueo con información sobre la notificación bloqueada.

Si Kaspersky Endpoint Security para Android no está habilitada como función de Accesibilidad, la aplicación envía una notificación push sobre las URL peligrosas detectadas en lugar de mostrar una pantalla de bloqueo. Tras tocar la notificación push, aparece una pantalla con información sobre la notificación bloqueada.

Protección de datos en un dispositivo robado o perdido

Esta sección describe cómo puede configurar las opciones de protección contra acceso no autorizado en caso de que el dispositivo se pierda o sea robado.

Enviar comandos a un dispositivo móvil perdido o robado

Para proteger los datos de un dispositivo móvil perdido o robado, puede enviar comandos especiales.

Puede enviar comandos a los siguientes tipos de dispositivos móviles administrados:

- Dispositivos Android administrados a través de la aplicación Kaspersky Endpoint Security para Android
- Dispositivos MDM con iOS

Cada tipo de dispositivo admite un conjunto específico de comandos (consulte las tablas a continuación).

Comandos para dispositivos Android

Comandos para proteger datos de un dispositivo Android perdido o robado

Comando	Resultado
Lock device	El dispositivo móvil está bloqueado. Para obtener acceso a los datos, debe desbloquear el dispositivo mediante el comando **Unlock device** o un código de acceso único.
Unlock device	El dispositivo móvil se desbloquea. Después de desbloquear un dispositivo con Android 5 a 6, la contraseña de desbloqueo de la pantalla se restablece a "1234". Después de desbloquear un dispositivo con Android 7 o versiones posteriores, la contraseña de desbloqueo de la pantalla no se modifica.
Reset to factory settings	Se eliminarán todos los datos del dispositivo móvil y se restablecerá la configuración de fábrica. Después de que este comando se ejecute, el dispositivo no podrá recibir o ejecutar comandos subsecuentes. Este comando no está disponible para dispositivos personales y dispositivos con un contenedor corporativo con Android 14 o posterior.
Wipe corporate data	Los datos corporativos se eliminan del dispositivo. La lista de datos eliminados depende del modo en el que esté funcionando el dispositivo: • En un dispositivo personal, se eliminan el contenedor de Knox, los archivos corporativos enviados al dispositivo y el certificado de correo. • En un dispositivo corporativo, el contenedor de Knox, los archivos corporativos enviados al dispositivo y los certificados instalados por Kaspersky Endpoint Security para Android (certificados de correo, VPN y perfil SCEP, excepto los certificados móviles) se eliminan. • Además, si se creó un contenedor corporativo, el contenedor corporativo (su contenido, archivos corporativos enviados al dispositivo, configuraciones y restricciones) y los certificados instalados en el contenedor corporativo (certificados de correo, VPN y perfil SCEP, excepto los certificados móviles) se eliminan.
Locate device	Se obtienen las coordenadas de la ubicación del dispositivo móvil. Para ver la ubicación del dispositivo en Yandex.Maps, vaya a la sección **Asset management** → **Mobile** → **Devices**. Luego, elija un dispositivo y seleccione **Command history** → **Locate device** → **Device coordinates** → **View on map**. Después de hacer clic en **View on map**, las coordenadas del dispositivo se transfieren a Yandex.Maps y el dispositivo se muestra en un mapa. En dispositivos con Android 12 o posterior, si el usuario otorgó el permiso "Usar ubicación aproximada", la aplicación Kaspersky Endpoint Security para Android primero intenta obtener la ubicación precisa del dispositivo. Si esto no es posible, se devuelve la ubicación aproximada del dispositivo solo si se recibió en los últimos 30 minutos. De lo contrario, el comando falla. Este comando no funciona en dispositivos Android si la Precisión de ubicación de Google está deshabilitada en la configuración. Tenga en cuenta que no todos los dispositivos Android vienen con esta configuración de ubicación.
Take photos	El dispositivo móvil está bloqueado. Se toman fotos con la cámara frontal del dispositivo cuando alguien intenta desbloquear el dispositivo. En dispositivos con una cámara frontal emergente, la foto será negra si la cámara está guardada. Al intentar desbloquear el dispositivo, el usuario acepta automáticamente que se le tome una foto en el dispositivo. Si se revocó el permiso para usar la cámara, el dispositivo móvil muestra una notificación y le pide que proporcione el permiso. En un dispositivo móvil con Android 12 o posterior, si se revocó el permiso para usar la cámara a través de la Configuración rápida, la notificación no se muestra, pero la foto tomada es negra.
Sound alarm	El dispositivo móvil hace sonar una alarma durante 5 minutos (durante 1 minuto si la batería del dispositivo está baja) o hasta que el usuario desbloquee el dispositivo.

Comando	Resultado
Wipe app data	Los datos de una aplicación especificada se eliminan del dispositivo móvil. Para esta acción, debe especificar el nombre del paquete para la aplicación cuyos datos se eliminarán. Como resultado, la aplicación se revierte a su estado predeterminado. Los datos del sistema y las aplicaciones administrativas no se eliminan.
Wipe data of all apps	Los datos de todas las aplicaciones se eliminan del dispositivo móvil. En un dispositivo corporativo, se eliminan los datos de todas las aplicaciones en el dispositivo. En un dispositivo con un contenedor corporativo, se eliminan los datos de todas las aplicaciones en el contenedor corporativo. Como resultado, las aplicaciones vuelven a su estado predeterminado. Los datos del sistema y las aplicaciones administrativas no se eliminan.
Get location history	Se muestra el historial de ubicaciones del dispositivo móvil durante los últimos 14 días. Para ver la ubicación del dispositivo en Yandex.Maps, vaya a la sección **Asset management** → **Mobile** → **Devices**. Luego, elija un dispositivo y seleccione **Command history** → **Get location history** → **View on map**. Después de hacer clic en **View on map**, las coordenadas del dispositivo se transfieren a Yandex.Maps y el dispositivo se muestra en un mapa. Debido a las limitaciones técnicas de los dispositivos Android, es posible que la ubicación del dispositivo se recupere con menos frecuencia de la especificada en la configuración **Location tracking**.

Comandos para dispositivos MDM con iOS

Comandos para proteger datos de un dispositivo MDM con iOS perdido o robado

Comando	Resultado
Lock device	El dispositivo móvil está bloqueado. Para acceder a los datos, debe desbloquear el dispositivo.
Reset unlock password	Se restablece la contraseña de desbloqueo de la pantalla del dispositivo móvil y se le solicita al usuario que establezca una nueva contraseña de acuerdo con los requisitos de la directiva.
Reset to factory settings	Se eliminarán todos los datos del dispositivo móvil y se restablecerá la configuración de fábrica. Después de que este comando se ejecute, el dispositivo no podrá recibir o ejecutar comandos subsecuentes.
Wipe corporate data	Todos los perfiles de configuración instalados, los perfiles de aprovisionamiento, el perfil de administración y las aplicaciones para las que se seleccionó la casilla **Remove when device management profile is deleted** se eliminan del dispositivo.
Enable Lost Mode (supervised only)	El modo perdido se habilita en el dispositivo móvil supervisado y se bloquea el dispositivo. La pantalla del dispositivo muestra un mensaje y un número de teléfono que puede editar. Si envía el comando **Habilitar modo perdido** a un dispositivo MDM con iOS supervisado sin una tarjeta SIM y este dispositivo se reinicia, el dispositivo no podrá conectarse a Wi-Fi y recibir el comando **Deshabilitar modo perdido**. Esta es una característica específica de los dispositivos iOS. Para evitar este problema, puede enviar el comando solo a dispositivos con una tarjeta SIM o insertar una tarjeta SIM en el dispositivo bloqueado para permitirle recibir el comando **Deshabilitar modo perdido** a través de la red móvil.
Locate device (Lost Mode only)	Se obtiene la ubicación del dispositivo móvil. Para ver la ubicación del dispositivo en Yandex.Maps, vaya a la sección **Asset management** → **Mobile** → **Devices**. Luego, elija un dispositivo y seleccione **Command history** → **Locate device** → **Device coordinates** → **View on map**. Después de hacer clic en **View on map**, las coordenadas del dispositivo se transfieren a Yandex.Maps y el dispositivo se muestra en un mapa.

Comando	Resultado
Sound alarm (Lost Mode only)	Se reproduce un sonido en el dispositivo móvil perdido.
Disable Lost Mode (supervised only)	El modo perdido se deshabilita en el dispositivo móvil y se desbloquea el dispositivo.

Permisos para la ejecución de comandos

Se requieren derechos y permisos especiales para ejecutar comandos de Kaspersky Endpoint Security para Android. Mientras se ejecuta el Asistente de configuración inicial, Kaspersky Endpoint Security para Android le pide al usuario que otorgue a la aplicación todos los permisos y derechos necesarios. El usuario puede omitir estos pasos o deshabilitar estos permisos más adelante en la configuración del dispositivo. Si este es el caso, será imposible ejecutar comandos.

En dispositivos con Android 10 o posterior, el usuario debe otorgar el permiso "Todo el tiempo" para acceder a la ubicación. En dispositivos con Android 11 o posterior, el usuario también debe otorgar el permiso "Mientras se usa la aplicación" para acceder a la cámara. De lo contrario, los comandos de antirrobo no funcionarán. Se notificará al usuario esta limitación y se le volverá a pedir que otorgue el nivel requerido de los permisos. Si el usuario selecciona la opción "Solo esta vez" para el permiso de la cámara, la aplicación considerará el permiso como otorgado. Se recomienda comunicarse con el usuario directamente si se vuelve a pedir el permiso de la cámara.

Para obtener la lista completa de comandos disponibles, consulte Comandos para dispositivos móviles. Para obtener más información sobre el envío de comandos desde la Consola de administración, consulte la sección Enviar comandos.

Desbloqueo del dispositivo móvil

Puede desbloquear un dispositivo móvil con los siguientes métodos:

- Enviar el comando de desbloqueo de dispositivo móvil
- Ingrese el código de acceso único en el dispositivo móvil (solo para dispositivos Android)

En ciertos dispositivos (por ejemplo, HUAWEI, Meizu y Xiaomi), debe agregar manualmente Kaspersky Endpoint Security para Android a la lista de aplicaciones que se inician al iniciarse el sistema operativo. Si la aplicación no se agrega a la lista, puede desbloquear el dispositivo con tan solo utilizar un código de acceso único. No puede usar comandos para desbloquear el dispositivo.

Para obtener más información sobre el envío de comandos desde la lista de dispositivos móviles de Kaspersky Next Expert View (on-premise), consulte la sección Enviar comandos.

Un código de acceso único es un código secreto para desbloquear el dispositivo móvil. El código de acceso lo genera Kaspersky Security Center y es único para cada dispositivo móvil. Puede cambiar la longitud del código de acceso único (4, 8, 12 o 16 dígitos) en la configuración **Anti-Theft** de la directiva.

Para desbloquear un dispositivo móvil con un código de acceso único, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.
2. Haga clic en el dispositivo móvil para el cual desea recibir un código de acceso único.
3. Seleccione **Applications** → **Kaspersky Mobile Devices Protection and Management**.

   Se abre la ventana de propiedades de Kaspersky Mobile Devices Protection and Management.
4. Seleccione la pestaña **Application settings**.

   Se muestra un código de acceso único para el dispositivo seleccionado en el campo **One-time code** de la sección **One-time device passcode**.
5. Use cualquier método disponible (por ejemplo, correo electrónico) para comunicar el código de acceso único al usuario del dispositivo bloqueado.

   El usuario debe ingresar el código de acceso único en la pantalla del dispositivo bloqueado por Kaspersky Endpoint Security para Android.

El dispositivo móvil del usuario se desbloquea.

Después de desbloquear un dispositivo con Android 5 a 6, la contraseña de desbloqueo de la pantalla se restablece a "1234". Después de desbloquear un dispositivo con Android 7 o versiones posteriores, la contraseña de desbloqueo de la pantalla no se modifica.

Para cambiar la longitud del código de acceso único del dispositivo, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **Android** y vaya a la sección **Protection**.
4. En la tarjeta **Anti-Theft**, haga clic en **Settings**.

   Se abre la ventana **Anti-Theft**.
5. Seleccione la longitud del código de acceso único del dispositivo en la lista desplegable correspondiente. De manera predeterminada, el código de acceso tiene 4 dígitos.
6. Si desea comunicarse con la persona que encuentra el dispositivo móvil, en el campo **Text displayed on locked device**, ingrese el texto del mensaje que se mostrará en la pantalla de bloqueo.
7. Haga clic en **Aceptar**.
8. Haga clic en el botón **Save** para guardar los cambios que realizó.

La longitud del código de acceso único se establece con el valor seleccionado.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Configuración de seguridad de la contraseña de desbloqueo del dispositivo

Para proteger el acceso al dispositivo móvil de un usuario, se debería establecer una contraseña de desbloqueo.

Esta sección contiene la información sobre cómo configurar la protección con contraseña en dispositivos iOS y Android.

Configuración de una contraseña de desbloqueo segura para un dispositivo Android

Para mantener un dispositivo Android seguro, debe configurar el uso de una contraseña que se le solicita al usuario que ingrese al desbloquear el dispositivo.

Puede imponer restricciones a la actividad del usuario en el dispositivo si la contraseña de desbloqueo es débil (por ejemplo, al bloquear el dispositivo). Puede imponer restricciones usando el componente Control de cumplimiento. Para hacerlo, en la configuración de la regla de análisis, debe seleccionar el criterio **Unlock password doesn't comply with security requirements**.

En ciertos dispositivos Samsung con Android 7 o versiones posteriores, cuando el usuario intenta configurar métodos no admitidos para desbloquear el dispositivo (por ejemplo, una contraseña gráfica), el dispositivo se puede bloquear si se satisfacen las siguientes condiciones: la protección de eliminación de está habilitada para Kaspersky Endpoint Security para Android y se establecieron requisitos de seguridad de la contraseña de desbloqueo de la pantalla. Para desbloquear el dispositivo, debe enviar un comando especial al dispositivo.

Ajustar la configuración de la contraseña de desbloqueo

Para configurar una contraseña de desbloqueo:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **Android** y vaya a la sección **Security controls**.
4. En la tarjeta **Screen unlock settings**, haga clic en **Settings**.

   Se abre la ventana **Screen unlock settings**.
5. Habilite la configuración con el interruptor **Screen unlock settings**, si desea que la aplicación verifique si se estableció una contraseña de desbloqueo.

   El interruptor de esta tarjeta no habilita ni deshabilita la funcionalidad correspondiente en los dispositivos. Habilitar el interruptor le permite utilizar configuraciones personalizadas. Deshabilitar el interruptor le permite usar la configuración predeterminada.

   Si la aplicación detecta que no estableció la contraseña del sistema en el dispositivo, le pedirá al usuario que lo haga. La contraseña se configura según los parámetros que define el administrador.

6. Especifique las siguientes opciones, si es necesario:

- **Minimum password length**

  La cantidad mínima de caracteres en la contraseña del usuario. Valores posibles: 4 a 16 caracteres.

  De manera predeterminada, la contraseña del usuario tiene 4 caracteres.

  Lo siguiente se aplica solo al espacio personal del usuario y al contenedor corporativo:

  - En el espacio personal del usuario, Kaspersky Endpoint Security convierte los requisitos de seguridad de la contraseña en uno de los valores disponibles en el sistema: medio o alto en dispositivos con Android 10 o posterior.

  - En el contenedor corporativo, Kaspersky Endpoint Security convierte los requisitos de seguridad de la contraseña en uno de los valores disponibles en el sistema: medio o alto en dispositivos con Android 12 o posterior.

  Los valores se determinan mediante las siguientes reglas:

  - Si la extensión de la contraseña requerida es de 1 a 4 caracteres, la app solicitará que el usuario establezca una contraseña con seguridad media. Debe ser o numérica (PIN) con una secuencia que no tenga números repetidos u ordenados en secuencias (por ejemplo, 1234), o alfabética/alfanumérica. El PIN o la contraseña debe tener al menos 4 caracteres.

  - Si la extensión de la contraseña requerida es de 5 caracteres o más, la app solicitará que el usuario establezca una contraseña con seguridad alta. Debe ser o numérica (PIN) con una secuencia que no tenga números repetidos u ordenados, o alfabética/alfanumérica (contraseña). Un PIN debe tener al menos 8 dígitos. La contraseña debe tener al menos 6 caracteres.

- **Minimum password complexity requirements**

  Especifica los requisitos mínimos de la contraseña de desbloqueo. Estos requisitos se aplican solo a las nuevas contraseñas de usuario. Están disponibles los siguientes valores:

  - **Numeric**

    El usuario puede establecer una contraseña que incluya números o establecer una contraseña más segura (por ejemplo, una contraseña alfabética o alfanumérica).

    Esta opción se selecciona de forma predeterminada.

  - **Alphabetic**

    El usuario puede establecer una contraseña que incluya letras (u otros símbolos que no sean números) o establecer una contraseña más segura (por ejemplo, una contraseña alfanumérica).

  - **Alphanumeric**

    El usuario puede establecer una contraseña que incluya tanto números como letras (u otros símbolos que no sean números) o establecer una contraseña compleja más segura.

  - **No requirements**

    El usuario puede establecer cualquier contraseña.

  - **Complex**

    El usuario debe establecer una contraseña compleja de acuerdo con las propiedades de contraseña especificadas:

    - **Minimum number of letters**

    - **Minimum number of digits**

- **Minimum number of special characters**
- **Minimum number of lowercase letters**
- **Minimum number of uppercase letters**
- **Minimum number of non-alphabetic characters**

- **Complex numeric**

  El usuario puede establecer una contraseña que incluya números sin repeticiones (por ejemplo, 4444) ni secuencias ordenadas (por ejemplo, 1234, 4321, 2468) o establecer una contraseña compleja más segura.

- **Maximum password lifetime (days)**

  Especifica la cantidad de días antes de que caduque la contraseña. La aplicación de un nuevo valor establecerá la duración de la contraseña actual al nuevo valor.

  El valor predeterminado es 0. Esto significa que la contraseña no caducará.

- **Number of days to send a notification before a required password change**

  Especifica la cantidad de días para notificar al usuario antes de que caduque la contraseña.

  El valor predeterminado es 0. Esto significa que no se notificará al usuario sobre la caducidad de la contraseña.

- **Number of recent passwords that cannot be set as a new password**

  Especifica el número máximo de contraseñas de usuario anteriores que no se pueden usar como una nueva contraseña. Esta configuración se aplica solo cuando el usuario establece una nueva contraseña en el dispositivo.

  El valor predeterminado es 0. Esto significa que la nueva contraseña de usuario puede coincidir con cualquier contraseña anterior, excepto la actual.

- **Period of inactivity before the screen locks (sec)**

  Especifica el período de inactividad antes de que el dispositivo se bloquee.

  El valor predeterminado es 0. Esto significa que el dispositivo no se bloqueará después de un período determinado.

- **Period after biometric unlock before password must be entered (min)**

  Especifica el período para desbloquear el dispositivo sin contraseña. Durante este período, el usuario puede usar métodos biométricos para desbloquear la pantalla. Después de este período, el usuario puede desbloquear la pantalla solo con una contraseña.

  El valor predeterminado es 0. Esto significa que el usuario no se verá obligado a desbloquear el dispositivo con una contraseña después de un período determinado.

- **Allow biometric unlock methods**

  Si la casilla está marcada, se autoriza el uso de métodos de desbloqueo biométricos en el dispositivo móvil.

  Si la casilla está desactivada, Kaspersky Endpoint Security para Android bloquea el uso de métodos biométricos para desbloquear la pantalla. El usuario puede desbloquear la pantalla solo con una contraseña.

  Esta casilla está marcada por defecto.

- **Allow fingerprint unlock**

  Especifica si se pueden usar huellas digitales para desbloquear la pantalla.

  > Esta casilla no restringe el uso de un escáner de huellas digitales al iniciar sesión en apps o confirmar compras.

  Si se selecciona la casilla, se permite el uso de huellas digitales en el dispositivo móvil.

  Si la casilla está desmarcada, Kaspersky Endpoint Security para Android bloquea el uso de huellas digitales para desbloquear la pantalla. El usuario puede desbloquear la pantalla solo con una contraseña. En la configuración del dispositivo, la opción de usar huellas digitales no estará disponible.

  Esta casilla solo está disponible si la casilla **Allow biometric unlock methods** está marcada.

  Esta casilla está marcada por defecto.

  > En algunos dispositivos Xiaomi con un contenedor corporativo, el contenedor corporativo puede desbloquearse mediante una huella digital solo si establece el valor **Period of inactivity before corporate container is locked (sec)** después de establecer una huella digital como el método de desbloqueo de pantalla.

- **Allow face unlock**

  Si la casilla está marcada, se autoriza el uso de reconocimiento facial en el dispositivo móvil.

  Si la casilla está desactivada, Kaspersky Endpoint Security para Android bloquea el uso de reconocimiento facial para desbloquear la pantalla.

  Esta casilla solo está disponible si la casilla **Allow biometric unlock methods** está marcada.

  Esta casilla está marcada por defecto.

- **Allow iris scanning**

  Si la casilla está marcada, se autoriza el uso de reconocimiento de iris en el dispositivo móvil.

  Si la casilla está desactivada, Kaspersky Endpoint Security para Android bloquea el uso de reconocimiento de iris para desbloquear la pantalla.

  Esta casilla solo está disponible si la casilla **Allow biometric unlock methods** está marcada.

  Esta casilla está marcada por defecto.

- **Reset to factory settings after failed attempts to enter password**

  Permite limitar la cantidad de intentos para ingresar la contraseña de desbloqueo de la pantalla.

  Si la casilla está marcada, la aplicación borra todos los datos del dispositivo si el usuario no puede ingresar la contraseña correcta luego del número de intentos especificado.

  Si la casilla está desactivada, no se limita el número de ingresos de la contraseña.

  La casilla está desactivada de manera predeterminada.

- **Maximum number of failed password attempts**

  Especifica el número de intentos para ingresar la contraseña que el usuario puede realizar para desbloquear el dispositivo. El valor predeterminado es 8. El valor máximo disponible es 20.

  El campo está disponible si se selecciona la casilla **Reset to factory settings after failed attempts to enter password**.

- **Set new password**

  Esta opción le permite establecer la contraseña en el dispositivo corporativo del usuario.

  Haga clic en este botón para abrir la ventana **New screen unlock password** e ingrese una nueva contraseña.

  La complejidad de la contraseña ingresada debe cumplir con los requisitos configurados anteriormente en la tarjeta **Screen unlock settings** de la directiva.

  Luego de guardar la directiva, esta opción se aplicará al dispositivo mediante el envío de un comando con la contraseña especificada. La entrada se borra y la contraseña especificada no se guarda en la Consola de administración.

  - Si el dispositivo no está protegido con la contraseña o si ejecuta Android 10 o una versión anterior, Kaspersky Endpoint Security para Android define la contraseña de inmediato.

  - Si el dispositivo está protegido con la contraseña o ejecuta Android 11 o versiones posteriores, Kaspersky Endpoint Security para Android le solicita al usuario que aplique la nueva contraseña.

  Si deja esta opción vacía, no se aplican cambios en el dispositivo.

7. Haga clic en **Aceptar**.

8. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Establecer una nueva contraseña de desbloqueo

Para establecer una nueva contraseña en el dispositivo corporativo de un usuario, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **Android** y vaya a la sección **Restrictions**.

4. En la tarjeta **New screen unlock password**, haga clic en **Settings**.

   Se abre la ventana **New screen unlock password**.

5. Habilite la configuración con el interruptor **New screen unlock password**.

6. Ingrese una nueva contraseña que se utilizará para desbloquear el dispositivo móvil del usuario. Esta contraseña debe cumplir con la configuración actual de la contraseña de desbloqueo de pantalla.

7. Si desea editar la configuración actual de la contraseña de desbloqueo, haga clic en el botón **Configure screen unlock settings**.

   En la ventana **Screen unlock settings** que se abre, configure los ajustes de la contraseña de desbloqueo de pantalla, si es necesario.

8. Haga clic en **Aceptar**.

Si el dispositivo no está protegido con una contraseña o si ejecuta Android 10 o una versión anterior, Kaspersky Endpoint Security para Android define la contraseña de inmediato. Si el dispositivo está protegido con la contraseña o ejecuta Android 11 o versiones posteriores, Kaspersky Endpoint Security para Android le solicita al usuario que aplique la nueva contraseña.

9. Haga clic en el botón **Save** para guardar los cambios que realizó.

La nueva contraseña se establece en el dispositivo móvil del usuario. La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Configurar un código PIN en dispositivos HUAWEI

Algunos dispositivos HUAWEI muestran un mensaje en el que se indica que el método de desbloqueo de pantalla es demasiado simple.

Para establecer un código PIN aceptable en un dispositivo HUAWEI, el usuario debe hacer lo siguiente:

1. En el mensaje sobre el problema, toque el botón **Editar**.
2. Ingrese el código PIN actual.
3. En la ventana **Establecer nueva contraseña**, toque el botón **Cambiar método de desbloqueo**.
4. Seleccione el método de desbloqueo **PIN personalizado**.
5. Configure el nuevo código PIN.

El código PIN debe cumplir con los requisitos de la directiva.

Se estableció un código PIN aceptable en el dispositivo.

Configuración de una contraseña de desbloqueo segura para un dispositivo MDM con iOS

Esta configuración se aplica a los dispositivos supervisados y a los dispositivos que funcionan en el modo de control básico.

Para proteger la información del dispositivo iOS con MDM, configure las opciones de seguridad de la contraseña de desbloqueo.

De forma predeterminada, el usuario puede usar una contraseña sencilla. Las *contraseñas simples* contienen caracteres sucesivos o repetidos, como "abcd" o "2222". No es necesario que el usuario introduzca una contraseña alfanumérica que incluya símbolos especiales. De forma predeterminada, el período de validez de la contraseña y la cantidad de ingresos de la contraseña no están limitados.

Para configurar las opciones de seguridad de la contraseña de desbloqueo de dispositivos MDM con iOS, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **iOS** y vaya a la sección **Security controls**.

4. En la tarjeta **Screen unlock settings**, haga clic en **Settings**.

   Se abre la ventana **Screen unlock settings**.

5. Habilite la configuración con el interruptor **Screen unlock settings**.

   El interruptor de esta tarjeta no habilita ni deshabilita la funcionalidad correspondiente en los dispositivos. Habilitar el interruptor le permite utilizar configuraciones personalizadas. Deshabilitar el interruptor le permite usar la configuración predeterminada.

6. Configure las opciones de seguridad de la contraseña de desbloqueo:

   - Para permitir al usuario utilizar una contraseña sencilla, active la casilla **Allow simple password**. Incluso si esta casilla no está marcada, el usuario puede establecer una contraseña con menos de 6 caracteres.

     Si solo se selecciona la casilla **Allow simple password**, no se solicitará ninguna contraseña. Para pedirle al usuario que establezca una contraseña, seleccione la casilla **Allow simple password** y la casilla **Force use of password**.

   - Para requerir el uso de letras y números en la contraseña, active la casilla **Prompt for alphanumeric value**.

   - Para solicitar el uso de una contraseña, seleccione la casilla **Force use of password**. Si la casilla está desactivada, el dispositivo móvil se puede utilizar sin contraseña.

     Si las opciones **Prompt for alphanumeric value**, **Minimum password length** o **Minimum number of special characters** están habilitadas, se solicita una contraseña incluso si la casilla **Force use of password** no está marcada.

   - En la lista **Minimum password length**, seleccione la longitud mínima de la contraseña en caracteres.

   - En la lista **Minimum number of special characters**, seleccione la cantidad mínima de caracteres especiales en la contraseña (como "$", "&", "!").

     En algunos dispositivos con MDM de iOS, si se especifica el valor **Minimum number of special characters** y se marca la casilla **Allow simple password**, el dispositivo muestra información sobre cómo establecer una contraseña de 6 o más caracteres, aunque es posible establecer una contraseña de 4 o más caracteres.

   - En el campo **Maximum password lifetime (days)**, especifique el período en días durante el cual la contraseña permanece vigente. Cuando este período expira, el Servidor de MDM para iOS solicita al usuario que cambie la contraseña.

   - En la lista **Auto-Lock**, seleccione la cantidad de tiempo después del cual se debe activar el bloqueo automático en el dispositivo MDM con iOS. Si el dispositivo móvil permanece inactivo durante este período de tiempo, cambia al modo de suspensión.

     En otros dispositivos de MDM de iOS, el tiempo real de bloqueo automático del dispositivo puede variar con respecto al valor que ha especificado:

En dispositivos iPhone, si establece el bloqueo automático en 10 o 15 minutos, el dispositivo se bloqueará en 5 minutos.

En dispositivos iPad: si establece el bloqueo automático en 1 o 4 minutos, el dispositivo se bloqueará en 2 minutos.

Para otros valores, el tiempo efectivo para el bloqueo automático del dispositivo es igual al tiempo especificado.

- En el campo **Reuse of previous passwords**, especifique la cantidad de contraseñas utilizadas (incluida la contraseña actual) que el Servidor de MDM para iOS comparará con la nueva contraseña cuando el usuario cambie la contraseña actual. Si las contraseñas coinciden, se rechaza la contraseña nueva.

- En la lista **Maximum time for unlock without password**, seleccione la cantidad de tiempo durante la cual el usuario puede desbloquear el dispositivo MDM con iOS sin ingresar la contraseña.

- En la lista **Maximum number of failed password attempts**, seleccione la cantidad de intentos de contraseña fallidos que el sistema permite al usuario antes de borrar el dispositivo.

  Si el valor es igual a 6 o menor, el sistema no tiene demora y activa el borrado de todos los datos y configuraciones de un dispositivo iOS tan pronto como el usuario excede el límite establecido.

  Si el valor es más de 7, luego de 6 intentos fallidos, el dispositivo impone una demora antes de que el usuario pueda ingresar la contraseña de desbloqueo nuevamente. El tiempo de demora comienza después del sexto intento y se incrementa con cada intento fallido. Después del último intento fallido, el sistema borra todos los datos y configuraciones del dispositivo iOS.

  De manera predeterminada, la cantidad de intentos para ingresar de contraseña no está limitada.

  Si el usuario supera la cantidad máxima de intentos fallidos de contraseña, el dispositivo se restablecerá a los ajustes de fábrica.

7. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se cambia después de la siguiente sincronización del dispositivo con el Servidor de MDM para iOS.

Como resultado, luego de que se aplica la directiva, el Servidor de MDM para iOS verifica la seguridad de la contraseña establecida en el dispositivo móvil del usuario. Si la seguridad de la contraseña de desbloqueo del dispositivo no cumple con la directiva, se solicitará al usuario que cambie la contraseña.

Configuración de una red privada virtual (VPN)

Esta sección contiene la información sobre la configuración de la red privada virtual (VPN) para la conexión segura con redes Wi-Fi.

Configuración de VPN en dispositivos Android (solo Samsung)

Para conectar de forma segura un dispositivo Android a Internet y proteger la transferencia de datos, puede configurar los ajustes de la VPN (red privada virtual).

La configuración de VPN solo es posible para dispositivos Samsung que ejecutan Android 11 o versiones anteriores.

Los siguientes requisitos se deben tener en cuenta cuando se utiliza una red privada virtual:

- La aplicación que usa la conexión VPN debe estar permitida en la configuración del **Firewall**.
- Las opciones de la VPN configuradas en la directiva no pueden aplicarse a las aplicaciones del sistema. La conexión VPN para las aplicaciones del sistema debe configurarse manualmente.
- Para algunas aplicaciones que utilizan una conexión VPN, se deben configurar opciones adicionales en el primer inicio. Para configurar opciones, una conexión VPN debe estar permitida en las opciones de la aplicación.

Para configurar la VPN en un dispositivo móvil del usuario:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **Android** y vaya a la sección **Samsung Knox settings**.
4. En la tarjeta **VPN**, haga clic en **Settings**.
   Se abre la ventana **VPN**.
5. Habilite la configuración con el interruptor **VPN**.
6. Especifique la siguiente configuración para la VPN:
   - Ajustes de la sección **Network**:
     - En el campo **Network name**, escriba el nombre del túnel VPN.
     - En la lista desplegable **Protocol**, seleccione el tipo de conexión VPN:
       - **IPSec Xauth PSK**. Un protocolo de túnel entre puertas de enlace que permite al usuario del dispositivo móvil establecer una conexión segura con el servidor VPN por medio de la utilidad de autenticación Xauth.
       - **L2TP IPSec PSK**. Un protocolo de túnel entre puertas de enlace que permite al usuario del dispositivo móvil establecer una conexión segura con el servidor VPN mediante el protocolo IKE usando una clave predefinida. Este protocolo está seleccionado de manera predeterminada.
       - **PPTP**. Un protocolo de túnel punto a punto que permite al usuario del dispositivo móvil establecer una conexión segura con el servidor VPN creando un túnel especial en una red estándar sin protección.
     - En el campo **Dirección del servidor**, escriba el nombre de la red o la dirección IP del servidor VPN.

- Ajustes de la sección **Protocol settings**:

  - En la lista **DNS search domain(s)**, escriba el dominio de búsqueda DNS que se agregará automáticamente al nombre del servidor DNS.

    Puede especificar varios dominios DNS separándolos con espacios en blanco.

  - En el campo **DNS server(s)**, escriba el nombre completo del dominio o de la dirección IP del servidor DNS.

    Se pueden especificar varios servidores DNS separados con espacios en blanco.

  - En el campo **Routing**, escriba el rango de direcciones IP dentro del cual se intercambia información a través de la conexión VPN.

    > Si el rango de direcciones IP no está especificado en el campo **Routing**, todo el tráfico de Internet pasa a través de la conexión VPN.

7. Además, configure los siguientes parámetros:

   - Para los protocolos **IPSec Xauth PSK** y **L2TP IPSec PSK**:

     - En el campo **IPSec shared key**, escriba la contraseña de la clave de seguridad preestablecida IPSec.

     - En el campo **IPSec ID**, escriba el nombre del usuario del dispositivo móvil.

   - Para el protocolo **L2TP IPSec PSK**, además puede especificar la contraseña para la clave L2TP en el campo **L2TP key**.

   - Para la red **PPTP**, seleccione la casilla **Use SSL connection** para que la aplicación utilice el método MPPE (Microsoft Point-to-Point Encryption) de cifrado de datos para proteger la transmisión de información cuando el dispositivo móvil se conecta al servidor VPN.

8. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Configuración de VPN en dispositivos iOS con MDM

> Esta configuración se aplica a los dispositivos supervisados y a los dispositivos que funcionan en el modo de control básico.

Para conectar un dispositivo MDM con iOS a una red privada virtual (VPN) y proteger los datos durante la conexión a la VPN, configure las opciones de conexión VPN. Los protocolos VPN IKEv2 e IPSec también le permiten configurar una conexión Per App VPN.

Para configurar una conexión VPN en el dispositivo MDM con iOS de un usuario, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **iOS** y vaya a la sección **Device configuration**.

4. En la tarjeta **VPN**, haga clic en **Settings**.

   Se abre la ventana **VPN**.

5. Habilite la configuración con el interruptor **VPN**.

6. Haga clic en **Agregar**.

   Se abre la ventana **Add VPN configuration**.

7. En la pestaña **General**, en la sección **Network**, configure los siguientes ajustes:

   a. En el campo **Network name**, escriba el nombre del túnel VPN.

   b. En la lista desplegable **Protocol**, seleccione el **tipo de conexión VPN**.

   - **L2TP** (Protocolo de Túnel de capa 2). La conexión admite autenticación del usuario de un dispositivo MDM con iOS mediante contraseña MS-CHAP v2, autenticación de dos factores y autenticación automática utilizando una clave pública.

   - **IKEv2** (Internet Key Exchange versión 2). La conexión establece el atributo Asociación de seguridad (SA) entre dos entidades de red y admite la autenticación mediante EAP (Protocolos de autenticación extensibles), secretos compartidos y certificados.

   - **IPSec**. La conexión admite autenticación del usuario mediante contraseña, autenticación de dos factores y autenticación automática utilizando una clave pública y certificados.

   - **Cisco AnyConnect**. La conexión admite dispositivos firewall Adaptive Security Appliance Cisco (ASA) de la versión 8.0(3).1 o posterior. Para configurar una conexión VPN, instale la aplicación Cisco AnyConnect desde App Store en el dispositivo MDM con iOS.

   - **Juniper SSL**. La conexión admite la puerta de enlace Juniper Networks SSL VPN, Series SA, versión 6.4 o posterior con el paquete Juniper Networks IVE, versión 7.0 o posterior. Para configurar la conexión VPN, instale la aplicación JUNOS desde App Store en el dispositivo MDM con iOS.

   - **F5 SSL**. La conexión admite F5 BIG-IP Edge Gateway, Administrador de la directiva de acceso y soluciones Fire SSL para VPN. Para configurar una conexión VPN, instale la aplicación para clientes F5 BIG-IP Edge desde App Store en el dispositivo MDM con iOS.

   - **SonicWALL Mobile Connect**. La conexión admite dispositivos seguros de acceso remoto SonicWALL Aventail E-Class, versión 10.5.4 o posterior, dispositivos SonicWALL SRA de versión 5.5 o posterior, como así también dispositivos firewall SonicWALL Next-Generation, incluidos TZ, NSA y E-Class NSA con SonicOS de versión 5.8.1.0 o posterior. Para configurar una conexión VPN, instale la aplicación SonicWALL Mobile Connect desde App Store en el dispositivo MDM con iOS.

- **Aruba VIA**. La conexión admite controladores de acceso al móvil Aruba. Para configurarlas, instale la aplicación Aruba Networks VIA desde App Store en el dispositivo MDM con iOS.
- **Custom SSL**. La conexión admite autenticación del usuario de un dispositivo MDM con iOS mediante contraseñas y autenticación de dos factores.

c. En el campo **Server address**, escriba el nombre de la red o la dirección IP del servidor VPN.

8. Configure los **ajustes para la conexión VPN** de acuerdo con el tipo de red privada virtual seleccionada.

- L2TP
  - Ajustes de la sección **Authentication**:
    - **Authentication type**

      Autenticación de dos factores del usuario de un dispositivo MDM con iOS mediante un token RSA SecurID o autenticación basada en contraseña.
    - **Account name**

      Nombre de la cuenta para obtener autorización en el servidor de VPN.
    - **Password**

      La contraseña de la cuenta para autenticación en la red virtual privada.
    - **Authentication method**

      Método para autenticar a los usuarios de dispositivos MDM con iOS en la red privada virtual.
    - **Shared secret**

      Contraseña para la clave de seguridad preestablecida IPSec para los protocolos L2TP y IPSec (Cisco).
    - **Authentication certificate**

      Certificado utilizado para la autenticación de usuarios.
  - Ajustes de la sección **Other**:
    - **Send all traffic via VPN**

      Transmisión de todo el tráfico de salida mediante la conexión VPN si se utiliza un servicio diferente de red (por ejemplo: AirPort o Ethernet).

      Si la casilla está marcada, todo el tráfico se envía a través de la conexión VPN.

      Si la casilla no está marcada, el tráfico saliente se transmite sin requerir el uso de la conexión VPN.

      Esta casilla está desactivada por defecto.
- IPSec
  - Ajustes de la sección **Authentication**:
    - **Authentication method**

      Método para autenticar a los usuarios de dispositivos MDM con iOS en la red privada virtual.

- **Account name**

  Nombre de la cuenta para obtener autorización en el servidor de VPN.

- **Password**

  La contraseña de la cuenta para autenticación en la red virtual privada.

- **Shared secret**

  Contraseña para la clave de seguridad preestablecida IPSec para los protocolos L2TP y IPSec (Cisco).

- **Group name**

  Nombre del grupo de dispositivos MDM con iOS que se conectan a una VPN a través de los protocolos L2TP y IPSec (Cisco). Si la casilla **Use hybrid authentication** está marcada, el nombre del grupo debe terminar en "[hybrid]" (por ejemplo: "mycompany [hybrid]").

- **Use hybrid authentication**

  Uso de la autenticación híbrida cuando el usuario se conecta a una VPN. El servidor VPN utiliza un certificado para la autenticación y el usuario del dispositivo MDM con iOS ingresa una clave pública para la autenticación mediante el protocolo IPSec (Cisco).

  Si la casilla está marcada, se utiliza autenticación híbrida cuando el usuario se conecta a una VPN.

  Si la casilla no está marcada, no se utiliza autenticación híbrida.

  Esta casilla está desactivada por defecto.

- **Authentication certificate**

  Certificado utilizado para la autenticación de usuarios.

- Ajustes de la sección **Domains**:

  - **Enable VPN when connecting to specified domains**

    Los dominios para los que se habilitará la conexión VPN.

- Ajustes de la sección **Other**:

  - **Prompt for PIN**

    La aplicación comprueba si la contraseña del sistema está establecida cuando se enciende el dispositivo móvil.

    Si la casilla está marcada, Kaspersky Mobile Devices Protection and Management comprueba si la contraseña del sistema está establecida en el dispositivo. Si no se ha establecido una contraseña de sistema en el dispositivo, el usuario debe hacerlo. La contraseña debe definirse de acuerdo con las opciones configuradas por el administrador.

    Si la casilla no está marcada, Kaspersky Mobile Devices Protection and Management no requiere una contraseña del sistema.

    Esta casilla está desactivada por defecto.

- **IKEv2**
  - Ajustes de la sección **Network**:
    - **Dead peer detection interval**

      La frecuencia con la que el cliente VPN IKEv2 debe ejecutar el algoritmo de Detección de pares muertos (DPD). Están disponibles los siguientes valores:
      - **Not selected**. No ejecutar DPD.
      - **Low**. Ejecutar DPD cada 30 minutos.
      - **Medium**. Ejecutar DPD cada 10 minutos.
      - **High**. Ejecutar DPD cada 1 minuto.

      El valor predeterminado es **Medium**.
  - Ajustes de la sección **Authentication**:
    - **Authentication method**

      Método para autenticar a los usuarios de dispositivos MDM con iOS en la red privada virtual.
    - **Local identifier**

      El identificador del cliente VPN IKEv2 (dispositivo MDM con iOS).
    - **Remote identifier**

      El identificador del servidor VPN IKEv2.
    - **Shared secret**

      El secreto compartido utilizado para la autenticación de la VPN IKEv2.
    - **Common Name (CN) of server certificate**

      Este nombre se utiliza para validar el certificado enviado por el servidor VPN IKEv2. Si no se establece esta opción, el certificado se valida mediante el identificador remoto.
    - **Common Name (CN) of server certificate publisher**

      Si se establece esta opción, IKEv2 envía una solicitud de certificado basada en este emisor de certificado al servidor.
    - **Authentication certificate**

      Certificado utilizado para la autenticación de usuarios.
    - **EAP authentication**

      El tipo de autenticación EAP utilizada para la conexión VPN IKEv2. Están disponibles los siguientes valores:
      - **Credentials**
      - **Certificate**

      El valor predeterminado es **Credentials**.

- **Account name**

  Nombre de la cuenta para obtener autorización en el servidor de VPN.

- **Password**

  La contraseña de la cuenta para autenticación en la red virtual privada.

- **Minimum TLS version**

  La versión mínima de TLS utilizada para la autenticación EAP. Están disponibles los siguientes valores:

  - **TLS 1.0**
  - **TLS 1.1**
  - **TLS 1.2**

  El valor predeterminado es **TLS 1.0**.

- **Maximum TLS version**

  La versión máxima de TLS utilizada para la autenticación EAP. Están disponibles los siguientes valores:

  - **TLS 1.0**
  - **TLS 1.1**
  - **TLS 1.2**

  El valor predeterminado es **TLS 1.2**.

- Ajustes de la sección **Security association**:

  - **SA parameters**

    Determina el objeto en el que se envían los parámetros. Valores posibles:

    - **IKEv2**
    - **Child**

    El valor predeterminado es **IKEv2**.

  - **Encryption algorithm**

    Determina el algoritmo de cifrado utilizado para la conexión. Valores posibles:

    - **DES**
    - **3DES**
    - **AES-128**
    - **AES-256**
    - **AES-128-GCM**

- **AES-256-GCM**
- **ChaCha20Poly1305**

El valor predeterminado es **AES-256**.

- **Integrity algorithm**

  Determina el algoritmo de integridad utilizado para la conexión. Valores posibles:

  - **SHA1-96**
  - **SHA1-160**
  - **SHA2-256**
  - **SHA2-384**
  - **SHA2-512**

  El valor predeterminado es **SHA2-256**.

- **Diffie-Hellman group**

  Determina el grupo Diffie-Hellman que se utiliza al configurar el túnel VPN.

  El valor predeterminado es 14.

- **SA Lifetime (min)**

  El intervalo de reintroducción en minutos.

- Ajustes de la sección **Other**:

  - **Disable redirect**

    Especifica si los redireccionamientos del servidor VPN IKEv2 están deshabilitados.

    Si la casilla está marcada, la conexión VPN IKEv2 no se redirige.

    Si la casilla está desactivada, la conexión VPN IKEv2 se redirige si se recibe una solicitud de redireccionamiento del servidor.

    Esta casilla está desactivada por defecto.

  - **Disable Mobility and Multi-homing Protocol**

    Especifica si el Protocolo de movilidad y multiconexión (MOBIKE) está deshabilitado para la conexión VPN IKEv2.

    Si la casilla está marcada, MOBIKE está deshabilitado

    Si la casilla está desactivada, MOBIKE está disponible.

    Esta casilla está desactivada por defecto.

  - **Use internal IPv4 and IPv6 subnet attributes**

    Especifica si el cliente VPN IKEv2 debe usar los atributos de configuración INTERNAL_IP4_SUBNET e INTERNAL_IP6_SUBNET enviados por el servidor VPN IKEv2.

    Si la casilla está marcada, se utilizan los atributos INTERNAL_IP4_SUBNET e INTERNAL_IP6_SUBNET.

Si la casilla no está marcada, los atributos INTERNAL_IP4_SUBNET e INTERNAL_IP6_SUBNET no se utilizan.

Esta casilla está desactivada por defecto.

- **Enable a tunnel over cellular data**

  Especifica si la reserva está habilitada.

  Si la casilla está marcada, el dispositivo habilita un túnel a través de datos móviles para transportar tráfico elegible para Asistencia Wi-Fi y que también requiera una VPN.

  Si la casilla está desactivada, la reserva no está disponible.

  Esta casilla está desactivada por defecto.

- **Enable Perfect Forward Secrecy**

  Especifica si el Secreto perfecto hacia adelante (PFS) está habilitado para la conexión VPN IKEv2.

  Si la casilla está marcada, PFS está habilitado.

  Si la casilla está desactivada, PFS no está disponible.

  Esta casilla está desactivada por defecto.

- **Cisco AnyConnect**
  - Ajustes de la sección **Network**:
    - **Idle time before disconnection (min)**

      El tiempo de espera antes de desconectar una conexión a pedido.
  - Ajustes de la sección **Authentication**:
    - **Authentication method**

      Método para autenticar a los usuarios de dispositivos MDM con iOS en la red privada virtual.
    - **Account name**

      Nombre de la cuenta para obtener autorización en el servidor de VPN.
    - **Password**

      La contraseña de la cuenta para autenticación en la red virtual privada.
    - **Group**

      Alias del grupo de túnel para los clientes de Cisco AnyConnect que se conectan a una VPN.
    - **Authentication certificate**

      Certificado utilizado para la autenticación de usuarios.
  - Ajustes de la sección **Domains**:
    - **Enable VPN when connecting to specified domains**

      Los dominios para los que se habilitará la conexión VPN.

- Ajustes de la sección **Other**:
  - **Send all traffic via VPN**

    Enruta todo el tráfico a través de la VPN.
  - **Exclude local traffic**

    Excluye el tráfico local del tráfico enrutado a través de la conexión VPN.
    Esta casilla está disponible si se selecciona la casilla **Send all traffic via VPN**.

- **Juniper SSL**
  - Ajustes de la sección **Network**:
    - **Idle time before disconnection (min)**

      El tiempo de espera antes de desconectar una conexión a pedido.
  - Ajustes de la sección **Authentication**:
    - **Authentication method**

      Método para autenticar a los usuarios de dispositivos MDM con iOS en la red privada virtual.
    - **Account name**

      Nombre de la cuenta para obtener autorización en el servidor de VPN.
    - **Password**

      La contraseña de la cuenta para autenticación en la red virtual privada.
    - **Scope**

      Nombre de la red que incluye los servidores VPN y los dispositivos MDM con iOS para la conexión VPN establecida utilizando Juniper SSL.
    - **Role**

      Nombre del rol del usuario que le otorga al usuario acceso a los recursos utilizando Juniper SSL. Una función puede combinar varios usuarios realizando funciones similares.
    - **Authentication certificate**

      Certificado utilizado para la autenticación de usuarios.
  - Ajustes de la sección **Domains**:
    - **Enable VPN when connecting to specified domains**

      Los dominios para los que se habilitará la conexión VPN.
  - Ajustes de la sección **Other**:
    - **Send all traffic via VPN**

      Enruta todo el tráfico a través de la VPN.

- **Exclude local traffic**

  Excluye el tráfico local del tráfico enrutado a través de la conexión VPN.
  Esta casilla está disponible si se selecciona la casilla **Send all traffic via VPN**.

- **F5 SSL**
  - Ajustes de la sección **Network**:
    - **Idle time before disconnection (min)**

      El tiempo de espera antes de desconectar una conexión a pedido.
  - Ajustes de la sección **Authentication**:
    - **Authentication method**

      Método para autenticar a los usuarios de dispositivos MDM con iOS en la red privada virtual.
    - **Account name**

      Nombre de la cuenta para obtener autorización en el servidor de VPN.
    - **Password**

      La contraseña de la cuenta para autenticación en la red virtual privada.
    - **Authentication certificate**

      Certificado utilizado para la autenticación de usuarios.
  - Ajustes de la sección **Domains**:
    - **Enable VPN when connecting to specified domains**

      Los dominios para los que se habilitará la conexión VPN.
  - Ajustes de la sección **Other**:
    - **Send all traffic via VPN**

      Enruta todo el tráfico a través de la VPN.
    - **Exclude local traffic**

      Excluye el tráfico local del tráfico enrutado a través de la conexión VPN.
      Esta casilla está disponible si se selecciona la casilla **Send all traffic via VPN**.
- **SonicWALL Mobile Connect**
  - Ajustes de la sección **Network**:
    - **Idle time before disconnection (min)**

      El tiempo de espera antes de desconectar una conexión a pedido.

- Ajustes de la sección **Authentication**:
  - **Authentication method**

    Método para autenticar a los usuarios de dispositivos MDM con iOS en la red privada virtual.
  - **Account name**

    Nombre de la cuenta para obtener autorización en el servidor de VPN.
  - **Password**

    La contraseña de la cuenta para autenticación en la red virtual privada.
  - **Domain or group**

    Nombre del dominio del servidor SSL VPN (ejemplo: vpn.compañía.com) o el nombre de un grupo de usuarios de SonicWALL Mobile Connect.
  - **Authentication certificate**

    Certificado utilizado para la autenticación de usuarios.
- Ajustes de la sección **Domains**:
  - **Enable VPN when connecting to specified domains**

    Los dominios para los que se habilitará la conexión VPN.
- Ajustes de la sección **Other**:
  - **Send all traffic via VPN**

    Enruta todo el tráfico a través de la VPN.
  - **Exclude local traffic**

    Excluye el tráfico local del tráfico enrutado a través de la conexión VPN.
    Esta casilla está disponible si se selecciona la casilla **Send all traffic via VPN**.

- **Aruba VIA**
  - Ajustes de la sección **Network**:
    - **Idle time before disconnection (min)**

      El tiempo de espera antes de desconectar una conexión a pedido.
  - Ajustes de la sección **Authentication**:
    - **Authentication method**

      Método para autenticar a los usuarios de dispositivos MDM con iOS en la red privada virtual.
    - **Account name**

      Nombre de la cuenta para obtener autorización en el servidor de VPN.

- **Password**

  La contraseña de la cuenta para autenticación en la red virtual privada.

- **Authentication certificate**

  Certificado utilizado para la autenticación de usuarios.

- Ajustes de la sección **Domains**:

  - **Enable VPN when connecting to specified domains**

    Los dominios para los que se habilitará la conexión VPN.

- Ajustes de la sección **Other**:

  - **Send all traffic via VPN**

    Enruta todo el tráfico a través de la VPN.

  - **Exclude local traffic**

    Excluye el tráfico local del tráfico enrutado a través de la conexión VPN.
    Esta casilla está disponible si se selecciona la casilla **Send all traffic via VPN**.

- **Custom SSL**

  - Ajustes de la sección **Network**:

    - **Idle time before disconnection (min)**

      El tiempo de espera antes de desconectar una conexión a pedido.

  - Ajustes de la sección **Configuration data**:

    - **Key**

      Contiene una clave con configuraciones adicionales para la conexión personalizada SSL.

    - **Value**

      Contiene un valor con configuraciones adicionales para la conexión personalizada SSL.

  - Ajustes de la sección **Authentication**:

    - **Authentication method**

      Método para autenticar a los usuarios de dispositivos MDM con iOS en la red privada virtual.

    - **Account name**

      Nombre de la cuenta para obtener autorización en el servidor de VPN.

    - **Password**

      La contraseña de la cuenta para autenticación en la red virtual privada.

    - **Authentication certificate**

Certificado utilizado para la autenticación de usuarios.

- **Bundle ID**

  Si la configuración de VPN personalizada tiene como objetivo una solución VPN que utiliza un proveedor de extensión de red, este campo contiene el identificador de paquete de la aplicación que contiene el proveedor. Comuníquese con el proveedor de la solución VPN para conocer el valor del identificador.

- Ajustes de la sección **Domains**:

  - **Enable VPN when connecting to specified domains**

    Los dominios para los que se habilitará la conexión VPN.

9. Si es necesario, en la pestaña **Additional**, en la sección **Proxy server**, configure los ajustes de la conexión VPN a través de un servidor proxy:

   a. Seleccione la casilla **Use a proxy server**.

   b. Configure una conexión a un servidor proxy:

      a. Si desea configurar la conexión automáticamente:

      - Seleccione **Automatic**.
      - En el campo **PAC file URL**, especifique la URL del archivo PAC del proxy.
      - Para permitir al usuario conectar el dispositivo móvil a una red inalámbrica sin usar un servidor proxy cuando no se puede acceder al archivo PAC, seleccione la casilla **Allow direct connection if PAC file cannot be accessed**.

      b. Si desea configurar la conexión manualmente:

      - Seleccione **Manual**.
      - En el campo **Proxy server address** y **Proxy server port**, escriba la dirección IP o nombre DNS del servidor proxy y el número de puerto.
      - En el campo **User name**, seleccione una macro que se utilizará como nombre de usuario para la conexión al servidor proxy.

      c. En el campo **Password**, especifique la contraseña para la conexión al servidor proxy.

10. Para las conexiones **IKEv2** e **IPSec**, si es necesario, configure la funcionalidad Per App VPN para las aplicaciones del sistema compatibles (Correo, Calendario, Contactos y Safari) o para aplicaciones de terceros.

11. Clic en el botón **Add**.

    La nueva VPN se muestra en la lista.

    Puede modificar o eliminar redes VPN en la lista con los botones **Edit** y **Delete** que se encuentran en la parte superior de la lista.

12. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se cambia después de la siguiente sincronización del dispositivo con el Servidor de MDM para iOS.

Como resultado, una vez que se aplica la directiva, la conexión VPN se configurará en el dispositivo MDM con iOS del usuario.

Configuración de firewall en dispositivos Android (solo Samsung)

Configure las opciones del firewall para controlar las conexiones a la red en el dispositivo móvil del usuario.

El firewall solo se puede configurar para dispositivos Samsung que operan en los siguientes modos:

- dispositivo corporativo
- dispositivo personal con Android 15 o anterior
- dispositivo con contenedor corporativo con Android 15 o anterior

Para configurar el firewall en el dispositivo móvil de un usuario, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **Android** y vaya a la sección **Samsung Knox settings**.
4. En la tarjeta **Firewall**, haga clic en **Settings**.

   Se abre la ventana **Firewall**.
5. Habilite la configuración con el interruptor **Firewall**.
6. En la lista desplegable **Internet access**, seleccione el modo Firewall. Según el modo de funcionamiento, el firewall supervisa las conexiones establecidas por el dispositivo móvil del usuario:
   - Si desea permitir las conexiones entrantes y salientes de todas las aplicaciones instaladas, seleccione **Allow for all apps**. Este modo está seleccionado de forma predeterminada.
   - Si desea bloquear toda la actividad de la red, excepto varias aplicaciones especificadas, seleccione **Allow for listed apps**.
7. Si seleccionó **Allow for listed apps** como el modo del firewall, cree una lista de aplicaciones para las que se permite toda la actividad de red:
   a. En la sección **Apps with internet access**, haga clic en **Add**.

      Se abre la ventana **Add app**.
   b. En el campo **App name**, escriba el nombre de una aplicación móvil.

c. En el campo **Package name**, escriba el nombre del sistema del paquete de la aplicación móvil (por ejemplo, `com.mobileapp.example`).

d. Haga clic en **Agregar**.

La nueva aplicación para la que se deshabilita el firewall aparece en la lista.

Puede modificar o eliminar redes aplicaciones móviles en la lista con los botones **Edit** y **Delete** que se encuentran en la parte superior de la lista.

8. Haga clic en **Aceptar**.

9. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Protección de Kaspersky Endpoint Security para Android contra eliminación

Para proteger los dispositivos móviles y cumplir con los requisitos de seguridad corporativa, puede habilitar la protección contra la eliminación de Kaspersky Endpoint Security para Android. En este caso, el usuario no puede eliminar la aplicación usando la interfaz de Kaspersky Endpoint Security para Android. Al eliminar la aplicación usando las herramientas del sistema operativo Android, se le solicita deshabilitar los derechos de administrador para Kaspersky Endpoint Security para Android. Después de deshabilitar los derechos, el dispositivo móvil se bloqueará.

En ciertos dispositivos Samsung con Android 7 o versiones posteriores, cuando el usuario intenta configurar métodos no admitidos para desbloquear el dispositivo (por ejemplo, una contraseña gráfica), el dispositivo se puede bloquear si se satisfacen las siguientes condiciones: la protección de eliminación de está habilitada para Kaspersky Endpoint Security para Android y se establecieron requisitos de seguridad de la contraseña de desbloqueo de la pantalla. Para desbloquear el dispositivo, debe enviar un comando especial al dispositivo.

Para proteger la aplicación contra la eliminación en dispositivos con Android 7 o posterior, Kaspersky Endpoint Security para Android debe estar configurado como función de accesibilidad. Cuando el Asistente de configuración inicial se está ejecutando, Kaspersky Endpoint Security para Android le pide al usuario que conceda a la aplicación todos los permisos requeridos. El usuario puede omitir estos pasos o deshabilitar estos permisos más adelante en la configuración del dispositivo. En ese caso, la aplicación no estará protegida de la eliminación.

Para habilitar la protección contra la eliminación de Kaspersky Endpoint Security para Android:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **Android** y vaya a la sección **KES for Android settings**.

4. En la tarjeta **Configure access to app settings**, haga clic en **Settings**.

   Se abre la ventana **Configure access to app settings**.

5. Habilite la configuración con el interruptor **Configure access to app settings**.

   El interruptor de esta tarjeta no habilita ni deshabilita la funcionalidad correspondiente en los dispositivos. Habilitar el interruptor le permite utilizar configuraciones personalizadas. Deshabilitar el interruptor le permite usar la configuración predeterminada.

6. Desmarque la casilla **Allow removing the app from device**.

7. Haga clic en **Aceptar**.

8. Haga clic en el botón **Save** para guardar los cambios que realizó.

   La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center. Si se intenta eliminar la aplicación, el dispositivo móvil se bloqueará.

Detectar dispositivos comprometidos

Kaspersky Next Expert View (on-premise) le permite detectar dispositivos Android pirateados (rooteados) y la liberación en dispositivos iOS. Los archivos de sistema están desprotegidos en un dispositivo atacado por hackers y, por lo tanto, pueden ser modificados. Si se detecta un intento de ataque de hackers, recomendamos que inmediatamente restaure el funcionamiento normal del dispositivo.

Si se piratea el dispositivo, recibe una notificación. Puede ver las notificaciones de piratería en Kaspersky Next Expert View (on-premise), en la sección **Monitoring → Dashboard**. También puede deshabilitar las notificaciones sobre ataques de hackers en la configuración de notificaciones de eventos.

En dispositivos Android, puede imponer restricciones a la actividad del usuario si el dispositivo es atacado (por ejemplo, bloquear el dispositivo). Puede imponer restricciones usando el componente Control de cumplimiento. Para ello, cree una regla de cumplimiento con el criterio **Device has been rooted**.

Configuración de un proxy HTTP global en dispositivos iOS con MDM

Esta configuración se aplica a los dispositivos supervisados.

Para proteger el tráfico de Internet del usuario, configure la conexión del dispositivo MDM con iOS a Internet a través del servidor proxy.

Tenga cuidado al configurar estos ajustes. Si los ajustes son incorrectos, los dispositivos pueden perder su conexión a Internet y dejar de sincronizarse con el servidor MDM de iOS. Si esto sucede, tendrá que volver a añadir los dispositivos.

Para configurar las opciones del proxy HTTP global en el dispositivo iOS con MDM del usuario:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management → Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **iOS** y vaya a la sección **Device configuration**.

4. En la tarjeta **Global HTTP proxy**, haga clic en **Settings**.

   Se abre la ventana **Global HTTP proxy**.

5. Habilite la configuración con el interruptor **Global HTTP proxy**.

6. Seleccione el tipo de configuración de proxy HTTP global:

   - Para especificar la configuración de conexión al servidor proxy manualmente:

     a. En la sección **Setting type**, seleccione **Manual**.

     b. En los campos **Proxy server address** y **Proxy server port**, escriba el nombre del host o la dirección IP del servidor proxy y el número de puerto del servidor proxy.

     c. En el campo **User name**, ingrese el nombre de la cuenta de usuario para obtener autorización en el servidor proxy.

     d. En el campo **Password**, establezca la contraseña de la cuenta de usuario para autenticarse en el servidor proxy.

     e. Para permitir al usuario acceder a redes cautivas, seleccione la casilla **Allow access to captive networks without connecting to proxy**.

   - Para configurar las opciones de conexión al servidor proxy mediante un archivo PAC (autoconfiguración de proxy) predefinido:

     a. En la sección **Setting type**, seleccione **Automatic**.

     b. En el campo **PAC file URL**, escriba la dirección web del archivo PAC (por ejemplo: `http://www.example.com/filename.pac`).

     c. Para permitir al usuario conectar el dispositivo móvil a una red inalámbrica sin usar un servidor proxy cuando no se puede acceder al archivo PAC, seleccione la casilla **Allow direct connection if PAC file cannot be accessed**.

     d. Para permitir al usuario acceder a redes cautivas, seleccione la casilla **Allow access to captive networks without connecting to proxy**.

7. Haga clic en **Aceptar**.

8. Haga clic en el botón **Save** para guardar los cambios que realizó.

Como resultado, el usuario del dispositivo móvil se conectará a Internet a través de un servidor proxy después de que se aplique la directiva.

Adición de certificados de seguridad a dispositivos iOS con MDM

Esta configuración se aplica a los dispositivos supervisados y a los dispositivos que funcionan en el modo de control básico.

Puede agregar certificados a los dispositivos MDM con iOS para simplificar la autenticación del usuario y garantizar la seguridad de los datos. Los datos firmados con un certificado están protegidos contra modificaciones mientras se transfieren a través de la red. El cifrado de datos mediante un certificado brinda un nivel adicional de protección de datos. El certificado también se puede utilizar para verificar la identidad del usuario.

Kaspersky Mobile Devices Protection and Management admite los siguientes estándares de certificados:

- **PKCS#1**. Cifrado con una clave pública basado en algoritmos RSA.
- **PKCS#12**. Almacenamiento y transmisión de un certificado y de una clave privada.

Para agregar un certificado de seguridad a los dispositivos MDM con iOS, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **iOS** y vaya a la sección **Device configuration**.
4. En la tarjeta **Certificate management**, haga clic en **Settings**.

   Se abre la ventana **Certificate management**.
5. Habilite la configuración con el interruptor **Certificate management**.
6. Haga clic en **Upload** y especifique la ruta al certificado.

   Los archivos de los certificados PKCS#1 tienen la extensión CER, DER o PEM. Los archivos de los certificados PKCS#12 tienen la extensión P12 o PFX. La contraseña para un certificado PKCS#12 no debe estar vacía.
7. Haga clic en **Abrir**.

   Si el certificado está protegido con contraseña, escriba la contraseña. El nuevo certificado aparece en la lista.
8. Haga clic en **Aceptar**.
9. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se cambia después de la siguiente sincronización del dispositivo con el Servidor de MDM para iOS.

Como resultado, una vez que se aplica la directiva, los certificados se instalan automáticamente en los dispositivos.

Adición de perfiles SCEP a dispositivos iOS con MDM

Esta configuración se aplica a los dispositivos supervisados y a los dispositivos que funcionan en el modo de control básico.

Debe agregar un perfil de SCEP para permitir al usuario del dispositivo iOS con MDM recibir automáticamente desde Internet certificados del Centro de certificación. El perfil SCEP habilita el soporte del protocolo de inscripción de certificados simple.

El perfil SCEP con la siguiente configuración se agrega de forma predeterminada:

- El nombre alternativo del titular no se utiliza para registrar certificados.
- Se realizan tres intentos a intervalos de 10 segundos para sondear el servidor SCEP. Si todos los intentos para firmar el certificado fallan, debe generar una nueva solicitud de firma de certificado.
- El certificado recibido no se puede utilizar para la firma o el cifrado de datos.

Puede editar la configuración especificada cuando agrega el perfil SCEP.

Para añadir un perfil SCEP:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **iOS** y vaya a la sección **Device configuration**.
4. En la tarjeta **SCEP**, haga clic en **Settings**.

   Se abre la ventana **SCEP**.
5. Habilite la configuración con el interruptor **SCEP**.
6. Haga clic en **Add**.

   Se abre la ventana **Add SCEP profile**.
7. En la sección **SCEP Server**, especifique la siguiente configuración del servidor SCEP:

   - En el campo **Configuration name**, especifique el nombre del Centro de certificación implementado en el servidor SCEP. El Centro de certificación provee al usuario de un dispositivo MDM iOS con certificados utilizando el Protocolo de inscripción de certificados simple (SCEP).
   - En el campo **Server URL**, escriba la dirección web del servidor SCEP en el que se implementa el Centro de certificación.

     La URL puede contener la dirección IP o el nombre de dominio completo (FQDN). Por ejemplo, `http://10.10.10.10/certserver/companyscep`.
   - En el campo **Maximum number of polling attempts**, especifique la cantidad máxima de intentos de sondear el servidor SCEP para obtener el certificado firmado. El valor predeterminado es 3 intentos.

     Si todos los intentos para firmar el certificado fallan, debe generar una nueva solicitud de firma de certificado.
   - En el campo **Polling interval (sec)**, especifique la cantidad de segundos entre un intento y otro de sondear el servidor SCEP para obtener la firma del certificado. El valor predeterminado es 10 segundos.

- En el campo **Static challenge phrase**, ingrese la clave de registro pre publicada.

  Antes de firmar un certificado, el servidor SCEP solicita al usuario del dispositivo móvil que ingrese la clave. Si este campo se deja en blanco, el SCEP no solicita la clave.

- En la lista desplegable **Method for uploading certificate thumbprint**, seleccione cómo agregar una huella digital del certificado. Puede utilizar huellas digitales de certificado con el algoritmo hash SHA-1 o MD5.

  - Si seleccionó la opción **Manually**, en el campo **Certificate thumbprint** que aparece, ingrese una huella digital del certificado única para verificar la autenticidad de la respuesta del Centro de certificación.

  - Si seleccionó la opción **From file**, cargue un archivo CER, KEY o PEM. La huella digital se generará y agregará automáticamente.

  Debe especificarse la huella digital del certificado si el intercambio de información entre el dispositivo móvil y el Centro de certificación ocurre mediante el protocolo HTTP.

8. En la sección **Subject**, especifique la siguiente configuración:

- En el campo **Subject Name**, escriba una cadena con los atributos del usuario del dispositivo MDM con iOS que se incluyen en el certificado X.500.

  Los atributos pueden contener detalles del país (C), localidad (L), estado (ST), organización (O), unidad organizativa (OU) y nombre de usuario común (CN). Por ejemplo, `/C=RU/O=MyCompany/CN=User/`.

  También puede usar otros atributos especificados en el RFC 5280.

  Los servidores DNS usan los atributos para validar el certificado emitido por la Autoridad de autenticación a pedido del usuario.

- Haga clic en el botón **Add Subject Alternative Name** para agregar un campo a fin de especificar el nombre alternativo del titular:

  - En la lista desplegable **Type of Subject Alternative Name** que aparece, seleccione el tipo de nombre alternativo del titular para el servidor SCEP. Solo puede agregar un nombre alternativo de cada tipo.

    Puede usar un nombre alternativo del titular para identificar al usuario del dispositivo MDM con iOS. De manera predeterminada, no se utiliza la identificación basada en el nombre alternativo.

    - **DNS name**. Identificación mediante el nombre de dominio.

    - **NT Principal Name**. El nombre DNS del usuario de un dispositivo MDM con iOS en la red Windows NT. El nombre del titular NT está contenido en la solicitud de certificado enviada al servidor SCEP. También puede usar el nombre del titular NT para identificar al usuario del dispositivo MDM con iOS.

    - **Email address**. Identificación mediante la dirección de correo electrónico. La dirección de correo electrónico debe ser especificada de acuerdo al RFC 822.

    - **Uniform Resource Identifier (URI)**. Identificación mediante la dirección IP o la dirección en formato FQDN.

  - En el campo **Subject Alternative Name**, escriba el nombre alternativo del titular del certificado X.500. El valor del nombre alternativo del titular depende del tipo de titular: el dominio, la dirección web o la dirección de correo electrónico del usuario.

9. En la sección **Key**, ajuste la configuración de la clave de cifrado:

   - En la lista desplegable **Key size (bit)**, seleccione el tamaño de la clave de registro en bits: 1024, 2048 o 4096. El valor predeterminado es 1024 bits.

   - Si desea permitir al usuario utilizar un certificado recibido del servidor SCEP como certificado para firmas, seleccione la casilla **Use as digital signature**.

     El firmado de información protege la información de modificaciones. Por ejemplo, Safari puede validar la autenticación del certificado y establecer una sesión segura de intercambio de información.

   - Si desea permitir al usuario utilizar un certificado recibido del servidor SCEP para el cifrado de información, seleccione la casilla **Use for encryption**.

     El cifrado de datos también protege los datos confidenciales durante el intercambio de datos a través de una red. Por ejemplo, Safari puede establecer una sesión segura de intercambio de información utilizando cifrado. Esto garantiza la autenticación del sitio web y confirma que la conexión al sitio web está cifrada para proteger de interceptación de información personal y confidencial.

     > No puede usar simultáneamente el certificado del servidor SCEP como un certificado de firma de datos y un certificado de cifrado de datos.

   - Si desea permitir que todas las aplicaciones instaladas accedan a la clave privada del certificado del servidor SCEP, seleccione la casilla **Allow all apps to access private key**.

   - Si no desea que la clave privada se exporte desde el llavero, seleccione la casilla **Prohibit exporting private key from the Keychain**.

10. Haga clic en **Agregar**.

    El nuevo perfil SCEP aparece en la lista.

    > Puede modificar o eliminar perfiles de SCEP en la lista con los botones **Edit** y **Delete** que se encuentran en la parte superior de la lista.

11. Haga clic en **Aceptar**.

12. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se cambia después de la siguiente sincronización del dispositivo con el Servidor de MDM para iOS.

Como resultado, luego de que se aplica la directiva, el dispositivo móvil del usuario está configurado para recibir automáticamente desde Internet un certificado del Centro de certificación.

Administración de dispositivos móviles

Esta sección contiene información sobre cómo administrar dispositivos móviles de forma remota en Kaspersky Next Expert View (on-premise).

Administrar dispositivos Android

Kaspersky Next Expert View (on-premise) le permite administrar dispositivos Android de las siguientes maneras:

- Administre centralmente los dispositivos mediante comandos.
- Vea información acerca de la configuración de administración de dispositivos Android.
- Instale las aplicaciones a través de paquetes de aplicaciones móviles.
- Conéctese a los dispositivos y contrólelos de forma remota.
- Desconecte los dispositivos Android de la administración.

Habilitar la autenticación basada en certificados para los dispositivos

Para habilitar la autenticación basada en certificados de un dispositivo, siga estos pasos:

1. Abra la línea de comandos en un dispositivo en el que esté instalado el Servidor de administración.
2. Vaya al directorio que contiene la utilidad klscflag.

   De manera predeterminada, la utilidad se encuentra en `/opt/kaspersky/ksc64/sbin`.

3. Ejecute el siguiente comando con una cuenta con privilegios raíz para configurar la autenticación basada en certificados de los dispositivos en el Servidor de administración:
   ```
   ./klscflag -fset -pv ".core/.independent" -s KLLIM -n
   LP_MobileMustUseTwoWayAuthOnPort13292 -t d -v 1
   ```
4. Reinicie el servicio del Servidor de administración.

   Después de iniciar el servicio del Servidor de administración, se requerirá la autenticación basada en certificados del dispositivo mediante un certificado compartido.

   No se exigirá un certificado cuando el dispositivo se conecte al Servidor de administración por primera vez.

De manera predeterminada, la autenticación basada en certificados de los dispositivos está deshabilitada.

Crear un paquete de aplicaciones móviles para dispositivos Android

Para crear un paquete de aplicaciones móviles, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Apps & files**.
2. Haga clic en **Android**.

3. Haga clic en **Apps** y luego en **Add**.

   Se abre la ventana **Add app**.

4. Especifique el nombre de la aplicación en el campo **App name**. Este nombre se usará para identificar la aplicación en la configuración de la directiva.

5. Haga clic en **Select** y seleccione un archivo APK en su equipo.

6. Haga clic en el botón **Save** para guardar los cambios que realizó.

El paquete de aplicaciones recién creado se muestra en la lista de aplicaciones en la pestaña **Apps**.

Si selecciona un archivo APK grande, la aplicación puede tardar un tiempo en cargarse. No cierre la sección **Apps & files** hasta que se cargue la aplicación.

En la sección **Apps & files**, también puede agregar aplicaciones iOS.

Ver la información acerca de un dispositivo Android

Para ver la información acerca de un dispositivo Android, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.

   Se abre la lista de dispositivos administrados.

2. Para filtrar dispositivos Android, haga clic en el encabezado de la columna **OS** y seleccione **Android**.

   Se muestra la lista de dispositivos Android.

   Según la base de datos que utilice, las búsquedas pueden distinguir entre mayúsculas y minúsculas.

3. Seleccione el dispositivo móvil sobre el que quiera ver información.

   Se abre una ventana con las propiedades del dispositivo Android.

La ventana de propiedades del dispositivo móvil muestra información sobre el dispositivo Android conectado.

Los números de IMEI se muestran para todos los dispositivos con Android 5 a 9, dispositivos corporativos con Android 10 o posterior y dispositivos con un contenedor corporativo con Android 10 y 11.

Si se instala una versión anterior de Kaspersky Endpoint Security para Android (10.52.1.3 o anterior) en los dispositivos, el valor del **Operating mode** se establece en **Desconocido**.

Desconectar de la administración un dispositivo Android

Para desconectar un dispositivo Android de la administración, el usuario debe eliminar Kaspersky Endpoint Security para Android del dispositivo móvil. Una vez que el usuario haya eliminado Kaspersky Endpoint Security para Android, el administrador puede eliminar el dispositivo móvil de la lista de dispositivos administrados en Kaspersky Next Expert View (on-premise).

Si Kaspersky Endpoint Security para Android no se ha eliminado del dispositivo móvil, este reaparecerá en la lista de dispositivos administrados después de la sincronización con el Servidor de administración.

Para eliminar un dispositivo Android de la lista de dispositivos administrados, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.

   Se abre la lista de dispositivos administrados.

2. Para filtrar dispositivos Android, haga clic en el encabezado de la columna **OS** y seleccione **Android**.

   Se muestra la lista de dispositivos Android.

3. Seleccione el dispositivo móvil que desea desconectar.

4. Haga clic en **Delete**.

El dispositivo móvil se elimina de la lista de dispositivos administrados.

Administrar dispositivos MDM con iOS

En esta sección se describen las características avanzadas para la administración de dispositivos MDM con iOS en Kaspersky Next Expert View (on-premise).

Firmar perfiles de administración con un certificado

Esta funcionalidad está disponible en Kaspersky Security Center Linux 15.2 o posterior.

Puede firmar perfiles de administración de dispositivos con un certificado recibido de una autoridad de certificación de confianza.

No se requiere un certificado para que el perfil de administración funcione correctamente. Si el perfil de administración no está firmado con un certificado, al instalar el perfil de administración, aparece una advertencia y se solicita a los usuarios que confirmen que confían en la organización que envió el certificado.

Para firmar perfiles de administración con un certificado:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **iOS MDM Servers**.

   Se abre la lista de Servidores de MDM para iOS.

2. Haga clic en **Signing certificate**.

   Se abre la ventana **Signing certificate**.

3. En el campo **Certificate format**, especifique el tipo de certificado público o privado:

   - Si está seleccionado el valor **PKCS #12**, especifique el archivo de certificado y la contraseña.
   - Si está seleccionado el valor **X.509**:

     a. Especifique el archivo de clave privada.

     b. Especifique el archivo de clave pública.

     c. Especifique la contraseña de la clave privada.

4. Haga clic en **Save**.

Los perfiles de administración que cree ahora se firmarán con el certificado especificado.

Agregar un perfil de configuración

Para crear un perfil de configuración, puede utilizar Apple Configurator 2, que está disponible en el sitio web de Apple. Apple Configurator 2 solo funciona en dispositivos que ejecutan macOS. Si no tiene estos dispositivos a su disposición, puede usar la Utilidad de configuración de iPhone. Sin embargo, Apple ya no es compatible con la Utilidad de configuración de iPhone.

Para agregar un perfil de configuración a un Servidor de MDM para iOS, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management → Mobile → iOS MDM Servers**. En la lista de Servidores de MDM para iOS que se abre, haga clic en el Servidor de MDM para iOS cuya configuración desea modificar.
2. En la ventana de configuración del Servidor de MDM para iOS, seleccione **Application settings**.
3. Seleccione la pestaña **Configuration profiles**.
4. Para agregar un nuevo perfil de configuración, haga clic en **Add**.
5. En la ventana que se abre, seleccione el perfil de configuración que desea agregar.

   El nombre del perfil de configuración no debe superar los 100 caracteres. Si ingresa un nombre más largo, solo se mostrará una parte.

El nuevo perfil de configuración se mostrará en la lista de perfiles de configuración.

Puede instalar el perfil que creó en dispositivos MDM con iOS.

Instalación de un perfil de configuración en un dispositivo

Puede instalar un perfil de configuración en un dispositivo MDM con iOS en la ventana **Send command** o en la pestaña **Configuration profiles** en la ventana de propiedades del dispositivo.

En la ventana **Send command**, puede instalar perfiles de configuración en varios dispositivos.

Para instalar un perfil de configuración en la ventana Send command, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.
2. En la lista de dispositivos que se abre, seleccione los dispositivos en los que desea instalar los perfiles de configuración.
3. Haga clic en **Send command**.
4. En la ventana **Send command** que se abre, en el campo **Command**, seleccione el comando **Install configuration profile**.
5. En la sección **Configuration profiles**, seleccione los perfiles de configuración que desea instalar en los dispositivos.
6. Haga clic en **Send**.

El comando se envía a los dispositivos seleccionados.

Para instalar un perfil de configuración en la ventana de propiedades del dispositivo, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.
2. En la lista de dispositivos que se abre, haga clic en el nombre del dispositivo en el que desea instalar los perfiles de configuración.

   Se abre la ventana de propiedades del dispositivo.
3. Seleccione la pestaña **Configuration profiles**.
4. En la parte superior de la lista de perfiles de configuración, haga clic en **Install**.
5. En la ventana que se abre, seleccione los perfiles de configuración que desea instalar en el dispositivo y haga clic en **Install**.

Se envía el comando al dispositivo.

La instalación de perfiles puede tardar unos minutos El comando se ejecuta solo si un dispositivo está conectado a Internet. Para comprobar si se instaló un perfil, haga clic en **Refresh list**.

Eliminar un perfil de configuración de un dispositivo

Puede eliminar un perfil de configuración de un dispositivo MDM con iOS en la ventana **Send command** o en la pestaña **Configuration profiles** en la ventana de propiedades del dispositivo.

En la ventana **Send command**, puede eliminar los perfiles de configuración de varios dispositivos.

Para eliminar un perfil de configuración en la ventana Send command, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.
2. En la lista de dispositivos que se abre, seleccione los dispositivos de los que desea eliminar los perfiles de configuración.
3. Haga clic en **Send command**.
4. En la ventana **Send command** que se abre, en el campo **Command**, seleccione el comando **Delete configuration profile**.
5. En la sección **Configuration profiles**, seleccione los perfiles de configuración que desea eliminar de los dispositivos.
6. Haga clic en **Send**.

El comando se envía a los dispositivos seleccionados.

El perfil puede aparecer en la lista de perfiles de configuración instalados en el dispositivo durante varios minutos después de que se haya eliminado.

Para eliminar un perfil de configuración en la ventana de propiedades del dispositivo, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.
2. En la lista de dispositivos que se abre, haga clic en el nombre del dispositivo del que desea eliminar los perfiles de configuración.

   Se abre la ventana de propiedades del dispositivo.
3. Seleccione la pestaña **Configuration profiles**.
4. En la lista de perfiles de configuración, seleccione los perfiles de configuración que desea eliminar del dispositivo y haga clic en **Eliminar**.

Se envía el comando al dispositivo.

La eliminación de los perfiles puede tardar unos minutos El comando se ejecuta solo si un dispositivo está conectado a Internet. Para comprobar si se eliminó un perfil, haga clic en **Refresh list**.

No puede impedir que los usuarios eliminen el perfil de configuración mediante la configuración del dispositivo.

Configurar aplicaciones administradas

Antes de instalar una aplicación en un dispositivo MDM con iOS, debe agregar esa aplicación al Servidor de administración. Una aplicación se considera administrada si se instaló en un dispositivo a través de Kaspersky Mobile Devices Protection and Management. Una aplicación administrada se puede administrar de forma remota mediante Kaspersky Mobile Devices Protection and Management.

Para agregar una aplicación administrada a un Servidor de MDM para iOS, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Apps & files**.

2. Haga clic en **iOS** y luego en **Add**.

   Se abre la ventana **Add app**.

3. Especifique el nombre de la aplicación en el campo **App name**. Este nombre se usará para identificar la aplicación en la configuración de la directiva.

4. En el campo **Installation method**, seleccione uno de los siguientes métodos para agregar la aplicación:

   - **Installation package**

   - **Link to manifest file**

     Un archivo de manifiesto es un archivo PLIST que se requiere para instalar una aplicación en un dispositivo iOS. Estos archivos son diccionarios que contienen los ajustes de instalación de la aplicación (por ejemplo, la ubicación del paquete de instalación). Cuando usa un archivo de manifiesto para agregar una aplicación, debe completar esta configuración manualmente. Cuando agrega una aplicación desde App Store o un archivo IPA, el archivo de manifiesto se genera automáticamente.

     Para obtener un archivo de manifiesto para una aplicación, recomendamos primero agregar la aplicación al Servidor de MDM para iOS mediante un archivo IPA. En este caso, el Servidor de MDM para iOS genera automáticamente un archivo de manifiesto, que puede descargar y modificar más tarde.

   - **App Store**

5. Realice una de las siguientes acciones:

   Utilice solo fuentes legítimas y de confianza. Al configurar los ajustes en esta sección, usted es el único responsable de los posibles riesgos y consecuencias asociados con el uso de fuentes no confiables.

   - Si seleccionó **Installation package**, haga clic en **Select** y cargue un archivo IPA desde su equipo.

   - Si seleccionó **Link to manifest file**, especifique un vínculo a un archivo de manifiesto que se puede usar para descargar la aplicación.

   - Si seleccionó **App Store**, especifique un vínculo o ID de la aplicación que se agregará desde App Store.

6. Si es necesario, en la sección **Per App VPN**, configure Per App VPN.

7. Si es necesario, ajuste la configuración siguiente:

   - Seleccione la casilla **Remove when device management profile is deleted** si desea que la aplicación se elimine del dispositivo móvil del usuario junto con el perfil de administración. Esta casilla está marcada por defecto.

   - Seleccione la casilla **Block backup of app data to iCloud** si desea bloquear la copia de seguridad de los datos de la aplicación en iCloud.

8. Si desea agregar una configuración personalizada para la aplicación, en la sección **App configuration**, haga clic en **Select** y seleccione un archivo de configuración en formato PLIST en su equipo.

   Para generar un archivo de configuración, puede usar un generador de configuración (por ejemplo, https://appconfig.jamfresearch.com/generator) o consultar la documentación oficial de la aplicación a configurar.

   Ejemplo de configuración básica para la aplicación Microsoft Outlook

   Configuración de la aplicación Microsoft Outlook

Clave de la configuración	Descripción	Tipo	Valor	Valo predeterr
`com.microsoft.outlook.EmailProfile.EmailAccountName`	Nombre de usuario	String	El nombre de usuario que se utilizará para extraer el nombre de usuario de Microsoft Active Directory. Puede ser diferente a la dirección de correo electrónico del usuario. Por ejemplo: `User`.	
`com.microsoft.outlook.EmailProfile.EmailAddress`	Dirección de correo electrónico	String	La dirección de correo electrónico que se utilizará para extraer la dirección de correo electrónico del usuario de Microsoft Active Directory. Por ejemplo, `user@companyname.com`.	
`com.microsoft.outlook.EmailProfile.EmailUPN`	Nombre principal del usuario o nombre de usuario para el perfil de correo electrónico que se utiliza para autenticar la cuenta	String	El nombre del usuario en formato de dirección de correo electrónico. Por ejemplo, `userupn@companyname.com`.	
`com.microsoft.outlook.EmailProfile.ServerAuthentication`	Método de autenticación	String	`Username and Password`: solicita al usuario del dispositivo su contraseña. `Certificates`: autenticación basada en certificados.	`Nombre usuario contras`
`com.microsoft.outlook.EmailProfile.ServerHostName`	ActiveSync FQDN	String	Dirección URL del servidor de correo electrónico Exchange ActiveSync. No es necesario que utilice HTTP:// o HTTPS:// delante de la URL. Por ejemplo, `mail.companyname.com`.	
`com.microsoft.outlook.EmailProfile.AccountDomain`	Dominio de correo electrónico	String	El dominio de la cuenta del usuario. Por ejemplo, `companyname`.	

Clave de la configuración	Descripción	Tipo	Valor	Valo predeterr
`com.microsoft.outlook.EmailProfile.AccountType`	Tipo de autenticación	String	`ModernAuth`: utiliza un método de administración de identidades basado en tokens. Especifique ModernAuth como el Tipo de cuenta para Exchange Online. `BasicAuth`: solicita al usuario del dispositivo su contraseña. Especifique BasicAuth como el Tipo de cuenta para Exchange local.	`BasicAu`
`IntuneMAMRequireAccounts`	Es necesario iniciar sesión	String	Especifica si es necesario iniciar sesión en la cuenta. Puede seleccionar uno de los siguientes valores: `Enabled`: la aplicación requiere que el usuario inicie sesión en la cuenta de usuario administrada definida por la clave `IntuneMAMUPN` para recibir datos de la organización. `Disabled`: no es necesario iniciar sesión en la cuenta.	
`IntuneMAMUPN`	Dirección UPN	String	El nombre principal del usuario de la cuenta a la que se le permite iniciar sesión en la aplicación. Por ejemplo, `userupn@companyname.com`.	

Ejemplo de un archivo de configuración para la aplicación de Microsoft Outlook

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>com.microsoft.outlook.EmailProfile.AccountType</key>
  <string>BasicAuth</string>
  <key>com.microsoft.outlook.EmailProfile.EmailAccountName</key>
  <string>My Work Email</string>
  <key>com.microsoft.outlook.EmailProfile.ServerHostName</key>
  <string>exchange.server.com</string>
  <key>com.microsoft.outlook.EmailProfile.EmailAddress</key>
  <string>%email%</string>
  <key>com.microsoft.outlook.EmailProfile.EmailUPN</key>
  <string>%full_name%</string>
  <key>com.microsoft.outlook.EmailProfile.AccountDomain</key>
  <string>my-domain</string>
  <key>com.microsoft.outlook.EmailProfile.ServerAuthentication</key>
  <string>Username and Password</string>
  <key>IntuneMAMAllowedAccountsOnly</key>
  <string>Enabled</string>
  <key>IntuneMAMUPN</key>
  <string>%full_name%</string>
</dict>
</plist>
```

Puede usar macros en los campos correspondientes del archivo de configuración para reemplazar valores.
Macros disponibles

Macros que se pueden usar en los archivos de configuración

Macro	Descripción
%full_name%	Nombre de usuario completo
%email%	Dirección de correo electrónico principal del usuario
%email1%	Primera dirección de correo electrónico de respaldo del usuario
%email2%	Segunda dirección de correo electrónico de respaldo del usuario
%mobile_phone%	Número de teléfono celular del usuario
%phone_number%	Número de teléfono principal del usuario
%phone_number1%	Primer número de teléfono de respaldo del usuario
%phone_number2%	Segundo número de teléfono de respaldo del usuario
%short_name%	Nombre de usuario
%domain_name%	Nombre de dominio del usuario
%job_title%	Puesto de trabajo del usuario
%department%	Nombre del departamento
%company%	Nombre de la empresa

9. Haga clic en el botón **Save** para guardar los cambios que realizó.

La aplicación recién creada se muestra en la tabla de aplicaciones en la pestaña **iOS**.

Si selecciona un archivo IPA grande, es posible que la aplicación tarde un poco en cargarse. No cierre la sección **Apps & files** hasta que se cargue la aplicación.

Puede ver y editar las propiedades de la aplicación haciendo clic en la aplicación en la lista o eliminar la aplicación con el botón **Delete**.

Instalar una app en un dispositivo móvil

Para instalar una aplicación en un dispositivo móvil, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.
2. En la lista de dispositivos que se abre, seleccione los dispositivos en los que desea instalar aplicaciones.
3. Haga clic en **Send command**.
4. En la ventana **Send command** que se abre, en el campo **Command**, seleccione el comando **Install app**.
5. En el campo **Apps**, seleccione las aplicaciones que desea instalar en los dispositivos.
6. Haga clic en **Send**.

El comando se envía a los dispositivos seleccionados.

Actualizar una app instalada en un dispositivo

Puede actualizar una aplicación en un dispositivo MDM con iOS en la ventana **Send command** o en la pestaña **Apps** en la ventana de propiedades del dispositivo.

En la ventana **Send command**, puede actualizar aplicaciones en varios dispositivos.

Para actualizar una aplicación en un dispositivo MDM con iOS en la ventana Send command, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.
2. En la lista de dispositivos que se abre, seleccione los dispositivos en los que desea actualizar aplicaciones.
3. Haga clic en **Send command**.
4. En la ventana **Send command** que se abre, en el campo **Command**, seleccione el comando **Update app**.
5. En la sección **Apps**, seleccione las aplicaciones que desea actualizar en los dispositivos.
6. Haga clic en **Send**.

El comando se envía a los dispositivos seleccionados.

Para actualizar una aplicación en un dispositivo MDM con iOS en la ventana de propiedades del dispositivo, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.
2. En la lista de dispositivos que se abre, haga clic en el nombre del dispositivo en el que desea actualizar las aplicaciones.

   Se abre la ventana de propiedades del dispositivo.
3. Seleccione la pestaña **Apps**.
4. En la parte superior de la lista de aplicaciones, haga clic en **Update**.
5. En la ventana que se abre, seleccione las aplicaciones que desea actualizar en el dispositivo y haga clic en **Update**.

Se envía el comando al dispositivo.

La actualización de aplicaciones puede tardar unos minutos El comando se ejecuta solo si un dispositivo está conectado a Internet. Para comprobar si se actualizó una aplicación, haga clic en **Refresh list**.

Eliminar una app de un dispositivo

Puede eliminar una aplicación de un dispositivo MDM con iOS en la ventana **Send command** o en la pestaña **Apps** en la ventana de propiedades del dispositivo.

En la ventana **Send command**, puede eliminar aplicaciones de varios dispositivos.

Para eliminar una aplicación de un dispositivo MDM con iOS en la ventana Send command, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.
2. En la lista de dispositivos que se abre, seleccione los dispositivos de los que desea eliminar las aplicaciones.
3. Haga clic en **Send command**.
4. En la ventana **Send command** que se abre, en el campo **Command**, seleccione el comando **Delete app**.
5. En la sección **Apps**, seleccione las aplicaciones que desea eliminar de los dispositivos.
6. Haga clic en **Send**.

El comando se envía a los dispositivos seleccionados.

Para eliminar una aplicación de un dispositivo MDM con iOS en la ventana de propiedades del dispositivo, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.
2. En la lista de dispositivos que se abre, haga clic en el nombre del dispositivo del que desea eliminar las aplicaciones.

   Se abre la ventana de propiedades del dispositivo.
3. Seleccione la pestaña **Apps**.
4. En la lista de aplicaciones, seleccione las aplicaciones que desea eliminar del dispositivo y haga clic en **Delete**.

Se envía el comando al dispositivo.

La eliminación de aplicaciones puede tardar unos minutos El comando se ejecuta solo si un dispositivo está conectado a Internet. Para comprobar si se eliminó una aplicación, haga clic en **Refresh list**.

Configuración de roaming en un dispositivo móvil MDM con iOS

Para configurar roaming:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.
2. En la lista de dispositivos que se abre, seleccione los dispositivos para los que desea establecer la configuración de roaming.

3. Haga clic en **Send command**.

4. En la ventana **Send command** que se abre, en el campo **Command**, seleccione el comando **Change roaming settings**.

5. En la sección **Action**, realice una de las siguientes acciones:

   - Si desea habilitar el roaming de datos, seleccione **Enable data roaming**.

   - Si desea deshabilitar el roaming de datos, seleccione **Disable data roaming**.

6. Haga clic en **Send**.

El comando se envía a los dispositivos seleccionados.

Ver la información acerca de un dispositivo MDM con iOS

Para ver información acerca de un dispositivo MDM con iOS:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.

   Se abre la lista de dispositivos administrados.

2. Para filtrar los dispositivos MDM con iOS, haga clic en el encabezado de la columna **Operating mode** y seleccione el modo de funcionamiento del dispositivo MDM con iOS sobre el que desea ver la información.

   Se muestra la lista de dispositivos MDM con iOS.

   > Según la base de datos que utilice, las búsquedas pueden distinguir entre mayúsculas y minúsculas.

3. Seleccione el dispositivo móvil sobre el que quiera ver información.

   Se abre una ventana con las propiedades del dispositivo MDM con iOS.

   > Al mostrar valores numéricos, es posible que se produzca un error de varias centésimas.

La pestaña **General** de la ventana de propiedades muestra información acerca del dispositivo MDM con iOS conectado.

> Es posible que no se muestren las siguientes propiedades de los dispositivos MDM con iOS 26 o versiones posteriores: **IMEI**, **Número de teléfono**, **MEID**, **ICCID**, **Nombre de la red móvil actual**, **Nombre de la red móvil local**, **Versión de la configuración del operador**, **Roaming de voz habilitado**, **En itinerancia**, **Código de país de la red local**, **Código de la red local**, **Código del país anfitrión**, **Código de red actual**.

La pestaña **Certificates** de la ventana de propiedades muestra información sobre los certificados instalados en el dispositivo MDM con iOS seleccionado.

La pestaña **Apps** de la ventana de propiedades muestra información sobre las aplicaciones instaladas en el dispositivo MDM con iOS seleccionado.

La pestaña **Configuration profiles** de la ventana de propiedades muestra información acerca de los perfiles de configuración instalados en el dispositivo MDM con iOS seleccionado.

Desconectar de la administración un dispositivo MDM con iOS

Si desea dejar de administrar un dispositivo MDM con iOS, puede desconectarlo de la administración en Kaspersky Security Center.

No recomendamos desconectar el dispositivo de la administración eliminando el perfil de administración de un dispositivo MDM con iOS, ya que es posible que dicho dispositivo no funcione correctamente cuando se vuelva a conectar. Para dejar de administrar un dispositivo MDM con iOS, desconéctelo del Servidor de MDM para iOS como se describe en esta sección.

Para desconectar un dispositivo MDM con iOS del Servidor de MDM para iOS:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.

   Se abre la lista de dispositivos administrados.

2. Para filtrar los dispositivos MDM con iOS, haga clic en el encabezado de la columna **Operating mode** y seleccione el modo de funcionamiento del dispositivo MDM con iOS que desea desconectar.

   Se muestra la lista de dispositivos MDM con iOS que funcionan en el modo seleccionado.

3. Seleccione el dispositivo móvil que desea desconectar.

4. Haga clic en **Delete**.

   En la lista, se marca el dispositivo MDM con iOS para su eliminación. En un minuto, el dispositivo se elimina de la base de datos del Servidor de MDM para iOS, después de lo cual se elimina automáticamente de la lista de dispositivos administrados.

Una vez que el dispositivo MDM con iOS se desconecta de la administración, todos los perfiles de configuración instalados, el perfil de administración y las aplicaciones para las que se habilitó la opción **Remove when device management profile is deleted** en la configuración del Servidor de MDM para iOS, se eliminarán del dispositivo. La directiva de MDM para iOS también se eliminará.

No puede evitar que los usuarios eliminen un perfil de administración a través de la configuración del dispositivo.

Administración de la configuración de dispositivos móviles

Esta sección contiene información sobre cómo administrar la configuración de dispositivos móviles de forma remota en Kaspersky Next Expert View (on-premise).

Configuración de conexión a una red Wi-Fi

Esta sección proporciona instrucciones acerca de cómo configurar la conexión automática a una red Wi-Fi corporativa en dispositivos iOS con MDM y en dispositivos Android.

Conexión de dispositivos Android a una red Wi-Fi

Para que un dispositivo Android se conecte automáticamente a una red Wi-Fi disponible y para proteger los datos durante la conexión, debe configurar las opciones de conexión.

Para conectar un dispositivo móvil a una red Wi-Fi, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **Android** y vaya a la sección **Device configuration**.
4. En la tarjeta **Wi-Fi**, haga clic en **Settings**.

   Se abre la ventana **Wi-Fi**.
5. Habilite la configuración con el interruptor **Wi-Fi**.
6. Haga clic en **Add**.

   Se abre la ventana **Add Wi-Fi network**.
7. En el campo **Service set identifier (SSID)**, escriba el nombre de la red Wi-Fi que incluye el punto de acceso (SSID).
8. Seleccione la casilla **Connect automatically** si desea que los dispositivos se conecten automáticamente a la red Wi-Fi.
9. Seleccione la casilla **Hidden network** si desea que la red Wi-Fi se oculte en la lista de redes disponibles en el dispositivo.

   En este caso, para conectarse a la red, el usuario debe ingresar manualmente el identificador de red (SSID) especificado en la configuración del enrutador Wi-Fi en el dispositivo móvil.
10. En la sección **Protection**, seleccione el tipo de seguridad de la red Wi-Fi (red abierta o red segura protegida con el protocolo WEP, WPA2 PSK, WPA3 PSK, WPA3-Enterprise, WPA3-Enterprise 192-bit o 802.1.x EAP).

    El protocolo de seguridad 802.1.x EAP solo es compatible con la versión 10.48.1.1 o posterior de Kaspersky Endpoint Security para Android. El protocolo WEP solo es compatible con Android 9 o versiones anteriores. Los protocolos WPA3 PSK, WPA3-Enterprise y WPA3-Enterprise 192-bit solo son compatibles con Android 10 o versiones posteriores.

11. Si seleccionó el protocolo de seguridad 802.1.x EAP, WPA3-Enterprise o WPA3-Enterprise 192-bit, especifique la siguiente configuración de protección de red:

- **EAP method**

  Especifica un método de Protocolo de autenticación extensible (EAP) para la autenticación de red. Valores posibles:

  - **TLS** (predeterminado)
  - **PEAP**
  - **TTLS**

- **Method for uploading root certificate**

  Especifica la forma en que desea cargar un certificado raíz. Valores posibles:

  - **From the list of root certificates**: permite seleccionar cualquier certificado disponible en la lista desplegable.
  - **From file**: le permite cargar un archivo de certificado desde su equipo.

- **Root certificate**

  Especifica el certificado raíz que utilizará la red Wi-Fi.

- **User certificate**

  Especifica el certificado de usuario utilizará la red Wi-Fi si se selecciona el método TLS EAP.

  Los siguientes valores están disponibles en la lista desplegable:

  - **Not selected**: el certificado de usuario no está especificado.
  - **User certificates**: los certificados VPN que se agregaron en la sección **Certificados** y se instalaron en el dispositivo del usuario. Si elige esta opción, pero no hay un certificado VPN instalado en el dispositivo, el certificado de usuario no se usa para esta red Wi-Fi.
  - **SCEP profiles**: perfiles de certificado SCEP configurados en los ajustes de **SCEP and NDES** y que se utilizan para obtener certificados.

- **Domain name**

  Especifica la restricción para el nombre de dominio del servidor.

  Si se establece, este nombre de dominio completo (FQDN) se usa como un requisito de coincidencia de sufijo para el certificado raíz en los elementos SubjectAltName dNSName. Si se encuentra un dNSName coincidente, se cumple esta restricción.

  Puede especificar varias cadenas de coincidencia utilizando punto y coma para separar las cadenas. Una coincidencia con cualquiera de los valores se considera una coincidencia suficiente para el certificado (es decir, se utiliza el operador OR).

  Si especifica *, cualquier certificado raíz se considera válido. Se especifica este valor de manera predeterminada.

- **Two-factor authentication type**

  Especifica un tipo de autenticación de dos factores. Valores posibles:

  - **Not selected** (predeterminado)
  - **MSCHAP**
  - **MSCHAPV2**
  - **GTC**

- **User ID**

  Especifica un ID de usuario que se utilizará para conectarse a la red Wi-Fi.

- **Anonymous ID**

  Especifica una identidad anónima que es diferente de la identidad del usuario y se utiliza si se selecciona el método PEAP o TTLS de autenticación de red.

- **Password**

  Especifica una contraseña para acceder a la red inalámbrica. La contraseña se enviará en un código QR.

  No envíe la contraseña para una red Wi-Fi confidencial que no debe estar disponible al público. La contraseña se transmite sin cifrar junto con otros datos para configurar el dispositivo.

12. En el campo **Password**, establezca una contraseña de acceso a la red si seleccionó una red segura en el paso 9.
13. En la pestaña **Additional**, seleccione la casilla **Use a proxy server** si desea usar un servidor proxy para conectarse a la red Wi-Fi.
14. Si seleccionó **Use a proxy server**, en los campos **Proxy server address** y **Proxy server port**, escriba la dirección IP o el nombre DNS del servidor proxy y el número de puerto, si corresponde.

    En dispositivos que ejecutan Android 8 o posterior, la configuración del servidor proxy para Wi-Fi no se puede redefinir con una directiva. Sin embargo, puede establecer manualmente la configuración del servidor proxy para una red Wi-Fi en el dispositivo móvil.

    Si no está utilizando un servidor proxy para conectarse a una red Wi-Fi, no hay limitaciones en el uso de directivas para administrar una conexión de red Wi-Fi.
15. En el campo **Do not use proxy server for the specified addresses**, agregue las direcciones web a la que se pueda acceder sin el uso del servidor proxy.

    Por ejemplo, puede escribir la dirección `example.com`. En este caso, el servidor proxy no se utilizará para las direcciones `pictures.example.com`, `example.com/movies`, etc. El protocolo (por ejemplo, `http://`) se puede omitir.

    En dispositivos con Android 8 o posterior, la exclusión de direcciones web del servidor proxy no funciona.
16. Haga clic en **Agregar**.

La red Wi-Fi agregada se muestra en la lista de redes Wi-Fi.

Esta lista contiene los nombres de las redes inalámbricas sugeridas.

En dispositivos personales con Android 10 o versiones posteriores, el sistema operativo solicita al usuario que se conecte a dichas redes. Las redes sugeridas no aparecen en la lista de redes guardadas en estos dispositivos.

En dispositivos corporativos y dispositivos personales con Android 9 o versiones anteriores, después de sincronizar el dispositivo con el Servidor de administración, el usuario del dispositivo puede seleccionar una red inalámbrica sugerida en la lista de redes guardadas y conectarse a ella sin tener que especificar ninguna configuración de red.

Puede modificar o eliminar redes Wi-Fi en la lista de redes con los botones **Edit** y **Delete** que se encuentran en la parte superior de la lista.

17. Haga clic en **Aceptar**.

18. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

En dispositivos con Android 10 o versiones posteriores, si un usuario se rehúsa a conectarse a la red Wi-Fi sugerida, se revoca el permiso de la aplicación para cambiar el estado de Wi-Fi. El usuario debe otorgar este permiso de manera manual.

Conexión de dispositivos MDM con iOS a una red Wi-Fi

Para que un dispositivo MDM con iOS se conecte automáticamente a una red Wi-Fi disponible y para proteger los datos durante la conexión, debe configurar las opciones de conexión.

Para configurar la conexión de un dispositivo iOS con MDM a una red Wi-Fi:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **iOS** y vaya a la sección **Device configuration**.

4. En la tarjeta **Wi-Fi**, haga clic en **Settings**.

   Se abre la ventana **Wi-Fi**.

5. Habilite la configuración con el interruptor **Wi-Fi**.

6. Haga clic en **Agregar**.

   Se abre la ventana **Add Wi-Fi network**.

7. En el campo **Service set identifier (SSID)**, escriba el nombre de la red Wi-Fi que incluye el punto de acceso (SSID).

8. Si desea que los dispositivos MDM con iOS se conecten a la red Wi-Fi automáticamente, seleccione la casilla **Connect automatically**.

   Si desactiva la conexión automática a una red Wi-Fi existente en la configuración de la directiva, no podrá volver a activar la conexión automática a esta red. Esto se debe a un problema reconocido por Apple.

9. Si no desea que los dispositivos MDM con iOS se conecten a redes Wi-Fi que requieran autenticación preliminar (redes cautivas), seleccione la casilla **Disable captive network detection**.

   Para usar una red cautiva, debe suscribirse, aceptar un contrato o hacer un pago. Las redes cautivas pueden implementarse en cafeterías y hoteles, por ejemplo.

10. Si desea que la red Wi-Fi esté oculta en la lista de redes disponibles en el dispositivo MDM con iOS, seleccione la casilla **Hidden network**.

    En este caso, para conectarse a la red, el usuario debe ingresar manualmente el identificador de red (SSID) especificado en la configuración del enrutador Wi-Fi en el dispositivo móvil.

11. Si desea que los dispositivos MDM con iOS utilicen direcciones MAC estáticas cuando se conecten a la red Wi-Fi, seleccione la casilla **Disable MAC address randomization**.

12. En la sección **Protection**, seleccione el tipo de seguridad de la red Wi-Fi (red abierta o red segura protegida con el protocolo WEP, WPA, WPA2 o WPA3).

    En dispositivos que ejecutan iOS 15 o versiones anteriores, la selección de WPA, WPA2 o WPA3 es idéntica y le permite conectarse a cualquier red protegida mediante WPA.

    - **Open network**. No se requiere autenticación de usuario.
    - **WEP**. La red está protegida con el protocolo de cifrado inalámbrico WEP.

      La protección WEP está disponible en dispositivos con iOS 5 o posterior.

    - **WPA**. La red está protegida mediante el protocolo WPA (acceso protegido a Wi-Fi) o WPA2.
    - **WPA2**. La red se protege con el protocolo de seguridad WPA2 o WPA3.
    - **WPA3**. La red está se protege con el protocolo de seguridad WPA3.
    - **Personal network (any)**. La red está protegida por los protocolos de cifrado WEP, WPA, WPA2 o WPA3 según el tipo de enrutador Wi-Fi. Para autenticación se utiliza una clave única de cifrado para cada usuario.
    - **WEP (corporate network)**. Se protege la red utilizando el protocolo WEP y con una clave dinámica.
    - **WPA (corporate network)**. La red está protegida mediante el protocolo de cifrado WPA o WPA2 con el uso del protocolo 802.1X.
    - **WPA2 (corporate network)**. La red está protegida mediante el protocolo de cifrado WPA2 o WPA3 y con una clave única para todos los usuarios (802.1X).

- **WPA3 (corporate network)**. La red está protegida mediante el protocolo de cifrado WPA3 y con una clave única para todos los usuarios (802.1X).

- **Corporate network (any)**. La red está protegida por los protocolos WEP, WPA, WPA2 o WPA3 según el tipo de enrutador Wi-Fi. La autenticación se realiza mediante una sola clave de cifrado compartida por todos los usuarios.

Si seleccionó alguna de las opciones de red corporativa, en la sección **EAP protocol** puede seleccionar los tipos de protocolos EAP (Protocolo de autenticación extensible) para la identificación de usuarios en la red Wi-Fi.

En la sección **Trusted certificates**, también puede crear una lista de certificados de confianza para la autenticación del usuario de dispositivos MDM con iOS en servidores de confianza.

13. En la sección **Authentication**, configure las opciones de la cuenta para la autenticación del usuario luego de que el dispositivo MDM con iOS se conecte a la red Wi-Fi:

    a. En el campo **User name**, escriba el nombre de la cuenta para la autenticación del usuario al conectarse a la red Wi-Fi.

    b. En el campo **User ID**, escriba el ID de usuario que se muestra durante la transmisión de información en la autenticación en lugar del nombre real del usuario.

    El ID de usuario está diseñado para hacer que el proceso de autenticación sea más seguro, ya que el nombre de usuario no se muestra, sino que se transmite a través de un túnel TLS cifrado.

    c. En el campo **Password**, escriba la contraseña de la cuenta para la autenticación en la red Wi-Fi.

    d. Si desea que el usuario escriba la contraseña manualmente cada vez que se conecta a una red Wi-Fi, active la casilla **Prompt for password at each connection**.

    e. En la lista desplegable **Authentication certificate**, seleccione un certificado para la autenticación del usuario en la red Wi-Fi.

    f. En la lista desplegable **Minimum TLS version**, seleccione la versión mínima de TLS permitida.

    g. En la lista desplegable **Maximum TLS version**, seleccione la versión máxima de TLS permitida.

14. Si es necesario, en la pestaña **Additional**, configure los ajustes para conectarse a la red Wi-Fi a través de un servidor proxy:

    a. Seleccione la casilla **Use a proxy server**.

    b. Configure una conexión a un servidor proxy:

        a. Si desea configurar la conexión automáticamente:

        - Seleccione **Automatic**.

        - En el campo **PAC file URL**, especifique la URL del archivo PAC del proxy.

        - Para permitir al usuario conectar el dispositivo móvil a una red inalámbrica sin usar un servidor proxy cuando no se puede acceder al archivo PAC, seleccione la casilla **Allow direct connection if PAC file cannot be accessed**.

b. Si desea configurar la conexión manualmente:

- Seleccione **Manual**.
- En el campo **Proxy server address** y **Proxy server port**, escriba la dirección IP o nombre DNS del servidor proxy y el número de puerto.
- En el campo **User name**, seleccione una macro que se utilizará como nombre de usuario para la conexión al servidor proxy.
- En el campo **Password**, especifique la contraseña para la conexión al servidor proxy.

15. Haga clic en **Agregar**.

    La nueva red Wi-Fi se muestra en la lista.

16. Haga clic en **Aceptar**.

17. Haga clic en el botón **Save** para guardar los cambios que realizó.

    Como resultado, luego de que se aplica la directiva, se configura una conexión a red Wi-Fi en el dispositivo iOS con MDM del usuario. El dispositivo móvil del usuario se conecta en forma automática a redes Wi-Fi disponibles. El método de autenticación seleccionado asegura la protección de datos durante la conexión a una red Wi-Fi.

Configuración de correo electrónico

Esta sección contiene información sobre la configuración de buzones de correo en dispositivos móviles.

Configuración de un buzón de correo en dispositivos iOS con MDM

Esta configuración se aplica a los dispositivos supervisados y a los dispositivos que funcionan en el modo de control básico.

Para permitir que un dispositivo MDM de iOS funcione con un correo electrónico, añada la cuenta del correo electrónico del usuario a la lista de cuentas en el dispositivo MDM de iOS.

De forma predeterminada, la cuenta de correo electrónico se agrega con la siguiente configuración:

- Protocolo de correo electrónico: IMAP.
- El usuario puede trasladar mensajes de correo electrónico entre las cuentas de usuario y sincronizar las direcciones de las cuentas.
- El usuario puede usar cualquier cliente de correo electrónico (que no sea Correo) para usar el correo electrónico.
- La conexión SSL no se usa durante la transmisión de mensajes.

Puede editar la configuración especificada cuando agrega una cuenta.

Para añadir una cuenta de correo electrónico del usuario del dispositivo iOS con MDM:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **iOS** y vaya a la sección **Device configuration**.
4. En la tarjeta **Email**, haga clic en **Settings**.

   Se abre la ventana **Email**.
5. Habilite la configuración con el interruptor **Email**.
6. Haga clic en **Add**.

   Se abre la ventana **Add email account**.
7. Especifique la configuración de la cuenta de correo electrónico:

   - En la pestaña **General**, defina los siguientes ajustes:

     a. En el campo **User name**, escriba el nombre del usuario del dispositivo MDM con iOS. Puede ingresar un valor o seleccionar una macro haciendo clic en el botón +.

     b. En el campo **Email address**, especifique la dirección de correo electrónico del usuario del dispositivo MDM con iOS. Puede ingresar un valor o seleccionar una macro haciendo clic en el botón +.

     c. En el campo **Account description**, escriba una descripción de la cuenta de correo electrónico del usuario.

     d. En el campo **Email protocol**, seleccione uno de los siguientes protocolos:

     - **POP**
     - **IMAP**

     e. Si seleccionó **IMAP**, especifique el prefijo de ruta IMAP en el campo **IMAP path prefix**.

     El prefijo de la ruta IMAP debe introducirse en letras mayúsculas (por ejemplo, GMAIL para Google Mail).

     f. En las secciones **Incoming mail server settings** y **Outgoing mail server settings**, configure los ajustes de conexión del servidor:

     - En el campo **Server address**, especifique los nombres de los hosts o las direcciones IP de los servidores de correo entrante y saliente.
     - En los campos **Server port**, especifique los números de puerto de los servidores de correo entrante y saliente.

Para configurar los ajustes opcionales para los servidores de correo entrante y saliente, haga clic en **More settings** y haga lo siguiente:

- En el campo **User name**, especifique el nombre de la cuenta del usuario para la autorización en los servidores de correo entrante y saliente. Puede ingresar un valor o seleccionar una macro haciendo clic en el botón +.
- En el campo **Authentication type**, seleccione el tipo de autenticación de la cuenta de correo electrónico del usuario en los servidores de correo entrante y saliente.
- En el campo **Password**, especifique la contraseña de la cuenta para la autenticación en los servidores de correo entrante y saliente protegidos mediante el método de autenticación seleccionado.
- Si desea usar el protocolo de transporte de datos SSL (Secure Sockets Layer), seleccione la casilla **Use SSL connection**.
- Si desea usar la misma contraseña para la autenticación del usuario en los servidores de correo entrante y saliente, seleccione la casilla **Use the same password for incoming and outgoing mail servers**.

- En la pestaña **Additional**, configure los ajustes adicionales de la cuenta de correo electrónico:

  a. En la sección **Permissions**, seleccione o desmarque las siguientes casillas, si es necesario:

  - **Allow syncing recent addresses**

    Mover mensajes de correo electrónico entre cuentas.

    Si se selecciona la casilla, el usuario puede mover mensajes de correo electrónico de una cuenta a otra.

    Si la casilla está desmarcada, el usuario no puede mover mensajes de correo electrónico de una cuenta a otra.

    Esta casilla está marcada por defecto.

    > Si desea prohibir guardar, mover y compartir archivos adjuntos desde un buzón de correo corporativo, desactive la casilla **Allow movement of messages between accounts (including work and personal accounts)** y seleccione la casilla **Prohibit non-managed apps from using documents from managed apps** y **Prohibit managed apps from using documents from non-managed apps**.

  - **Allow movement of messages between accounts (including work and personal accounts)**

    Sincronización de direcciones de correo electrónico entre cuentas.

    Si la casilla está marcada, al crear mensajes, el usuario puede usar el historial de direcciones de otra cuenta de correo electrónico.

    Si la casilla está desactivada, las direcciones de correo electrónico usadas no se sincronizan. Al crear un mensaje, el usuario de un dispositivo con MDM de iOS no puede usar el historial de direcciones de otra cuenta de correo electrónico.

    Esta casilla está marcada por defecto.

  - **Allow Mail Drop**

    Uso del servicio Mail Drop para reenviar archivos adjuntos de gran tamaño.

    Si la casilla está marcada, el usuario puede utilizar Mail Drop.

Si la casilla no está marcada, el usuario no puede utilizar Mail Drop.

Esta casilla está desactivada por defecto.

- **Allow using only the Mail app**

  Uso únicamente del cliente de correo estándar de iOS para procesar mensajes.

  Si se selecciona la casilla, el usuario solo podrá usar el correo electrónico en el cliente de correo electrónico estándar de iOS.

  Si la casilla no está marcada, el usuario puede usar el correo electrónico tanto en el cliente de correo estándar de iOS como en otras aplicaciones.

  Esta casilla está desactivada por defecto.

b. En las secciones **Signature** y **Encryption**, configure los ajustes para firmar y cifrar el correo saliente mediante el protocolo S/MIME en la aplicación Correo.

S/MIME es un protocolo para transmitir mensajes cifrados firmados digitalmente. S/MIME proporciona capacidades de la seguridad criptográficas tales como autentificación, control de integridad del mensaje y no rechazo del origen (usando firmas digitales). Este protocolo también ayuda a mejorar la confidencialidad y seguridad de los datos en mensajes de correo electrónico, gracias al uso del cifrado.

- **Sign messages**

  Firma digital de mensajes salientes en la aplicación del Correo.

  Si se selecciona la casilla, los mensajes salientes se firman con una firma digital mediante el protocolo S/MIME. Una firma digital confirma la autenticidad del remitente e indica que los contenidos del mensaje no se han modificado durante la transmisión al destinatario. Se debe seleccionar un certificado de destinatario (clave pública) para la firma de mensajes.

  Esta casilla está desactivada por defecto.

- **Signing certificate for outgoing messages**

  Certificado para firmar mensajes salientes con una firma digital utilizando el protocolo S/MIME. La firma digital garantiza que el mensaje lo envió el usuario del dispositivo MDM con iOS. Puede agregar certificados en la configuración **Certificate management** de la directiva o en la sección **Certificates** de Kaspersky Next Expert View (local).

  Esta lista desplegable está disponible solo si la casilla **Sign messages** está marcada.

- **Encrypt messages by default**

  Codificación de mensajes salientes en la aplicación del Correo.

  Si la casilla está marcada, los mensajes salientes se cifran de manera predeterminada mediante el protocolo S/MIME. Deberá seleccionar un certificado de destinatario (clave pública) para enviar mensajes cifrados. Si no hay un certificado de destinatario instalado, los mensajes no se pueden cifrar. Los mensajes cifrados solo pueden ser vistos por usuarios cuyos dispositivos tengan un certificado instalado.

  Esta casilla está desactivada por defecto.

- **Encryption certificate**

  Certificado de cifrado para cifrar los mensajes salientes mediante el protocolo S/MIME. El cifrado mantiene los mensajes confidenciales durante la transmisión y el almacenamiento. Puede agregar certificados en la configuración **Certificate management** de la directiva o en la sección **Certificates** de Kaspersky Next Expert View (on-premise).

  Esta lista desplegable está disponible solo si la casilla **Encrypt messages by default** está marcada.

- **Show toggle button for encrypting selected messages**

  La visualización del icono en la aplicación del Correo en el campo **Para** para enviar mensajes cifrados.

  Si se selecciona esta casilla, el usuario del dispositivo móvil puede cifrar mensajes individuales al hacer clic en el ícono.

  Si la casilla se desactiva, el icono para cifrar mensajes no se muestra. En este caso, la casilla **Encrypt messages by default** determina si el correo saliente se cifra.

- Si es necesario, en la sección **Per App VPN**, configure Per App VPN.

8. Haga clic en **Save**.

   La nueva cuenta de correo electrónico aparece en la lista.

   Puede modificar o eliminar cuentas de correo electrónico en la lista con los botones **Edit** y **Delete** que se encuentran en la parte superior de la lista.

9. Haga clic en **Aceptar**.

10. Haga clic en el botón **Save** para guardar los cambios que realizó.

    La configuración del dispositivo móvil se cambia después de la siguiente sincronización del dispositivo con el Servidor de MDM para iOS.

    Como resultado, luego de que se aplica la directiva, las cuentas de correo electrónico de la lista se agregan al dispositivo móvil del usuario.

    Recomendamos cerrar y abrir la aplicación Configuración en el dispositivo MDM con iOS después de configurar un buzón.

Configuración de un buzón de correo de Exchange en dispositivos iOS con MDM

Esta configuración se aplica a los dispositivos supervisados y a los dispositivos que funcionan en el modo de control básico.

Para permitir al usuario del dispositivo MDM con iOS utilizar el correo electrónico corporativo, el calendario, los contactos, las notas y las tareas, agregue la cuenta Exchange ActiveSync del usuario en el servidor de Microsoft Exchange.

De forma predeterminada, se agrega una cuenta con la siguiente configuración en el servidor Microsoft Exchange:

- El correo electrónico se sincroniza una vez por semana.
- El usuario puede trasladar mensajes entre las cuentas de usuario y sincronizar las direcciones de las cuentas.
- El usuario puede usar cualquier cliente de correo electrónico (que no sea Mail) para usar el correo electrónico.
- La conexión SSL no se usa durante la transmisión de mensajes.

Puede editar la configuración especificada cuando agrega la cuenta Exchange ActiveSync.

Para agregar una cuenta Exchange ActiveSync del usuario de un dispositivo MDM con iOS, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **iOS** y vaya a la sección **Device configuration**.

4. En la tarjeta **Exchange ActiveSync**, haga clic en **Settings**.

   Se abre la ventana **Exchange ActiveSync**.

5. Habilite la configuración con el interruptor **Exchange ActiveSync**.

6. Haga clic en **Add**.

   Se abre la ventana **Add Exchange ActiveSync account**.

7. Especifique la configuración de Exchange ActiveSync:

   - En la pestaña **General**, especifique los datos del usuario:

     - En el campo **Account name**, escriba el nombre de la cuenta para la autorización en el servidor Microsoft Exchange. Puede ingresar un valor o seleccionar una macro haciendo clic en el botón +.

     - En el campo **Exchange ActiveSync server address**, escriba el nombre DNS o la dirección IP del servidor Microsoft Exchange.

     - Ajustes de la sección **User credentials**:

       - En el campo **User domain**, escriba el nombre de dominio del usuario del dispositivo MDM con iOS. Puede ingresar un valor o seleccionar una macro haciendo clic en el botón +.

       - En el campo **User name**, escriba el nombre del usuario del dispositivo MDM con iOS. Puede ingresar un valor o seleccionar una macro haciendo clic en el botón +.

         Si deja este campo en blanco, Kaspersky Mobile Devices Protection and Management solicita al usuario que ingrese el nombre de usuario cuando aplica la directiva en el dispositivo MDM con iOS.

       - En el campo **Email address**, especifique la dirección de correo electrónico del usuario del dispositivo MDM con iOS. Puede ingresar un valor o seleccionar una macro haciendo clic en el botón +.

     - Ajustes de la sección **Authentication**:

       - En el campo **Password**, escriba la contraseña de la cuenta Exchange ActiveSync para la autorización en el servidor Microsoft Exchange.

       - En la lista desplegable **Authentication certificate**, seleccione el certificado utilizado para autenticar al usuario del dispositivo MDM con iOS en el servidor de Microsoft Exchange. Puede agregar certificados en la configuración **Certificate management** de la directiva o en la sección **Certificates** de Kaspersky Next Expert View (on-premise).

- En la pestaña **Additional**, configure las opciones adicionales de la cuenta de Exchange ActiveSync:

  - En la sección **Email synchronization**, en la lista desplegable **Synchronization period**, seleccione el intervalo de tiempo para el cual el correo electrónico se sincronizará y se almacenará automáticamente en el dispositivo MDM con iOS. Cuanto más largo sea el período de sincronización del correo electrónico, más espacio libre se requerirá en la memoria del dispositivo móvil. Los mensajes que no se sincronizaron no están disponibles sin conexión a Internet. El valor predeterminado es **1 week**.

  - En la sección **Restrictions**, seleccione o desmarque las siguientes casillas, si es necesario:

    - **Allow movement of messages between accounts (including work and personal accounts)**

      Mover mensajes de correo electrónico entre cuentas.

      Si se selecciona la casilla, el usuario puede mover mensajes de correo electrónico de una cuenta a otra.

      Si la casilla está desmarcada, el usuario no puede mover mensajes de correo electrónico de una cuenta a otra.

      Esta casilla está marcada por defecto.

      > Si desea prohibir guardar, mover y compartir archivos adjuntos desde un buzón de correo corporativo, desactive la casilla **Allow movement of messages between accounts (including work and personal accounts)** y seleccione la casilla Prohibit non-managed apps from using documents from managed apps y Prohibit managed apps from using documents from non-managed apps.

    - **Allow syncing recent addresses**

      Sincronización de direcciones de correo electrónico entre cuentas.

      Si la casilla está marcada, al crear mensajes, el usuario puede usar el historial de direcciones de otra cuenta de correo electrónico.

      Si la casilla está desactivada, las direcciones de correo electrónico usadas no se sincronizan. Al crear un mensaje, el usuario de un dispositivo con MDM de iOS no puede usar el historial de direcciones de otra cuenta de correo electrónico.

      Esta casilla está marcada por defecto.

    - **Allow using only the Mail app**

      Uso únicamente del cliente de correo estándar de iOS para procesar mensajes.

      Si se selecciona la casilla, el usuario solo podrá usar el correo electrónico en el cliente de correo electrónico estándar de iOS.

      Si la casilla no está marcada, el usuario puede usar el correo electrónico tanto en el cliente de correo estándar de iOS como en otras aplicaciones.

      Esta casilla está desactivada por defecto.

    - **Use SSL connection**

      Seleccione esta casilla para usar el protocolo de transporte de datos SSL (Secure Sockets Layer) para proteger la transmisión de datos.

      Esta casilla está marcada por defecto.

- En la sección **Signature and encryption**, configure los ajustes para firmar y cifrar el correo saliente mediante el protocolo S/MIME en la aplicación Correo. *S/MIME* es un protocolo para transmitir mensajes cifrados firmados digitalmente. S/MIME proporciona capacidades de la seguridad criptográficas tales como autentificación, control de integridad del mensaje y no rechazo del origen (usando firmas digitales). El protocolo también usa el cifrado para ayudar a mejorar el nivel de confidencialidad y seguridad de datos en mensajes de correo electrónico.

  - **Sign messages**

    Firma digital de mensajes salientes en la aplicación del Correo.

    Si se selecciona la casilla, los mensajes salientes se firman con una firma digital mediante el protocolo S/MIME. Una firma digital confirma la autenticidad del remitente e indica que los contenidos del mensaje no se han modificado durante la transmisión al destinatario. Se debe seleccionar un certificado de destinatario (clave pública) para la firma de mensajes.

    Esta casilla está desactivada por defecto.

  - **Signing certificate for outgoing messages**

    Certificado para firmar mensajes salientes con una firma digital utilizando el protocolo S/MIME. La firma digital garantiza que el mensaje lo envió el usuario del dispositivo MDM con iOS. Puede agregar certificados en la configuración **Certificate management** de la directiva o en la sección **Certificates** de Kaspersky Next Expert View (local).

    Esta lista desplegable está disponible solo si la casilla **Sign messages** está marcada.

  - **Encrypt messages by default**

    Codificación de mensajes salientes en la aplicación del Correo.

    Si la casilla está marcada, los mensajes salientes se cifran de manera predeterminada mediante el protocolo S/MIME. Deberá seleccionar un certificado de destinatario (clave pública) para enviar mensajes cifrados. Si no hay un certificado de destinatario instalado, los mensajes no se pueden cifrar. Los mensajes cifrados solo pueden ser vistos por usuarios cuyos dispositivos tengan un certificado instalado.

    Esta casilla está desactivada por defecto.

  - **Encryption certificate**

    Certificado de cifrado para cifrar los mensajes salientes mediante el protocolo S/MIME. El cifrado mantiene los mensajes confidenciales durante la transmisión y el almacenamiento. Puede agregar certificados en la configuración **Certificate management** de la directiva o en la sección **Certificates** de Kaspersky Next Expert View (on-premise).

    Esta lista desplegable está disponible solo si la casilla **Encrypt messages by default** está marcada.

  - **Show toggle button for encrypting selected messages**

    La visualización del icono en la aplicación del Correo en el campo **Para** para enviar mensajes cifrados.

    Si se selecciona esta casilla, el usuario del dispositivo móvil puede cifrar mensajes individuales al hacer clic en el ícono.

    Si la casilla se desactiva, el icono para cifrar mensajes no se muestra. En este caso, la casilla **Encrypt messages by default** determina si el correo saliente se cifra.

- Si es necesario, en la sección **Per App VPN**, configure Per App VPN.

8. Haga clic en **Agregar**.

La nueva cuenta de Exchange ActiveSync aparece en la lista.

Puede modificar o eliminar cuentas de Exchange ActiveSync en la lista con los botones **Edit** y **Delete** que se encuentran en la parte superior de la lista.

9. Haga clic en **Aceptar**.
10. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se cambia después de la siguiente sincronización del dispositivo con el Servidor de MDM para iOS.

Como resultado, luego de que se aplica la directiva, las cuentas de Exchange ActiveSync de la lista compilada se agregan al dispositivo móvil del usuario.

Configurar un buzón de correo de Exchange en dispositivos Android

Para trabajar con el calendario, el correo y los contactos corporativos en el dispositivo móvil, puede ajustar la configuración del buzón de correo de Exchange para la aplicación de correo electrónico estándar de Samsung.

Un buzón de correo de Exchange solo se puede configurar para dispositivos Samsung con Android 9 o versiones anteriores.

Para configurar un buzón de correo de Exchange en el dispositivo móvil de un usuario, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **Android** y vaya a la sección **Samsung Knox settings**.
4. En la tarjeta **Exchange ActiveSync**, haga clic en **Settings**.

   Se abre la ventana **Exchange ActiveSync**.
5. Habilite la configuración con el interruptor **Exchange ActiveSync**.
6. En el campo **Server address**, escriba la dirección IP o el nombre DNS del servidor que aloja al servidor de correo.
7. En el campo **Domain name**, escriba el nombre de dominio del usuario del dispositivo móvil en la red corporativa.
8. En la lista desplegable **Synchronization interval**, seleccione el intervalo que desee para la sincronización del dispositivo móvil con el servidor Microsoft Exchange.
9. Para usar el protocolo SSL (Secure Sockets Layer) de transporte de datos, seleccione la casilla **Use SSL connection**. El protocolo SSL utiliza cifrado y autenticación basada en certificados para la transferencia de datos segura. Esta casilla está marcada por defecto.

10. Para usar certificados digitales para proteger la transferencia de datos entre el dispositivo móvil y el servidor Microsoft Exchange, seleccione la casilla **Verify server certificate**. Se verifica que el certificado del servidor se haya emitido a partir del certificado raíz de confianza. Esta casilla está marcada por defecto.

11. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Configurar niveles de protección en Kaspersky Security Center

Esta configuración se aplica a los dispositivos Android.

Para configurar reglas para asignar niveles de protección en Kaspersky Security Center, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **Android** y vaya a la sección **KES for Android settings**.

4. En la tarjeta **Severity settings for device protection level**, haga clic en **Settings**.

   Se abre la ventana **Severity settings for device protection level**.

5. Habilite la configuración mediante el interruptor **Severity settings for device protection level**.

6. Seleccione el nivel de protección **OK**, **Warning** o **Critical** para cada una de las siguientes condiciones:

   - **Real-time protection is not running**

     La lista desplegable en la cual puede seleccionar el nivel de protección de un dispositivo móvil en el que la protección en tiempo real no se está ejecutando.

     La protección en tiempo real le permite detectar amenazas en los archivos que se abren, así como analizar aplicaciones nuevas y detener las infecciones del dispositivo en tiempo real.

     Es posible que la protección en tiempo no se ejecute por los siguientes motivos:

     - El usuario rechazó usar Kaspersky Security Network en el dispositivo móvil en la configuración del Antimalware de Kaspersky Endpoint Security para Android.

     - El usuario no otorgó acceso a la aplicación para administrar todos los archivos.

     Si la protección en tiempo real no se está ejecutando, también puede configurar restricciones en el funcionamiento del dispositivo móvil en la configuración **Compliance Control** de la directiva.

   - **Web Protection and Web Control are not running**

     Lista desplegable en la cual puede seleccionar el nivel de protección de un dispositivo móvil en el que Protección web y Control web no se están ejecutando.

     La Protección web le permite analizar sitios web y bloquear sitios web de phishing y maliciosos.

     Control web le permite configurar el acceso de los usuarios a sitios web específicos y categorías de sitios web.

Es posible que Protección web y Control web no se ejecuten por los siguientes motivos:

- El usuario desactivó la Protección web en el dispositivo móvil en la configuración de Kaspersky Endpoint Security para Android.
- El usuario no activó Kaspersky Endpoint Security para Android como una función de Accesibilidad.
- No se concedió el permiso Ignorar optimización de la batería.
- La Declaración de Protección web no fue aceptada.

Si Protección web y Control web no se están ejecutando, también puede configurar restricciones en el funcionamiento del dispositivo móvil en la configuración **Compliance Control** de la directiva.

- **App Control is not running**

  La lista desplegable en la cual puede seleccionar el nivel de protección de un dispositivo móvil en el que Control de aplicaciones no se está ejecutando.

  Control de aplicaciones le permite impedir que las aplicaciones se ejecuten en dispositivos móviles si esas aplicaciones no cumplen con los requisitos de la seguridad corporativa.

  Es posible que Control de aplicaciones no se ejecute si el usuario no activó la aplicación como una función de Accesibilidad en dispositivos con Android 5 o posterior.

  Si Control de aplicaciones no se está ejecutando, también puede configurar restricciones en el funcionamiento del dispositivo móvil en la configuración **Compliance Control** de la directiva.

- **Device lock is not available**

  La lista desplegable en la cual puede seleccionar el nivel de protección de un dispositivo móvil en el que el bloqueo del dispositivo no está disponible.

  El dispositivo se puede bloquear en los casos siguientes:

  - Se recibe el comando Antirrobo.
  - La tarjeta SIM se reemplaza o el dispositivo se enciende sin una tarjeta SIM.
  - Se realiza un intento de eliminar Kaspersky Endpoint Security para Android mientras la protección de eliminación de aplicaciones está activada.

  El bloqueo del dispositivo puede no estar disponible debido a los siguientes motivos:

  - El usuario no configuró la aplicación como administrador del dispositivo.
  - El usuario no activó la aplicación como una servicio de Accesibilidad en dispositivos con Android 7 o posterior.
  - El usuario no activó la aplicación para que se muestre sobre otras ventanas en dispositivos con Android 7 o posterior.

- **Device location is not available**

  Lista desplegable en la cual puede seleccionar el nivel de protección de un dispositivo móvil cuya ubicación no se puede determinar.

  La ubicación se establece después de recibir el comando **Locate device**.

  Es posible que la ubicación del dispositivo no esté disponible por los siguientes motivos:

  - El usuario no otorgó el permiso para localizar el dispositivo a la aplicación.
  - El usuario desactivó el módulo GPS en la configuración del dispositivo.

- **Versions of the Kaspersky Security Network Statement do not match**

  Lista desplegable en la cual puede seleccionar el nivel de protección de un dispositivo móvil si la versión de la declaración de Kaspersky Security Network aceptada por el administrador no coincide con la versión aceptada por el usuario del dispositivo. Las estadísticas que no figuran en la versión de la Declaración aceptada por el usuario no se envían a Kaspersky Security Network.

- **Versions of the Marketing Statement do not match**

  Lista desplegable en la cual puede seleccionar el nivel de protección de un dispositivo móvil si la versión de la Declaración sobre el procesamiento de datos con fines de marketing aceptada por el administrador no coincide con la versión aceptada por el usuario del dispositivo. Los datos no se transfieren a servicios de terceros.

  > La lista de servicios de terceros se puede encontrar en la Declaración respecto del procesamiento de datos para fines de marketing.

7. Haga clic en **Aceptar**.
8. Haga clic en el botón **Save** para guardar los cambios que realizó.

   La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Para obtener más información sobre los valores predeterminados, los motivos y las condiciones para asignar niveles de protección, consulte la sección Niveles de protección de dispositivos móviles.

Crear un informe sobre aplicaciones móviles instaladas

El **Report on installed mobile apps** le permite obtener información detallada sobre las aplicaciones instaladas en los dispositivos Android de los usuarios.

> Para permitir que el informe muestre información, la casilla **Send data on installed apps** debe estar seleccionada en la configuración **App Control** y el tipo de evento informativo **Se instaló o eliminó una aplicación (lista de aplicaciones instaladas)** debe almacenarse en la base de datos del Servidor de administración.

Para habilitar el envío de datos, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **Android** y vaya a la sección **Security controls**.
4. En la tarjeta **App Control**, haga clic en **Settings**.

   Se abre la ventana **App Control**.
5. En la sección **Report on installed apps**, seleccione la casilla **Send data on installed apps**.

6. Si desea recibir datos sobre las aplicaciones del sistema, seleccione la casilla **Send data on built-in apps**.
7. Si desea recibir datos sobre aplicaciones de servicio, que no tienen una interfaz y el usuario no puede abrirlas, seleccione la casilla **Send data on service apps**.
8. Haga clic en **Aceptar**.
9. Haga clic en el botón **Save** para guardar los cambios que realizó.
10. Haga clic en el nombre de la directiva y seleccione **Event configuration**.
11. Vaya a la sección **Info**.
12. Haga clic en el evento **Se instaló o eliminó una aplicación (lista de aplicaciones instaladas)** para abrir sus propiedades.
13. En la ventana de propiedades del evento, active el interruptor **Store in the Administration Server database for (days)** y configure el período de almacenamiento. De forma predeterminada, el período de almacenamiento es de 30 días.

    Una vez que caduca el período de almacenamiento, el Servidor de administración elimina la información desactualizada de la base de datos. Para obtener más información acerca de los eventos, consulte la Ayuda de Kaspersky Security Center.

    No es posible configurar el tiempo durante el cual se almacenan los eventos en el dispositivo móvil del usuario. El período de retención del registro de eventos en el dispositivo es ilimitado. Sin embargo, el tamaño es limitado: cuando el registro de eventos alcanza 200 entradas, las 50 más antiguas se eliminan automáticamente.

14. Haga clic en **Aceptar**.
15. Haga clic en el botón **Save** para guardar los cambios que realizó.

Se habilita el envío de datos.

Para configurar un informe sobre las aplicaciones móviles instaladas, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Monitoring → Reports**.
2. Haga clic en la plantilla de informe **Report on installed mobile apps** para abrir sus propiedades.
3. En la ventana que se abre, haga clic en **Edit**.
4. Modifique las propiedades de la plantilla de informe:
   - En la pestaña **General**, especifique los siguientes parámetros:
     - Nombre de la plantilla de informe
     - **Maximum number of entries to display**

       Si esta opción está habilitada, la tabla con los datos detallados del informe mostrará, como máximo, el número de entradas indicado aquí.

Las entradas del informe se ordenan primero siguiendo las reglas especificadas en la sección **Fields → Details fields** de las propiedades de la plantilla de informe, y luego se conservan solo las primeras de las entradas resultantes. El encabezado de la tabla con los datos detallados del informe indica el número de entradas mostradas y el total de entradas disponibles que coinciden con otros parámetros de la plantilla del informe.

Si deshabilita esta opción, se mostrarán todas las entradas disponibles en la tabla con los datos detallados del informe. No recomendamos deshabilitar esta opción. Al limitar el número de entradas que se muestran en un informe, se aminora la carga en el sistema de administración de bases de datos y se reduce el tiempo requerido para generar y exportar el informe. Algunos informes contienen un número excesivo de entradas. En tales casos, no es sencillo leer y analizar todas las entradas. Además, su dispositivo puede quedarse sin memoria al generar dicho informe. Por lo tanto, no podrá ver el informe.

Esta opción está activada de forma predeterminada. El valor predeterminado es 1000.

- **Group**

  El conjunto de dispositivos cliente para los que se crea el informe.

- **Include data from secondary and virtual Administration Servers**

  Cuando esta opción se encuentra habilitada, el informe incluye información de los servidores de administración secundarios y virtuales que están subordinados al Servidor de administración para el cual se ha creado la plantilla de informe.

  Deshabilite esta opción si solo desea ver datos del Servidor de administración con el que está trabajando.

  Esta opción está activada de forma predeterminada.

- **Up to nesting level**

  El informe incluye datos de los Servidores de administración secundarios y virtuales que se encuentran bajo el Servidor de administración actual en un nivel de anidamiento inferior o igual al valor especificado.

  El valor predeterminado es 1. Puede cambiar este valor si necesita obtener información de Servidores de administración secundarios que se encuentren aún más abajo en el árbol.

- **Data wait interval (min)**

  Antes de generar el informe, el Servidor de administración para el que se haya creado la plantilla de informe esperará, durante el tiempo especificado, a que los servidores de administración secundarios le envíen datos. Transcurrido este período de espera, el Servidor generará el informe aunque no haya recibido información de los servidores de administración secundarios. En ese caso, en lugar de los datos actualizados, el informe mostrará el valor **N/D** (no disponible) o, si la opción **Cache data from secondary Administration Servers** está habilitada, mostrará información tomada de la caché.

  El valor predeterminado es 5 (minutos).

- **Cache data from secondary Administration Servers**

  Los servidores de administración secundarios transfieren datos periódicamente al Servidor de administración para el que se ha creado la plantilla de informe. Los datos transferidos se almacenan en la caché de ese Servidor de administración.

  Si, al momento de generar un informe, el Servidor de administración no puede recibir datos de algún Servidor de administración secundario, el informe contendrá los datos de esta caché. La fecha en que los datos se transfirieron a la caché estará indicada en el informe.

  Si habilita esta opción, podrá ver información de los Servidores de administración secundarios incluso cuando no se pueda obtener información actualizada. Sin embargo, los datos mostrados podrían ser obsoletos.

  Esta opción está deshabilitada de forma predeterminada.

- **Transfer detailed information from secondary Administration Servers**

  En el informe generado, la tabla con los datos detallados del informe contendrá datos de los servidores de administración secundarios que estén subordinados al Servidor de administración para el cual se haya creado la plantilla de informe.

  Si habilita esta opción, los informes tardarán más tiempo en generarse y habrá más tráfico entre los Servidores de administración. Sin embargo, le permite ver toda la información en un solo informe.

  En lugar de habilitar esta opción, podría analizar los datos detallados de un informe para detectar un Servidor de administración secundario con problemas y, hecho esto, generar ese mismo informe únicamente para ese Servidor de administración.

  Esta opción está deshabilitada de forma predeterminada.

- En la pestaña **Fields**, seleccione los campos que se mostrarán en el informe y el orden de estos campos, y configure si cada uno de los campos debe clasificar y filtrar el informe.

5. Haga clic en el botón **Save** para guardar los cambios que realizó.

La plantilla de informe actualizada aparece en la lista de plantillas de informe.

Para crear y ver un informe sobre las aplicaciones móviles instaladas, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Monitoring → Reports**.
2. Haga clic en un informe con el tipo **Report on installed mobile apps**.

Se creará y mostrará un informe basado en la plantilla seleccionada.

Para obtener más información sobre el uso de informes, la administración de plantillas de informes personalizadas, el uso de plantillas de informes para generar nuevos informes y la creación de tareas de entrega de informes, consulte la Ayuda de Kaspersky Security Center.

Configuración de notificaciones de Kaspersky Endpoint Security para Android

Si no desea que el usuario del dispositivo móvil se distraiga con las notificaciones de Kaspersky Endpoint Security para Android, puede deshabilitar ciertas notificaciones.

Kaspersky Endpoint Security para Android utiliza las siguientes herramientas para mostrar el estado de protección del dispositivo:

- **Notificación del estado de protección**. Esta notificación está anclada a la barra de notificaciones. La notificación del estado de protección no se puede eliminar. La notificación muestra el estado de protección del dispositivo (por ejemplo,) y el número de problemas, si los hubiera. Puede presionar el estado de protección del dispositivo y ver los problemas de seguridad en la aplicación.
- **Notificaciones de la app**. Estas notificaciones informan al usuario del dispositivo sobre la aplicación (por ejemplo, detección de una amenaza).
- **Mensajes emergentes**. Los mensajes emergentes requieren una acción del usuario del dispositivo (por ejemplo, qué hacer cuando se detecta una amenaza).

Todas las notificaciones de Kaspersky Endpoint Security para Android están activadas de forma predeterminada.

En Android 13, el usuario del dispositivo debe conceder permiso para enviar notificaciones durante el Asistente de configuración inicial o más tarde.

El usuario puede deshabilitar todas las notificaciones de Kaspersky Endpoint Security para Android en la configuración de la barra de notificaciones. Si las notificaciones se deshabilitan, el usuario no controla el funcionamiento de la aplicación y puede perderse información importante (por ejemplo, información sobre fallas durante la sincronización del dispositivo con Kaspersky Security Center). En este caso, para averiguar el estado de funcionamiento de la aplicación, el usuario debe abrir Kaspersky Endpoint Security para Android.

Para configurar la visualización de notificaciones sobre el funcionamiento de Kaspersky Endpoint Security para Android, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **Android** y vaya a la sección **KES for Android settings**.
4. En la tarjeta **Configure notifications**, haga clic en **Settings**.

   Se abre la ventana **Configure notifications**.
5. Habilite la configuración con el interruptor **Configure notifications**.
6. Si desea ocultar todas las notificaciones y los mensajes emergentes, en la sección **Notifications from Kaspersky Endpoint Security**, seleccione la casilla **Disable notifications when Kaspersky Endpoint Security is in the background**.

   Kaspersky Endpoint Security para Android mostrará solo la notificación del estado de protección. La notificación muestra el estado de protección del dispositivo (por ejemplo,) y la cantidad de problemas.

   Las notificaciones dentro de la aplicación (por ejemplo, cuando el usuario actualiza las bases de datos antimalware manualmente) aún se mostrarán.

   Recomendamos habilitar las notificaciones y los mensajes emergentes. Si deshabilita las notificaciones y los mensajes emergentes cuando la aplicación se ejecuta en segundo plano, la aplicación no advertirá a los usuarios sobre las amenazas en tiempo real. En este caso, los usuarios de dispositivos móviles no verán el estado de protección del dispositivo a menos que abran la aplicación.
7. En la sección **Kaspersky Endpoint Security in-app notifications**, seleccione los problemas de Kaspersky Endpoint Security para Android que desea mostrar en el dispositivo móvil del usuario.

   De manera predeterminada, el usuario puede ignorar la notificación **Device has not been synchronized with the Administration Server for a long time**. Si desea tener más control sobre la frecuencia de sincronización, al configurar las reglas para verificar el cumplimiento de la directiva, seleccione el criterio **Device has not been synchronized for a long time** para llamar la atención del usuario sobre el problema.

Es obligatorio mostrar ciertos problemas de Kaspersky Endpoint Security para Android. Estos problemas siempre se muestran en el dispositivo (por ejemplo, problemas relacionados con la caducidad de la licencia).

8. Haga clic en **Aceptar**.

9. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center. Las notificaciones que deshabilite no se mostrarán en el dispositivo móvil del usuario.

Seleccionar el administrador de descargas para dispositivos Android

Si utiliza el Servidor web con un certificado autofirmado en lugar de uno firmado por una autoridad de certificación (CA), el administrador de descargas estándar de Android solo le permite descargar aplicaciones y paquetes de instalación de Kaspersky Endpoint Security para Android desde su Servidor web a los dispositivos a través de HTTP.

Para descargar de forma segura aplicaciones y paquetes de instalación desde un Servidor web con un certificado autofirmado a los dispositivos, puede utilizar el administrador de descargas integrado de Kaspersky Endpoint Security para Android que siempre utiliza el protocolo HTTPS.

El administrador de descargas integrado de Kaspersky Endpoint Security para Android está habilitado de manera predeterminada.

Para cambiar el administrador de descargas utilizado por Kaspersky Endpoint Security para Android, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **Android** y vaya a la sección **KES for Android settings**.

4. Realice una de las siguientes acciones:

   - Para usar el administrador de descargas de Kaspersky Endpoint Security para Android, active el interruptor **Built-in download manager**.

   - Para usar el administrador de descargas estándar de Android, desactive el interruptor **Built-in download manager**.

Se configura el administrador de descargas utilizado en los dispositivos.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Conexión de dispositivos iOS con MDM a AirPlay

Configure la conexión a dispositivos AirPlay para transmitir música, fotos y videos de dispositivos MDM con iOS a dispositivos AirPlay. Para poder utilizar la tecnología AirPlay, el dispositivo móvil y los dispositivos AirPlay deben estar conectados a la misma red inalámbrica. Los dispositivos AirPlay incluyen dispositivos Apple TV (segunda generación o posteriores), dispositivos AirPort Express, altavoces, televisores y radios compatibles con AirPlay.

La conexión automática a dispositivos AirPlay está disponible para dispositivos que funcionan en modo de control básico y para dispositivos supervisados.

Para configurar la conexión de un dispositivo iOS con MDM a dispositivos AirPlay:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **iOS** y vaya a la sección **Device configuration**.
4. En la tarjeta **AirPlay**, haga clic en **Settings**.

   Se abre la ventana **AirPlay**.
5. Habilite la configuración con el interruptor **AirPlay**.
6. En la sección **Passwords**, haga clic en **Add password**.
7. En el campo **Device**, escriba el nombre del dispositivo AirPlay en la red inalámbrica.
8. En la columna **Password**, escriba la contraseña del dispositivo AirPlay.
9. Si desea que los dispositivos MDM con iOS se conecten solo a dispositivos AirPlay específicos, cree una lista de dispositivos permitidos en la sección **Allowed devices**. Para hacerlo, haga clic en **Add device** y especifique las direcciones MAC de los dispositivos AirPlay.

   Para conectar dispositivos MDM con iOS 18 o versiones posteriores a cualquier dispositivo AirPlay, debe especificar el **Nombre del dispositivo**.

   Para conectar dispositivos MDM con iOS 17 o versiones anteriores a cualquier dispositivo AirPlay, debe especificar tanto la dirección Wi-Fi como la dirección Ethernet para cada dispositivo.

   Se bloquea el acceso a los dispositivos AirPlay que no están en la lista de dispositivos permitidos. Si la lista de dispositivos permitidos está vacía, Kaspersky Mobile Devices Protection and Management permite el acceso a todos los dispositivos AirPlay.
10. Haga clic en **Aceptar**.
11. Haga clic en el botón **Save** para guardar los cambios que realizó.

Como resultado, luego de que se aplica la directiva, el dispositivo móvil del usuario se conecta en forma automática a los dispositivos AirPlay para transmitir contenido multimedia.

Conexión de dispositivos iOS con MDM a AirPrint

Para habilitar la impresión de documentos de forma inalámbrica desde el dispositivo MDM con iOS mediante AirPrint, configure la conexión automática a las impresoras AirPrint. El dispositivo móvil y la impresora deben estar conectados a la misma red inalámbrica. El acceso compartido para todos los usuarios debe configurarse en la impresora de AirPrint.

Para configurar la conexión de un dispositivo iOS con MDM a una impresora AirPrint:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **iOS** y vaya a la sección **Device configuration**.
4. En la tarjeta **AirPrint**, haga clic en **Settings**.

   Se abre la ventana **AirPrint**.
5. Habilite la configuración con el interruptor **AirPrint**.
6. Haga clic en **Agregar**.

   Se abre la ventana **Add printer**.
7. En el campo **IP address or FQDN**, ingrese la dirección IP o el nombre de dominio completo (FQDN) de la impresora AirPrint.
8. En el campo **Port**, ingrese el puerto de escucha del destino de AirPrint.
9. En el campo **Resource path**, escriba la ruta a la impresora AirPrint.

   La ruta a la impresora corresponde a la clave "rp" (ruta de recurso) del protocolo Bonjour. Por ejemplo:

   - printers/Canon_MG5300_series
   - ipp/print
   - Epson_IPP_Printer
10. Si desea brindar proteger la conexión a la impresora AirPrint mediante el protocolo TLS, seleccione la casilla **Use TLS**.
11. Haga clic en **Agregar**.

    La impresora AirPrint recién agregada aparece en la lista.
12. Haga clic en **Aceptar**.
13. Haga clic en el botón **Save** para guardar los cambios que realizó.

Como resultado, luego de que se aplica la directiva, el usuario del dispositivo móvil puede imprimir en forma inalámbrica documentos en la impresora AirPrint.

Configuración del nombre de punto de acceso (APN)

En esta sección se proporcionan instrucciones sobre cómo conectar un dispositivo móvil a los servicios de datos móviles en una red móvil.

Configuración de APN en dispositivos Android (solo Samsung)

APN solo se puede configurar para dispositivos Samsung.

Debe insertar una tarjeta SIM para poder utilizar un punto de acceso en el dispositivo móvil del usuario. La operadora de telefonía móvil proporciona la configuración de punto de acceso. Si la configuración del punto de acceso es incorrecta, es posible que genere cargos adicionales de datos móviles.

Para configurar el nombre del punto de acceso (APN) del dispositivo móvil de un usuario, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **Android** y vaya a la sección **Samsung Knox settings**.
4. En la tarjeta **APN settings**, haga clic en **Settings**.

   Se abre la ventana **APN settings**.
5. Habilite la configuración con el interruptor **APN settings**.

   El interruptor de esta tarjeta no habilita ni deshabilita la funcionalidad correspondiente en los dispositivos. Habilitar el interruptor le permite utilizar configuraciones personalizadas. Deshabilitar el interruptor le permite usar la configuración predeterminada.
6. Especifique la siguiente configuración del punto de acceso para conectar al usuario al servicio de datos:
   - En la lista desplegable **APN type**, seleccione el tipo de punto de acceso (APN) para la transmisión de datos en una red móvil GPRS/3G/4G:
     - **Internet**. Conexión del dispositivo móvil del usuario a Internet.
     - **MMS**. Intercambio de mensajes multimedia MMS.
     - **Internet and MMS**. Conexión a Internet e intercambio de mensajes multimedia. Este es el valor predeterminado.
   - En el campo **APN name**, especifique el nombre del punto de acceso.

- En el campo **MCC**, ingrese el código de país de móvil (MCC).
- En el campo **MNC**, ingrese el código de operador de móvil (MNC).

7. Si seleccionó **MMS** o **Internet and MMS** como el tipo de punto de acceso, especifique las siguientes opciones adicionales del servidor de MMS en la sección **MMS server**:
   - En el campo **MMS server name**, especifique el nombre de dominio completo del servidor de la empresa de telefonía móvil que se utiliza para intercambiar MMS (por ejemplo, `mms.mobile.com`).
   - En el campo **MMS proxy server address**, especifique el nombre de la red o la dirección IP del servidor proxy.
   - En el campo **MMS proxy server port**, especifique el número de puerto del servidor de la empresa de telefonía móvil que se utiliza para intercambiar MMS.
8. En la sección **Authentication**, especifique la siguiente configuración de autenticación:
   - En la lista desplegable **Authentication type**, seleccione el tipo de autenticación del usuario del dispositivo móvil que se utiliza en el servidor de la empresa de telefonía móvil para acceder a la red. De forma predeterminada, no se requiere la autenticación del usuario. Están disponibles los siguientes tipos:
     - **None**. No se requiere autenticación de usuario para acceder a la red móvil.
     - **PAP** (Password Authentication Protocol). Un protocolo de autenticación que utiliza contraseñas como texto no cifrado.
     - **CHAP** (Challenge Handshake Authentication Protocol). Un protocolo de autenticación de solicitud-respuesta que utiliza hashing MD5 estándar para cifrar la respuesta.
     - **Concurrently**. Uso combinado de los protocolos CHAP y PAP.
   - En el campo **User name**, escriba el nombre usuario para la autorización en la red móvil.
   - En el campo **Password**, escriba la contraseña para la autorización del usuario en la red móvil.
9. En la sección **Network**, especifique la siguiente configuración de la red:
   - En el campo **Network name**, escriba el nombre de la red.
   - En el campo **Server address**, especifique el nombre de la red del servidor de la empresa de telefonía móvil a través del cual se accede a los servicios de transmisión de datos.
10. En la sección **Proxy server**, especifique la siguiente configuración del servidor proxy:
    - Seleccione la casilla **Use a proxy server** para habilitar el uso de un servidor proxy. Esta casilla está desactivada por defecto.
    - En el campo **Proxy server address**, especifique el nombre de la red o la dirección IP del servidor proxy de la empresa de telefonía móvil que se utiliza para acceder a la red. Este campo está disponible solo si la casilla **Use a proxy server** está marcada.
    - En el campo **Proxy server port**, especifique el número de puerto del servidor proxy de la empresa de telefonía móvil que se utiliza para acceder a la red. Este campo está disponible solo si la casilla **Use a proxy server** está marcada.

11. Haga clic en **Aceptar**.

12. Haga clic en el botón **Save** para guardar los cambios que realizó.

    La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Configuración de APN en dispositivos iOS con MDM

El nombre de punto de acceso (APN) debe configurarse para permitir el servicio de transmisión de información de la red móvil en el dispositivo iOS con MDM del usuario.

Para configurar el punto de acceso en el dispositivo iOS con MDM de un usuario:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **iOS** y vaya a la sección **Device configuration**.

4. En la tarjeta **APN settings**, haga clic en **Settings**.

   Se abre la ventana **APN settings**.

5. Habilite la configuración con el interruptor **APN settings**.

   El interruptor de esta tarjeta no habilita ni deshabilita la funcionalidad correspondiente en los dispositivos. Habilitar el interruptor le permite utilizar configuraciones personalizadas. Deshabilitar el interruptor le permite usar la configuración predeterminada.

6. En la lista desplegable **APN type**, seleccione el tipo de punto de acceso para la transferencia de datos en una red móvil GPRS/3G/4G:

   - **Built-in APN**. Configurar el APN (nombre del punto de acceso) para la transferencia de datos mediante un operador de red móvil que admite la operación con una SIM de Apple incorporada. Para obtener más información sobre dispositivos con tarjeta Apple SIM incorporada, visite Sitio web de soporte técnico de Apple.

   - **APN**. Configurar el Nombre de punto de acceso para la transferencia de datos mediante el operador de red móvil de la tarjeta SIM insertada.

   - **Built-in APN and APN**. Configurar los ajustes de comunicaciones celulares para transferencia de datos a través del operador de red móvil de la tarjeta SIM insertada y la SIM de Apple integrada. Para obtener más información sobre dispositivos con SIM de Apple integrada y una ranura de tarjeta SIM, visite el Sitio web de soporte técnico de Apple.

7. Si seleccionó **APN**, en la sección **APN**, haga clic en **Agregar**.

   Se abre la ventana **Add APN**.

8. Especifique la siguiente configuración:

    a. En el campo **APN name**, especifique el nombre del punto de acceso.

    b. En la lista desplegable **Authentication type**, seleccione el tipo de autenticación del usuario en el servidor de la empresa de telefonía móvil que se utiliza para acceder a la red (Internet y MMS).

    c. En el campo **User name**, escriba el nombre usuario para la autorización en la red móvil.

    d. En el campo **Password**, escriba la contraseña para la autorización del usuario en la red móvil.

    e. En el campo **Proxy server address**, ingrese el nombre del host o la dirección IP del servidor proxy.

    f. En el campo **Proxy server port**, ingrese el número del puerto del servidor proxy.

    g. En la lista desplegable **Allowed protocol**, seleccione el protocolo de Internet.

    h. En la lista desplegable **Allowed protocol for roaming**, seleccione el protocolo de Internet que se utilizará durante el roaming internacional.

    i. En la lista desplegable **Allowed protocol for domestic roaming**, seleccione el protocolo de Internet que se utilizará durante el roaming nacional.

    j. Si desea que los dispositivos de las redes solo IPv6 puedan acceder a servicios de Internet solo IPv4, seleccione la casilla **Use the 464XLAT technology**.

    k. Haga clic en **Aceptar**.

9. Si seleccionó **Built-in APN**, configure los siguientes ajustes:

    a. En el campo **Built-in APN name**, especifique el nombre del punto de acceso.

    b. En la lista desplegable **Authentication type**, seleccione el tipo de autenticación del usuario en el servidor de la empresa de telefonía móvil que se utiliza para acceder a la red (Internet y MMS).

    c. En el campo **User name**, escriba el nombre usuario para la autorización en la red móvil.

    d. En el campo **Password**, escriba la contraseña para la autorización del usuario en la red móvil.

    e. En la lista desplegable **Allowed protocol**, seleccione el protocolo de Internet.

10. Haga clic en **Aceptar**.

11. Haga clic en el botón **Save** para guardar los cambios que realizó.

Como resultado, el nombre de punto de acceso (APN) se configura en el dispositivo móvil del usuario después de que se aplica la directiva.

Contenedor corporativo

Esta sección contiene información sobre el funcionamiento con contenedores corporativos.

Acerca de los contenedores corporativos

Android Enterprise es una plataforma para administrar la infraestructura móvil corporativa y proporciona a los empleados de empresas un entorno de trabajo seguro en el que pueden utilizar dispositivos móviles. Para obtener información sobre el uso de Android Enterprise, consulte el sitio web de soporte de Google.

Puede crear un contenedor corporativo que use un perfil de trabajo de Android en el dispositivo móvil personal de un usuario. Un contenedor corporativo es un entorno seguro en el que el administrador puede administrar aplicaciones y cuentas de usuario sin restringir el uso de sus propios datos por parte del usuario. Cuando se crea un contenedor corporativo en el dispositivo móvil del usuario, se instalan automáticamente las siguientes aplicaciones corporativas: Google Play Market, Google Chrome, Descargas, Kaspersky Endpoint Security para Android, entre otras. Las aplicaciones instaladas en el contenedor corporativo, así como las notificaciones de estas aplicaciones, están marcadas con un ícono de maletín. Debe crear una cuenta corporativa de Google separada para la aplicación Google Play. Las aplicaciones instaladas en contenedor corporativo aparecen en la lista común de aplicaciones.

Configurar un contenedor corporativo

Para configurar los ajustes de un contenedor corporativo, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **Android** y vaya a la sección **Contenedor corporativo**.
4. En la tarjeta **Corporate container on devices**, haga clic en **Settings**.

   Se abre la ventana **Corporate container on devices**.
5. Habilite la configuración mediante el interruptor **Corporate container on devices**.
6. Especifique la configuración del contenedor corporativo:
   - En la pestaña **General**, puede especificar la configuración para compartir datos, contactos y más.
     - Ajustes de la sección **Data access and sharing**:
       - **Prohibit personal apps from sharing data with corporate container apps**

         Restringe el uso compartido de archivos, imágenes u otros datos de aplicaciones personales con aplicaciones de contenedor corporativo.

         Si la casilla está marcada, las aplicaciones personales no pueden compartir datos con las aplicaciones de contenedor corporativo.

         Si la casilla no está marcada, las aplicaciones personales pueden compartir datos con las aplicaciones de contenedor corporativo.

         Esta casilla está marcada por defecto.

       - **Prohibit corporate container apps from sharing data with personal apps**

Restringe el uso compartido de archivos, imágenes u otros datos de aplicaciones de contenedor corporativo con aplicaciones personales.

Si la casilla está marcada, las aplicaciones del contenedor corporativo no pueden compartir datos con aplicaciones personales.

Si la casilla no está marcada, las aplicaciones del contenedor corporativo pueden compartir datos con aplicaciones personales.

Esta casilla está marcada por defecto.

- **Prohibit corporate container apps from accessing personal files**

  Restringe el acceso de las aplicaciones de contenedor corporativo a los archivos personales.

  Si la casilla está marcada, el usuario no puede acceder a los archivos personales cuando usa aplicaciones de contenedor corporativo.

  Si la casilla no está marcada, el usuario puede acceder a los archivos personales cuando utiliza aplicaciones de contenedor corporativo. Tenga en cuenta que las aplicaciones que se están utilizando deben admitir el acceso.

  Esta casilla está marcada por defecto.

- **Prohibit personal apps from accessing files in corporate container**

  Restringe el acceso de las aplicaciones personales a los archivos del contenedor corporativo.

  Si la casilla está marcada, el usuario no puede acceder a los archivos del contenedor corporativo cuando usa aplicaciones personales.

  Si la casilla no está marcada, el usuario puede acceder a los archivos del contenedor corporativo cuando utiliza aplicaciones personales. Tenga en cuenta que las aplicaciones que se están utilizando también deben admitir el acceso.

  Esta casilla está marcada por defecto.

- **Prohibit use of clipboard between personal apps and corporate container**

  Seleccione o desmarque esta casilla para especificar si el usuario del dispositivo puede copiar datos a través del portapapeles entre las aplicaciones personales y el contenedor corporativo.

  Esta casilla está marcada por defecto.

- **Prohibit activation of USB debugging**

  Restringe el uso de depuración de USB en el dispositivo móvil del usuario en el contenedor corporativo. En el modo de depuración de USB, el usuario puede descargar una aplicación mediante una estación de trabajo, por ejemplo.

  Si la casilla está marcada, el modo de depuración de USB no está disponible para el usuario. El usuario no puede configurar el dispositivo móvil mediante USB después de conectar el dispositivo a una estación de trabajo.

  Si se desactiva la casilla, el usuario puede activar el modo de depuración de USB, conectar el dispositivo móvil a una estación de trabajo mediante USB y configurar el dispositivo.

  Esta casilla está marcada por defecto.

- **Prohibit users from adding and removing accounts in corporate container**

  Si la casilla está marcada, el usuario tiene prohibido agregar y eliminar cuentas en el contenedor corporativo a través de la configuración o las aplicaciones de Google. Esto incluye restringir la capacidad de iniciar sesión en las aplicaciones de Google por primera vez. Sin embargo, el usuario puede iniciar sesión, agregar y eliminar cuentas a través de otras aplicaciones de terceros en el contenedor corporativo.

Las cuentas que se agregaron antes de que se estableciera la restricción no se eliminarán y el inicio de sesión en estas cuentas no está restringido.

Esta casilla está marcada por defecto.

- **Prohibit screen sharing, recording, and screenshots in corporate container apps**

  Seleccione o desmarque esta casilla para especificar si el usuario del dispositivo puede tomar capturas de pantalla, grabar y compartir la pantalla del dispositivo en las aplicaciones de contenedor corporativo. También especifica si se permite capturar el contenido de la pantalla del dispositivo con fines de inteligencia artificial.

  Esta casilla está marcada por defecto.

- Ajustes de la sección **File sharing**:

  - **Copy shared files to user's personal space**

    Seleccione o desmarque esta casilla para especificar si los archivos enviados al dispositivo con del usuario con un contenedor corporativo se copian en el espacio personal del usuario en el dispositivo.

    Esta casilla se aplica solo a los archivos que aún no se enviaron al dispositivo. Los archivos que se enviaron al dispositivo antes de que se seleccionara la casilla no se copian en el espacio personal del usuario.

    Esta casilla está desactivada por defecto.

- Ajustes de la sección **Contacts**:

  - **Prohibit showing contact name from corporate container for incoming personal calls**

    Seleccione o desmarque esta casilla para especificar si se mostrará un nombre de contacto del contenedor corporativo para las llamadas entrantes personales.

    Esta casilla está marcada por defecto.

  - **Prohibit personal apps from accessing corporate container contacts**

    Seleccione o desmarque esta casilla para especificar si las aplicaciones de administración de contactos personales pueden acceder a los contactos del contenedor corporativo.

    Esta casilla está marcada por defecto.

- En la pestaña **Apps**, puede configurar los siguientes ajustes:

  - Ajustes de la sección **General**:

    - **Enable App Control in corporate container only**

      Controla el inicio de aplicaciones en el contenedor corporativo del dispositivo móvil del usuario. Puede crear listas de aplicaciones permitidas, prohibidas y recomendadas, así como categorías de aplicaciones permitidas y prohibidas en la sección **App Control**.

      Si se selecciona esta casilla, según la configuración de Control de apps, Kaspersky Endpoint Security bloquea o permite el inicio de aplicaciones solo en el contenedor corporativo. Además, Control de aplicaciones no funciona en el espacio personal del usuario.

      Esta casilla está marcada por defecto.

    - **Enable Web Protection and Web Control in corporate container only**

      Restringe el acceso de usuarios a sitios web en el contenedor corporativo del dispositivo. Puede especificar la configuración de acceso al sitio web en la configuración **Web Control**.

Si esta casilla está marcada, Protección web y Control web bloquean o permiten el acceso a sitios web solo en el contenedor corporativo. Además, Protección web y Control web no funcionan en el espacio personal del usuario.

Si esta casilla no está marcada, según la configuración de Protección web y Control web, Kaspersky Endpoint Security bloquea o permite el acceso a sitios web en el espacio personal del usuario y el contenedor corporativo.

Esta casilla está marcada por defecto.

- **Prohibit installation of apps from unknown sources in corporate container**

  Restringe la instalación de aplicaciones en contenedor corporativo de orígenes que no son Google Play Enterprise.

  Si la casilla está marcada, el usuario puede instalar aplicaciones solo desde Google Play. Los usuarios utilizan sus propias cuentas corporativas para instalar aplicaciones.

  Si se desactiva la casilla, el usuario puede instalar aplicaciones de cualquier manera disponible. Solo las aplicaciones prohibidas en la configuración **App Control** no se pueden instalar.

  Esta casilla está desactivada por defecto.

- **Prohibit removing apps from corporate container**

  Seleccione o desmarque esta casilla para especificar si el usuario tiene prohibido eliminar aplicaciones del contenedor corporativo.

  Esta casilla está desactivada por defecto.

- **Prohibit displaying notifications from corporate container apps when screen is locked**

  Restringe la visualización del contenido de las notificaciones de aplicaciones de contenedor corporativo en la pantalla de bloqueo del dispositivo.

  Si la casilla está marcada, el contenido de las notificaciones de aplicaciones con contenedor corporativo no se puede ver en la pantalla de bloqueo del dispositivo. Para ver estas notificaciones, el usuario debe desbloquear el dispositivo o el contenedor corporativo.

  Si la casilla no está marcada, las notificaciones de aplicaciones de contenedor corporativo se muestran en la pantalla de bloqueo del dispositivo.

  Esta casilla está marcada por defecto.

- **Prohibit use of camera for corporate container apps**

  Seleccione o desmarque esta casilla para especificar si las aplicaciones de contenedor corporativo pueden acceder a la cámara del dispositivo.

  Esta casilla está marcada por defecto.

- En la sección **Granting runtime permissions for corporate container apps** puede seleccionar una acción que se realizará cuando las aplicaciones de contenedor corporativo se estén ejecutando y solicitar permisos adicionales. Esto no se aplica a los permisos otorgados en la configuración del dispositivo (por ejemplo, Acceder a todos los archivos).

  - **Allow users to configure permissions**

    Cuando se solicita un permiso, el usuario decide si otorga el permiso especificado a la aplicación.

    Esta opción se selecciona de forma predeterminada.

  - **Grant permissions automatically**

A todas las aplicaciones de contenedor corporativo se les otorgan permisos sin interacción del usuario.

En Android 12 o posterior, los siguientes permisos no se pueden otorgar automáticamente, pero se pueden denegar automáticamente. Si selecciona esta opción, la aplicación le pedirá al usuario estos permisos:

- Permisos de ubicación
- Permisos para la cámara
- Permiso para grabar audio
- Permiso para reconocimiento de actividad
- Permisos para monitorear mensajes SMS y MMS entrantes
- Permiso para acceder a los datos de los sensores corporales

- **Deny permissions automatically**

  A todas las aplicaciones de contenedor corporativo se les niegan los permisos sin la interacción del usuario.

  Los usuarios pueden ajustar los permisos de la aplicación en la configuración del dispositivo antes de que estos permisos se denieguen automáticamente.

- En la sección **Adding widgets of corporate container apps to device home screen** puede elegir si el usuario del dispositivo puede agregar widgets de aplicaciones de contenedor corporativo a la pantalla de inicio del dispositivo.

  - **Prohibit for all apps**

    El usuario del dispositivo tiene prohibido agregar widgets de aplicaciones instaladas en el contenedor corporativo.

    Esta opción se selecciona de forma predeterminada.

  - **Allow for all apps**

    El usuario del dispositivo puede agregar widgets de todas las aplicaciones instaladas en el contenedor corporativo.

  - **Allow only for the listed apps**

    El usuario del dispositivo puede agregar widgets de las aplicaciones enumeradas instaladas en el contenedor corporativo.

    Para agregar una aplicación a la lista, haga clic en **Agregar** e ingrese el nombre del paquete de la aplicación.

    Cómo obtener el nombre del paquete de una aplicación

    Para obtener el nombre de un paquete de aplicación:

    1. Abrir Google Play.
    2. Busque la aplicación y abra su página.

       La URL de la aplicación termina con el nombre de su paquete (por ejemplo, https://play.google.com/store/apps/details?id= **com.android.chrome**).

Para obtener el nombre de un paquete de aplicaciones que se agregó a Kaspersky Security Center, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management → Mobile → Apps & files**.

2. Seleccione **Android → Apps**.

   En la lista de aplicaciones que se abre, los identificadores de aplicaciones se muestran en la columna **Package name**.

- En la pestaña **Certificates**, puede configurar los siguientes ajustes:

  - **Duplicate installation of VPN certificates in user's personal space**

    Seleccione o desmarque la casilla para especificar si el certificado de VPN agregado en la sección **Mobile → Certificates** de Kaspersky Next Expert View (on-premise) e instalado en el contenedor corporativo también se instalará en el espacio personal del usuario.

    De manera predeterminada, los certificados VPN recibidos de Kaspersky Security Center se instalan en el contenedor corporativo. Esta configuración se aplica cuando se emite un nuevo certificado VPN.

    Esta casilla está desactivada por defecto.

  - **Duplicate installation of root certificates in user's personal space**

    Seleccione o desmarque la casilla para especificar si los certificados raíz agregados en la configuración **Root certificates** e instalados en el contenedor corporativo también se instalarán en el espacio personal del usuario.

    Esta casilla está desactivada por defecto.

- En la pestaña **Password**, especifique la configuración de la contraseña del contenedor corporativo:

  - **Require setting a password for corporate container**

    Le permite especificar los requisitos para la contraseña del contenedor corporativo de acuerdo con los requisitos de seguridad de la empresa.

    Si la casilla está marcada, los requisitos de contraseña están disponibles para la configuración. Cuando se aplica la directiva, el usuario recibe una notificación en la que se le solicita que configure una contraseña de contenedor corporativo de acuerdo con los requisitos de la empresa.

    Si la casilla no está marcada, no se puede editar la configuración de la contraseña.

    Esta casilla está desactivada por defecto.

  - **Minimum password length**

    La cantidad mínima de caracteres en la contraseña del usuario. Valores posibles: 4 a 16 caracteres.

    De manera predeterminada, la contraseña del usuario tiene 4 caracteres.

    Lo siguiente se aplica solo al espacio personal del usuario y al contenedor corporativo:

    - En el espacio personal del usuario, Kaspersky Endpoint Security convierte los requisitos de seguridad de la contraseña en uno de los valores disponibles en el sistema: medio o alto en dispositivos con Android 10 o posterior.

    - En el contenedor corporativo, Kaspersky Endpoint Security convierte los requisitos de seguridad de la contraseña en uno de los valores disponibles en el sistema: medio o alto en dispositivos con Android 12 o posterior.

Los valores se determinan mediante las siguientes reglas:

- Si la extensión de la contraseña requerida es de 1 a 4 caracteres, la app solicitará que el usuario establezca una contraseña con seguridad media. Debe ser o numérica (PIN) con una secuencia que no tenga números repetidos u ordenados en secuencias (por ejemplo, 1234), o alfabética/alfanumérica. El PIN o la contraseña debe tener al menos 4 caracteres.

- Si la extensión de la contraseña requerida es de 5 caracteres o más, la app solicitará que el usuario establezca una contraseña con seguridad alta. Debe ser o numérica (PIN) con una secuencia que no tenga números repetidos u ordenados, o alfabética/alfanumérica (contraseña). Un PIN debe tener al menos 8 dígitos. La contraseña debe tener al menos 6 caracteres.

- **Minimum password complexity requirements**

  Especifica los requisitos mínimos de la contraseña de desbloqueo. Estos requisitos se aplican solo a las nuevas contraseñas de usuario. Están disponibles los siguientes valores:

  - **Numeric**

    El usuario puede establecer una contraseña que incluya números o establecer una contraseña más segura (por ejemplo, una contraseña alfabética o alfanumérica).

    Esta opción se selecciona de forma predeterminada.

  - **Alphabetic**

    El usuario puede establecer una contraseña que incluya letras (u otros símbolos que no sean números) o establecer una contraseña más segura (por ejemplo, una contraseña alfanumérica).

  - **Alphanumeric**

    El usuario puede establecer una contraseña que incluya tanto números como letras (u otros símbolos que no sean números) o establecer una contraseña compleja más segura.

  - **No requirements**

    El usuario puede establecer cualquier contraseña.

  - **Complex**

    El usuario debe establecer una contraseña compleja de acuerdo con las propiedades de contraseña especificadas:

    - **Minimum number of letters**
    - **Minimum number of digits**
    - **Minimum number of special characters (for example, !@#$%)**
    - **Minimum number of uppercase letters**
    - **Minimum number of lowercase letters**
    - **Minimum number of non-alphabetic characters (for example, 1^*9)**

  - **Complex numeric**

    El usuario puede establecer una contraseña que incluya números sin repeticiones (por ejemplo, 4444) ni secuencias ordenadas (por ejemplo, 1234, 4321, 2468) o establecer una contraseña compleja más segura.

- **Maximum number of failed password attempts before corporate container is deleted**

  Especifica el número máximo de intentos que tiene el usuario para ingresar la contraseña para desbloquear el contenedor corporativo. Cuando se aplica la directiva, el contenedor corporativo se elimina del dispositivo cuando se excede el número máximo de intentos fallidos.

  Los valores posibles son de 4 a 16.

  No se establece un valor predeterminado. Esto significa que los intentos no son limitados.

- **Maximum password lifetime (days)**

  Especifica la cantidad de días antes de que caduque la contraseña. La aplicación de un nuevo valor establecerá la duración de la contraseña actual al nuevo valor.

  El valor predeterminado es 0. Esto significa que la contraseña no caducará.

- **Number of days to send a notification before a required password change**

  Especifica la cantidad de días para notificar al usuario antes de que caduque la contraseña.

  El valor predeterminado es 0. Esto significa que no se notificará al usuario sobre la caducidad de la contraseña.

- **Number of recent passwords that cannot be set as a new password**

  Especifica el número máximo de contraseñas de usuario anteriores que no se pueden usar como una nueva contraseña. Esta configuración se aplica solo cuando el usuario establece una nueva contraseña en el dispositivo.

  El valor predeterminado es 0. Esto significa que la nueva contraseña de usuario puede coincidir con cualquier contraseña anterior, excepto la actual.

- **Period of inactivity before corporate container is locked (sec)**

  Especifica el período de inactividad antes de que el dispositivo se bloquee.

  El valor predeterminado es 0. Esto significa que el dispositivo no se bloqueará después de un período determinado.

- **Period after biometric unlock before password must be entered (min)**

  Especifica el período para desbloquear el dispositivo sin contraseña. Durante este período, el usuario puede usar métodos biométricos para desbloquear la pantalla. Después de este período, el usuario puede desbloquear la pantalla solo con una contraseña.

  El valor predeterminado es 0. Esto significa que el usuario no se verá obligado a desbloquear el dispositivo con una contraseña después de un período determinado.

- **Allow biometric unlock methods**

  Si la casilla está marcada, se autoriza el uso de métodos de desbloqueo biométricos en el dispositivo móvil.

  Si la casilla está desactivada, Kaspersky Endpoint Security para Android bloquea el uso de métodos biométricos para desbloquear la pantalla. El usuario puede desbloquear la pantalla solo con una contraseña.

  Esta casilla está marcada por defecto.

- **Allow fingerprint unlock**

  Especifica si se pueden usar huellas digitales para desbloquear la pantalla.

  > Esta casilla no restringe el uso de un escáner de huellas digitales al iniciar sesión en apps o confirmar compras.

  Si se selecciona la casilla, se permite el uso de huellas digitales en el dispositivo móvil.

  Si la casilla está desmarcada, Kaspersky Endpoint Security para Android bloquea el uso de huellas digitales para desbloquear la pantalla. El usuario puede desbloquear la pantalla solo con una contraseña. En la configuración del dispositivo, la opción de usar huellas digitales no estará disponible.

  Esta casilla solo está disponible si la casilla **Allow biometric unlock methods** está marcada.

  Esta casilla está marcada por defecto.

  > En algunos dispositivos Xiaomi con un contenedor corporativo, el contenedor corporativo puede desbloquearse mediante una huella digital solo si establece el valor **Period of inactivity before corporate container is locked (sec)** después de establecer una huella digital como el método de desbloqueo de pantalla.

- **Allow face unlock**

  Si la casilla está marcada, se autoriza el uso de reconocimiento facial en el dispositivo móvil.

  Si la casilla está desactivada, Kaspersky Endpoint Security para Android bloquea el uso de reconocimiento facial para desbloquear la pantalla.

  Esta casilla solo está disponible si la casilla **Allow biometric unlock methods** está marcada.

  Esta casilla está marcada por defecto.

- **Allow iris scanning**

  Si la casilla está marcada, se autoriza el uso de reconocimiento de iris en el dispositivo móvil.

  Si la casilla está desactivada, Kaspersky Endpoint Security para Android bloquea el uso de reconocimiento de iris para desbloquear la pantalla.

  Esta casilla solo está disponible si la casilla **Allow biometric unlock methods** está marcada.

  Esta casilla está marcada por defecto.

- En la pestaña **Passcode**, especifique la configuración del código de acceso único. Se le pedirá al usuario que ingrese el código de acceso único para desbloquear su contenedor corporativo si está bloqueado.

  - **Passcode length**

    El número de dígitos del código de acceso. Valores posibles: 4, 8, 12 o 16 caracteres.

    De manera predeterminada, la longitud del código de acceso es de 4 caracteres.

7. Haga clic en **Aceptar**.

8. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center. El dispositivo móvil del usuario se divide en un contenedor corporativo y un espacio personal.

Desbloquear el contenedor corporativo

El contenedor corporativo se puede bloquear si el dispositivo no cumple con los requisitos de seguridad del Control de cumplimiento.

Para desbloquear el contenedor corporativo, el usuario del dispositivo móvil debe ingresar un código de acceso único del contenedor corporativo en la pantalla bloqueada. El código de acceso lo genera Kaspersky Security Center y es único para cada dispositivo móvil. Cuando se desbloquea el contenedor corporativo, la contraseña del contenedor corporativo se establece en el valor predeterminado (1234).

Como administrador, puede ver el código de acceso en la configuración de la directiva que se aplica al dispositivo móvil. La longitud del código de acceso se puede cambiar (4, 8, 12 o 16 dígitos) en la configuración **Corporate container on devices** de la directiva.

Para desbloquear un contenedor corporativo con un código de acceso único, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.
2. Haga clic en el dispositivo móvil para el cual desea recibir un código de acceso único.
3. Seleccione **Applications** → **Kaspersky Mobile Devices Protection and Management**.

   Se abre la ventana de propiedades de Kaspersky Mobile Devices Protection and Management.
4. Seleccione la pestaña **Application settings**.

   Se muestra un código de acceso único para el dispositivo seleccionado en el campo **One-time code** de la sección **One-time corporate container passcode**.
5. Use cualquier método disponible (por ejemplo, correo electrónico) para comunicar el código de acceso único al usuario.

   Luego, el usuario debe ingresar el código de acceso único recibido en su dispositivo.

Se desbloquea el contenedor corporativo del dispositivo móvil del usuario.

Una vez que se bloquea el contenedor corporativo en un dispositivo, se borra su historial de contraseñas. Esto significa que el usuario puede especificar una contraseña reciente, independientemente de la configuración de la contraseña del contenedor corporativo.

Agregar una cuenta LDAP

Esta configuración se aplica a los dispositivos supervisados y a los dispositivos que funcionan en el modo de control básico.

Para permitir al usuario del dispositivo MDM con iOS acceder a contactos corporativos en el servidor LDAP, agregue una cuenta LDAP.

Para agregar una cuenta LDAP del usuario del dispositivo MDM con iOS, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **iOS** y vaya a la sección **Device configuration**.

4. En la tarjeta **LDAP**, haga clic en **Settings**.

   Se abre la ventana **LDAP**.

5. Habilite la configuración con el interruptor **LDAP**.

6. Haga clic en **Add**.

   Se abre la ventana **Add LDAP account**.

7. En la pestaña **General**, especifique las siguientes opciones de LDAP:

   - En la sección **Server**, especifique la configuración del servidor:

     - En el campo **Description**, escriba una descripción de la cuenta LDAP del usuario. Puede ingresar un valor o seleccionar una macro haciendo clic en el botón +.

     - En el campo **Server address**, escriba el nombre de dominio del servidor LDAP.

   - En la sección **Authentication**, especifique las credenciales del usuario:

     - En el campo **Account name**, escriba el nombre de la cuenta para la autorización en el servidor LDAP. Puede ingresar un valor o seleccionar una macro haciendo clic en el botón +.

     - En el campo **Password**, escriba la contraseña de la cuenta LDAP para la autorización en el servidor LDAP.

     - Para usar el protocolo SSL (Secure Sockets Layer) de transporte de datos para proteger la transmisión de mensajes, active la casilla **Use SSL connection**.

   - Si es necesario, en la sección **Per App VPN**, configure Per App VPN.

8. En la pestaña **Search**, compile una lista de búsquedas del usuario del dispositivo MDM con iOS para acceder a información corporativa del servidor LDAP:

   a. Haga clic en el botón **Add setting** para agregar un bloque de la configuración de búsqueda.

   b. En la columna **Name**, escriba el nombre de una búsqueda.

c. En la lista desplegable **Search scope**, seleccione el nivel de anidamiento de la carpeta para la búsqueda de datos corporativos en el servidor LDAP:

- **Root folder of the LDAP server**. Búsqueda en la carpeta base del servidor LDAP.
- **First level subfolders**. Búsqueda en las carpetas del primer nivel de anidamiento contando desde la carpeta base.
- **All subfolders**. Búsqueda en las carpetas en todos los niveles de anidamiento contando desde la carpeta base.

d. En la columna **Search base**, escriba la ruta a la carpeta en el servidor LDAP con la cual comienza la búsqueda (por ejemplo: "ou=persona", "o=ejemplo corp").

e. Repita los pasos a-d para todas las búsquedas que desee añadir al dispositivo iOS con MDM.

9. Haga clic en **Agregar**.

La nueva cuenta LDAP aparece en la lista.

Puede modificar o eliminar cuentas LDAP en la lista con los botones **Edit** y **Delete** que se encuentran en la parte superior de la lista.

10. Haga clic en **Aceptar**.

11. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se cambia después de la siguiente sincronización del dispositivo con el Servidor de MDM para iOS.

Como resultado, luego de que se aplica la directiva, las cuentas LDAP de la lista compilada se agregan al dispositivo móvil del usuario. El usuario puede acceder a los contactos corporativos en las aplicaciones estándar iOS: Contactos, Mensajes y Correspondencia.

Agregar una cuenta de contactos

Esta configuración se aplica a los dispositivos supervisados y a los dispositivos que funcionan en el modo de control básico.

Para permitir al usuario del dispositivo MDM con iOS sincronizar información con el servidor CardDAV, agregue una cuenta CardDAV. La sincronización con el servidor CardDAV permite al usuario acceder a los detalles de contacto desde cualquier dispositivo.

Para agregar una cuenta CardDAV del usuario del dispositivo MDM con iOS, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **iOS** y vaya a la sección **Device configuration**.

4. En la tarjeta **Contacts**, haga clic en **Settings**.

   Se abre la ventana **Contacts**.

5. Habilite la configuración con el interruptor **Contacts**.

6. Haga clic en **Add**.

   Se abre la ventana **Add CardDAV account**.

7. En la sección **Server**, en el campo **Description**, ingrese una descripción de la cuenta CardDAV del usuario.

8. En los campos **Server address** y **Server port**, escriba el nombre de host o la dirección IP del servidor CardDAV y el número de puerto del servidor CardDAV.

9. En el campo **Contact URL**, especifique la URL de la cuenta CardDAV del usuario del dispositivo MDM con iOS en el servidor CardDAV (por ejemplo: `http://example.com/carddav/users/mycompany/user`).

   La URL debe empezar por `http://` o `https://`.

10. En la sección **Authentication**, en el campo **Account name**, escriba el nombre de la cuenta para la autorización en el servidor CardDAV.

11. En el campo **Password**, ingrese la contraseña de la cuenta de CardDAV para la autorización en el servidor CardDAV.

12. Si desea usar el protocolo de transporte de datos SSL (Secure Sockets Layer) para proteger la transmisión de datos entre el servidor CardDAV y el dispositivo móvil, seleccione la casilla la casilla **Use SSL connection**.

13. Si es necesario, en la sección **Per App VPN**, configure Per App VPN.

14. Haga clic en **Agregar**.

    La nueva cuenta CardDAV aparece en la lista.

    > Puede modificar o eliminar cuentas CardDAV en la lista con los botones **Edit** y **Delete** que se encuentran en la parte superior de la lista.

15. Haga clic en **Aceptar**.

16. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se cambia después de la siguiente sincronización del dispositivo con el Servidor de MDM para iOS.

Como resultado, luego de que se aplica la directiva, las cuentas CardDAV de la lista compilada se agregan al dispositivo móvil del usuario.

> Si tiene problemas para agregar o actualizar cuentas, verifique si la configuración que estableció es correcta.

Agregar una cuenta de calendario

Para permitir que un usuario del dispositivo MDM con iOS acceda a sus eventos en un servidor CalDAV, agregue una cuenta CalDAV. La sincronización con el servidor de CalDAV permite que el usuario cree y reciba invitaciones, reciba actualizaciones de eventos y sincronice tareas con la aplicación Recordatorios.

Para agregar una cuenta CalDAV del usuario de un dispositivo MDM con iOS, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **iOS** y vaya a la sección **Device configuration**.

4. En la tarjeta **Calendar**, haga clic en **Settings**.

   Se abre la ventana **Calendar**.

5. Habilite la configuración con el interruptor **Calendar**.

6. Haga clic en **Add**.

   Se abre la ventana **Add CalDAV account**.

7. En la sección **Server**, en el campo **Description**, ingrese una descripción de la cuenta CalDAV del usuario.

8. En los campos **Server address** y **Server port**, escriba el nombre de host o la dirección IP del servidor CalDAV y el número de puerto del servidor CalDAV.

9. En el campo **Calendar URL**, especifique la URL de la cuenta CalDAV del usuario del dispositivo MDM con iOS en el servidor CalDAV (por ejemplo: http://example.com/caldav/users/mycompany/user).

   La URL debe empezar por `http://` o `https://`.

10. En la sección **Authentication**, en el campo **Account name**, escriba el nombre de la cuenta para la autorización en el servidor CalDAV.

11. En el campo **Password**, establezca la contraseña de la cuenta de CalDAV para autenticarse en el servidor CalDAV.

12. Si desea usar el protocolo de transporte de datos SSL (Secure Sockets Layer) para proteger la transmisión de datos de eventos entre el servidor CalDAV y el dispositivo móvil, seleccione la casilla la casilla **Use SSL connection**.

13. Si es necesario, en la sección **Per App VPN**, configure Per App VPN.

14. Haga clic en **Agregar**.

    La nueva cuenta de usuario de CalDAV aparece en la lista.

    Puede modificar o eliminar cuentas CalDAV en la lista con los botones **Edit** y **Delete** que se encuentran en la parte superior de la lista.

15. Haga clic en **Aceptar**.

16. Haga clic en el botón **Save** para guardar los cambios que realizó.

    La configuración del dispositivo móvil se cambia después de la siguiente sincronización del dispositivo con el Servidor de MDM para iOS.

    Como resultado, luego de que se aplica la directiva, las cuentas CalDAV de la lista compilada se agregan al dispositivo móvil del usuario.

Si tiene problemas para agregar o actualizar cuentas, verifique si la configuración que estableció es correcta.

Configurar una suscripción al calendario

Esta configuración se aplica a los dispositivos supervisados y a los dispositivos que funcionan en el modo de control básico.

Para permitir que el usuario del dispositivo MDM con iOS agregue eventos de calendarios compartidos (como un calendario corporativo) al calendario del usuario, agregue una suscripción a estos calendarios. Los *calendarios compartidos* son calendarios de otros usuarios que tienen una cuenta de CalDAV, calendarios iCal y otros calendarios publicados.

Para agregar una suscripción al calendario, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **iOS** y vaya a la sección **Device configuration**.

4. En la tarjeta **Calendar subscriptions**, haga clic en **Settings**.

   Se abre la ventana **Calendar subscriptions**.

5. Habilite la configuración con el interruptor **Calendar subscriptions**.

6. Haga clic en **Add**.

   Se abre la ventana **Add calendar subscription**.

7. En el campo **Description**, escriba una descripción para la suscripción al calendario.

8. En el campo **Server address**, especifique la URL de un calendario de otras empresas.

   En este campo, puede ingresar la URL principal de la cuenta de CalDAV del usuario a cuyo calendario desea suscribirse. También puede especificar la dirección web de un calendario de iCal o de otro calendario publicado.

9. En el campo **User name**, escriba el nombre de la cuenta de usuario que se usará para la autenticación ante el servidor del calendario de terceros.

10. En el campo **Password**, escriba la contraseña de suscripción al calendario para la autenticación ante el servidor del calendario de terceros.

11. Si desea usar el protocolo de transporte de datos SSL (Secure Sockets Layer) para proteger la transmisión de datos de eventos entre el servidor CalDAV y el dispositivo móvil, seleccione la casilla la casilla **Use SSL connection**.

12. Si es necesario, en la sección **Per App VPN**, configure Per App VPN.

13. Haga clic en **Agregar**.

    La nueva suscripción al calendario aparece en la lista.

    Puede modificar o eliminar suscripciones al calendario en la lista con los botones **Edit** y **Delete** que se encuentran en la parte superior de la lista.

14. Haga clic en **Aceptar**.

15. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se cambia después de la siguiente sincronización del dispositivo con el Servidor de MDM para iOS.

Como resultado, luego de que se aplica la directiva, los eventos del calendario compartido de la lista se agregan al calendario en el dispositivo móvil del usuario.

Configurar SSO

Esta configuración se aplica a los dispositivos supervisados y a los dispositivos que funcionan en el modo de control básico.

La configuración **SSO** le permite configurar la cuenta para utilizar la tecnología de inicio de sesión único. El *inicio de sesión único (SSO)* es un método de autenticación que permite que un usuario inicie sesión en varios servicios con un único ID. Se utiliza el protocolo Kerberos para autenticación del usuario.

Para configurar el uso de SSO en dispositivos MDM con iOS, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **iOS** y vaya a la sección **Device configuration**.

4. En la tarjeta **SSO**, haga clic en **Settings**.

   Se abre la ventana **SSO**.

5. Habilite la configuración con el interruptor **SSO**.

6. Especifique la siguiente configuración:

- En el campo **Account name**, especifique el nombre de la cuenta de inicio de sesión único del usuario para la autorización del servidor Kerberos. Puede ingresar un valor o seleccionar una macro haciendo clic en el botón +.
- En la sección **Authentication**, especifique la siguiente configuración de autenticación:
  - **Kerberos user name**

    Nombre principal de la cuenta de un usuario de dispositivo MDM con iOS en el servidor Kerberos. El nombre de usuario Kerberos distingue entre mayúsculas y minúsculas y debe especificarse en el formato `<principal>/<instancia>`, donde:

    1. `<principal>` es el nombre de usuario.
    2. `<instancia>` es una descripción del nombre principal, por ejemplo "admin". Puede omitirse el ejemplo

    Ejemplo: si el nombre de usuario de Kerberos es `mycompany/admin@EXAMPLE.COM` o `mycompany@EXAMPLE.COM`, debe ingresar `mycompany/admin` o `mycompany` respectivamente.

    Puede ingresar un valor o seleccionar una macro haciendo clic en el botón +.

    > No use el símbolo arroba (@) en este campo. De lo contrario, el perfil SSO no se aplicará al dispositivo.

  - **Kerberos scope**

    Nombre de la red a la cual el servidor Kerberos y los dispositivos MDM con iOS pertenecen. El ámbito debe escribirse en letras mayúsculas.

    El nombre de la red debe coincidir con el nombre del dominio. Por ejemplo, si los nombres coinciden, el nombre del ámbito para el dominio example.com es `EXAMPLE.COM`.

    Ejemplo: si el nombre de usuario de Kerberos es `mycompany/admin@EXAMPLE.COM`, debe ingresar `EXAMPLE.COM`.

  - **Authentication certificate**

    Certificado utilizado para la autenticación de usuarios.

- En la sección **URL prefixes**, especifique las direcciones de los sitios web en los que Kaspersky Mobile Devices Protection and Management permite el uso de SSO:
  - **Limit account to the listed URLs**

    Uso de un inicio de sesión único para el inicio de sesión automático solo en los sitios web agregados a la lista de direcciones web permitidas. Puede crear una lista de direcciones web permitidas al hacer clic en el botón **Add URL** junto a la casilla.

    Si la casilla está marcada, el usuario puede utilizar el inicio de sesión único para la autorización en los sitios web que fueron agregados a la lista de direcciones web permitidas.

    Si la casilla no está marcada o la lista está vacía, el usuario puede usar el inicio de sesión único para todos los sitios web dentro del **ámbito Kerberos**.

    Nombre de la red a la cual el servidor Kerberos y los dispositivos MDM con iOS pertenecen. El ámbito debe escribirse en letras mayúsculas.

    El nombre de la red debe coincidir con el nombre del dominio. Por ejemplo, si los nombres coinciden, el nombre del ámbito para el dominio example.com es `EXAMPLE.COM`.

Ejemplo: si el nombre de usuario de Kerberos es `mycompany/admin@EXAMPLE.COM`, debe ingresar `EXAMPLE.COM`.

Esta casilla está desactivada por defecto.

- **Add URL**

  Al hacer clic en el botón, se agrega el campo **URL prefix** para especificar un nuevo sitio web en la lista de direcciones web para las que se permite el inicio de sesión único automático.

  Este botón está disponible si la casilla **Limit account to the listed URLs** está marcada.

  La dirección web debe comenzar con `http://` o `https://`. El inicio de sesión automático único se lleva a cabo solo cuando la URL coincide totalmente con la plantilla de URL. Por ejemplo, la dirección web `https://example.com/` no coincide con la dirección web `https://example.com:443/`.

  Para permitir el acceso de inicio de sesión único solo a sitios web que utilizan el protocolo HTTP, escriba el valor `http://`. Para permitir el acceso solo a los sitios web que utilizan el protocolo seguro HTTPS, ingrese `https://`.

  Si la dirección web no termina con el símbolo "/", Kaspersky Mobile Devices Protection and Management agrega este símbolo automáticamente.

  Si la lista de direcciones web permitidas está vacía, el usuario puede usar el inicio de sesión único para iniciar sesión automáticamente en todos los sitios web en el **Ámbito Kerberos**.

  Nombre de la red a la cual el servidor Kerberos y los dispositivos MDM con iOS pertenecen. El ámbito debe escribirse en letras mayúsculas.

  El nombre de la red debe coincidir con el nombre del dominio. Por ejemplo, si los nombres coinciden, el nombre del ámbito para el dominio example.com es `EXAMPLE.COM`.

  Ejemplo: si el nombre de usuario de Kerberos es `mycompany/admin@EXAMPLE.COM`, debe ingresar `EXAMPLE.COM`.

- En la sección **Bundle IDs**, especifique los ID de las aplicaciones en las que Kaspersky Mobile Devices Protection and Management permite el uso de SSO:

  - **Limit account to the listed apps**

    Uso de inicio de sesión único para el inicio de sesión automático en las aplicaciones agregadas a la lista de identificadores de paquetes. Puede crear una lista de ID de paquetes al hacer clic en el botón **Add app** junto a la casilla.

    Si la casilla está marcada, el usuario puede utilizar un inicio de sesión único solo para la autorización en las aplicaciones que se agregaron a la lista de ID de paquetes.

    Si la casilla no está marcada o la lista está vacía, el usuario puede usar el inicio de sesión único para todas las aplicaciones dentro del **ámbito Kerberos**.

    Nombre de la red a la cual el servidor Kerberos y los dispositivos MDM con iOS pertenecen. El ámbito debe escribirse en letras mayúsculas.

    El nombre de la red debe coincidir con el nombre del dominio. Por ejemplo, si los nombres coinciden, el nombre del ámbito para el dominio example.com es `EXAMPLE.COM`.

    Ejemplo: si el nombre de usuario de Kerberos es `mycompany/admin@EXAMPLE.COM`, debe ingresar `EXAMPLE.COM`.

    Esta casilla está desactivada por defecto.

  - **Add app**

    Al hacer clic en el botón, se agrega el campo **Bundle ID** para especificar un nuevo ID de paquete en la lista de aplicaciones para las que se permite el inicio de sesión único automático.

El botón está disponible si la casilla **Limit account to the listed apps** está marcada.

El inicio de sesión automático único se lleva a cabo solo cuando el ID agregado coincide completamente con el ID de paquete. Por ejemplo: `com.mycompany.myapp`.

Para otorgar acceso a varias aplicaciones utilizando el inicio de sesión único, utilice el símbolo "*" luego del carácter ".". Por ejemplo: `com.mycompany.*`. Se permitirá el acceso a todas las aplicaciones a las que su ID de paquete comienza con el prefijo especificado.

Si la lista de ID de paquetes está vacía, el usuario puede usar el inicio de sesión único para iniciar sesión automáticamente en todas las aplicaciones en el **Ámbito Kerberos**.

Nombre de la red a la cual el servidor Kerberos y los dispositivos MDM con iOS pertenecen. El ámbito debe escribirse en letras mayúsculas.

El nombre de la red debe coincidir con el nombre del dominio. Por ejemplo, si los nombres coinciden, el nombre del ámbito para el dominio example.com es `EXAMPLE.COM`.

Ejemplo: si el nombre de usuario de Kerberos es `mycompany/admin@EXAMPLE.COM`, debe ingresar `EXAMPLE.COM`.

7. Haga clic en **Aceptar**.

8. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se cambia después de la siguiente sincronización del dispositivo con el Servidor de MDM para iOS.

Como resultado, una vez que se aplica la directiva, el SSO se configura en el dispositivo MDM con iOS.

Administrar Clips web

Un *Clip web* es una aplicación que abre un sitio web desde la pantalla de inicio de un dispositivo móvil. Cuando hace clic en los íconos de los Clips web en la pantalla de inicio del dispositivo, el usuario puede abrir sitios web rápidamente (como el sitio web corporativo).

Puede agregar o eliminar Clips web en los dispositivos de usuarios y configurar el aspecto del ícono que se muestra en la pantalla.

Administrar Clips web en dispositivos MDM con iOS

De manera predeterminada, se aplican las siguientes restricciones a los Clips web:

- El usuario no puede quitar manualmente los Clips web del dispositivo móvil.
- Los efectos visuales de redondeo de bordes, sombra y brillo se aplican al ícono del Clip web en la pantalla.
- Los sitios web que se abren cuando el usuario toca el ícono de un Clip web no se abren en el modo pantalla completa.

Para agregar un Clip web al dispositivo MDM con iOS de un usuario, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **iOS** y vaya a la sección **Device configuration**.

4. En la tarjeta **Web Clips**, haga clic en **Settings**.

   Se abre la ventana **Web Clips**.

5. Habilite la configuración con el interruptor **Web Clips**.

6. Haga clic en **Agregar**.

   Se abre la ventana **Add Web Clip**.

7. En el campo **Web Clip name**, escriba el nombre del Clip web a mostrar en la pantalla de inicio del dispositivo MDM con iOS.

8. En el campo **Website URL**, escriba la dirección web del sitio web que se abrirá cuando el usuario toque el ícono del Clip web. La dirección debe comenzar con "`http://`" o "`https://`".

   Utilice solo fuentes legítimas y de confianza. Al configurar los ajustes en este campo, usted es el único responsable de los posibles riesgos y consecuencias asociados con el uso de fuentes no confiables.

   Si el sitio web ingresado está prohibido o no está en la lista de sitios web permitidos en la configuración de **Web Control** de la directiva, los usuarios no podrán acceder a este sitio web a través del Clip web.

9. Haga clic en **Select** para especificar la imagen del ícono de Clip web.

   La imagen debe cumplir con los siguientes requisitos:

   - Tamaño de la imagen de 400 x 400 píxeles como máximo.
   - Formato de archivo: PNG, JPEG o ICO.
   - Tamaño del archivo no mayor a 1 MB.

   Si no selecciona una imagen para el Clip web, se muestra un cuadrado en blanco como ícono.

   Si la imagen seleccionada tiene un fondo transparente, el fondo será negro en el dispositivo.

10. En la sección **Options**, especifique la siguiente configuración adicional:

    a. Si desea permitir que el usuario elimine el Clip web del dispositivo MDM con iOS, seleccione la casilla **Allow removal of Web Clip**.

    b. Si desea que el ícono de Clip web se muestre sin efectos visuales especiales (efecto de redondeo de bordes y brillo del icono), active la casilla **Precomposed icon**.

c. Si desea que el sitio web se abra en modo pantalla completa en el dispositivo MDM con iOS cuando toca el ícono, active la casilla **Full screen Web Clip**.

> En el modo de pantalla completa, la barra de herramientas de Safari está oculta y solo se muestra el sitio web en la pantalla del dispositivo.

11. Haga clic en **Agregar**.

    El nuevo Clip web aparece en la lista.

> Puede modificar o eliminar redes Clips web en la lista con los botones **Editar** y **Eliminar** que se encuentran en la parte superior de la lista.

12. Haga clic en **Aceptar**.

13. Haga clic en el botón **Save** para guardar los cambios que realizó.

Luego de que se aplica la directiva, los íconos de los Clips web de la lista que creó se agregan a la pantalla de inicio del dispositivo móvil del usuario.

Los Clips web eliminados se eliminan de la pantalla de inicio del dispositivo MDM con iOS.

Agregar fuentes

> Esta configuración se aplica a los dispositivos supervisados y a los dispositivos que funcionan en el modo de control básico.

Para añadir una fuente en el dispositivo iOS con MDM de un usuario:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **iOS** y vaya a la sección **Device configuration**.

4. En la tarjeta **Custom fonts**, haga clic en **Settings**.

   Se abre la ventana **Custom fonts**.

5. Habilite la configuración con el interruptor **Custom fonts**.

6. Haga clic en **Add**.

7. Seleccione el archivo de fuente guardado en su equipo. El archivo debe tener la extensión .OTF o .TTF.

> No se admiten las fuentes con extensión .OTC o .TTC.

Las fuentes son identificadas utilizando nombres PostScript. No instale fuentes con el mismo nombre PostScript aunque su contenido sea distinto. La instalación de fuentes con el mismo nombre PostScript generará un error.

8. Haga clic en **Abierta**.

   La nueva fuente aparece en la lista.

   Puede eliminar las fuentes de la lista con el botón **Delete** en la parte superior de la lista.

9. Haga clic en **Aceptar**.

10. Haga clic en el botón **Save** para guardar los cambios que realizó.

    La configuración del dispositivo móvil se cambia después de la siguiente sincronización del dispositivo con el Servidor de MDM para iOS.

    Como resultado, luego de que se aplica la directiva, se le solicitará al usuario que instale fuentes de la lista que se ha creado.

Trabajar con comandos para dispositivos móviles

Esta sección contiene información sobre los comandos para la administración de dispositivos móviles admitidos por Kaspersky Security Center. Proporciona instrucciones sobre cómo enviar comandos a dispositivos móviles, además de cómo ver los estados de ejecución de los comandos en el historial de comandos.

Comandos para dispositivos móviles

Kaspersky Security Center admite comandos para la administración remota de dispositivos móviles. Por ejemplo, si un dispositivo móvil se perdió o alguien lo robó, puede enviar comandos para localizar el dispositivo o eliminar todos los datos corporativos que almacena.

Puede enviar comandos a los siguientes tipos de dispositivos móviles administrados:

- Dispositivos Android administrados a través de la aplicación Kaspersky Endpoint Security para Android
- Dispositivos MDM con iOS

Cada tipo de dispositivo admite un conjunto de comandos dedicado.

Puede cancelar comandos en el **Command history**.

Los comandos pueden enviarse casi de inmediato a los dispositivos conectados a Internet. Como resultado, es posible que no se cancelen a pesar de que se muestran como cancelados.

Comandos para dispositivos Android

Comando	Resultado
Lock device	El dispositivo móvil está bloqueado. Para obtener acceso a los datos, debe desbloquear el dispositivo mediante el comando **Unlock device** o un código de acceso único.
Unlock device	El dispositivo móvil se desbloquea. Después de desbloquear un dispositivo con Android 5 a 6, la contraseña de desbloqueo de la pantalla se restablece a "1234". Después de desbloquear un dispositivo con Android 7 o versiones posteriores, la contraseña de desbloqueo de la pantalla no se modifica.
Reset to factory settings	Se eliminarán todos los datos del dispositivo móvil y se restablecerá la configuración de fábrica. Después de que este comando se ejecute, el dispositivo no podrá recibir o ejecutar comandos subsecuentes. Este comando no está disponible para dispositivos personales y dispositivos con un contenedor corporativo con Android 14 o posterior.
Wipe corporate data	Los datos corporativos se eliminan del dispositivo. La lista de datos eliminados depende del modo en el que esté funcionando el dispositivo: • En un dispositivo personal, se eliminan el contenedor de Knox, los archivos corporativos enviados al dispositivo y el certificado de correo. • En un dispositivo corporativo, el contenedor de Knox, los archivos corporativos enviados al dispositivo y los certificados instalados por Kaspersky Endpoint Security para Android (certificados de correo, VPN y perfil SCEP, excepto los certificados móviles) se eliminan. • Además, si se creó un contenedor corporativo, el contenedor corporativo (su contenido, archivos corporativos enviados al dispositivo, configuraciones y restricciones) y los certificados instalados en el contenedor corporativo (certificados de correo, VPN y perfil SCEP, excepto los certificados móviles) se eliminan.
Synchronize device	Los datos del dispositivo móvil se sincronizan con el Servidor de administración. El estado *Executed* puede mostrarse cuando el comando se envió correctamente pero el dispositivo aún no recibió.
Locate device	Se obtienen las coordenadas de la ubicación del dispositivo móvil. Las marcas de tiempo de la localización se muestran según la hora del servidor de Kaspersky Security Center. Para ver la ubicación del dispositivo en Yandex.Maps, vaya a la sección **Asset management** → **Mobile** → **Devices**. Luego, elija un dispositivo y seleccione **Command history** → **Locate device** → **Device coordinates** → **View on map**. Después de hacer clic en **View on map**, las coordenadas del dispositivo se transfieren a Yandex.Maps y el dispositivo se muestra en un mapa. En dispositivos con Android 12 o posterior, si el usuario otorgó el permiso "Usar ubicación aproximada", la aplicación Kaspersky Endpoint Security para Android primero intenta obtener la ubicación precisa del dispositivo. Si esto no es posible, se devuelve la ubicación aproximada del dispositivo solo si se recibió en los últimos 30 minutos. De lo contrario, el comando falla. Este comando no funciona en dispositivos Android si la Precisión de ubicación de Google está deshabilitada en la configuración. Tenga en cuenta que no todos los dispositivos Android vienen con esta configuración de ubicación.

Comando	Resultado
Take photos	El dispositivo móvil está bloqueado. Se toman fotos con la cámara frontal del dispositivo cuando alguien intenta desbloquear el dispositivo. En dispositivos con una cámara frontal emergente, la foto será negra si la cámara está guardada. Al intentar desbloquear el dispositivo, el usuario acepta automáticamente que se le tome una foto en el dispositivo. Si se revocó el permiso para usar la cámara, el dispositivo móvil muestra una notificación y le pide que proporcione el permiso. En un dispositivo móvil con Android 12 o posterior, si se revocó el permiso para usar la cámara a través de la Configuración rápida, la notificación no se muestra, pero la foto tomada es negra.
Sound alarm	El dispositivo móvil hace sonar una alarma durante 5 minutos (durante 1 minuto si la batería del dispositivo está baja) o hasta que el usuario desbloquee el dispositivo.
Wipe app data	Los datos de una aplicación especificada se eliminan del dispositivo móvil. Para esta acción, debe especificar el nombre del paquete para la aplicación cuyos datos se eliminarán. Como resultado, la aplicación se revierte a su estado predeterminado. Los datos del sistema y las aplicaciones administrativas no se eliminan.
Wipe data of all apps	Los datos de todas las aplicaciones se eliminan del dispositivo móvil. En un dispositivo corporativo, se eliminan los datos de todas las aplicaciones en el dispositivo. En un dispositivo con un contenedor corporativo, se eliminan los datos de todas las aplicaciones en el contenedor corporativo. Como resultado, las aplicaciones vuelven a su estado predeterminado. Los datos del sistema y las aplicaciones administrativas no se eliminan.
Send message	Se envía un mensaje con el título y el texto especificados al dispositivo móvil del usuario. Puede enviar solo una notificación push o una notificación push y una alerta.
Get location history	Se muestra el historial de ubicaciones del dispositivo móvil durante los últimos 14 días. Las marcas de tiempo de localización se muestran según la hora del dispositivo. Para ver la ubicación del dispositivo en Yandex.Maps, vaya a la sección **Asset management** → **Mobile** → **Devices**. Luego, elija un dispositivo y seleccione **Command history** → **Get location history** → **View on map**. Después de hacer clic en **View on map**, las coordenadas del dispositivo se transfieren a Yandex.Maps y el dispositivo se muestra en un mapa. Debido a las limitaciones técnicas de los dispositivos Android, es posible que la ubicación del dispositivo se recupere con menos frecuencia de la especificada en la configuración **Location tracking**.
Reboot device	Se reinicia el dispositivo móvil. El resultado de la ejecución del comando se enviará a Kaspersky Security Center después de que el usuario desbloquee su dispositivo. El dispositivo no se puede reiniciar durante una llamada. Kaspersky Endpoint Security para Android intentará ejecutar el comando nuevamente una vez que finalice la llamada. Este comando solo está disponible para dispositivos corporativos que ejecutan Android 7 o versiones posteriores.
Reset password	Se restablece la contraseña de desbloqueo del dispositivo corporativo o del contenedor corporativo. Este comando no está disponible para dispositivos personales.

Comandos para dispositivos MDM con iOS

Comando	Resultado
Lock device	El dispositivo móvil está bloqueado. Para acceder a los datos, debe desbloquear el dispositivo.
Reset unlock password	Se restablece la contraseña de desbloqueo de la pantalla del dispositivo móvil y se le solicita al usuario que establezca una nueva contraseña de acuerdo con los requisitos de la directiva.
Reset to factory settings	Se eliminarán todos los datos del dispositivo móvil y se restablecerá la configuración de fábrica. Después de que este comando se ejecute, el dispositivo no podrá recibir o ejecutar comandos subsecuentes.
Wipe corporate data	Todos los perfiles de configuración instalados, el perfil de administración y las aplicaciones para las que se seleccionó la casilla **Remove when device management profile is deleted** se eliminan del dispositivo.
Synchronize device	Los datos del dispositivo móvil se sincronizan con el Servidor de administración.
Install configuration profile	Se instala un perfil de configuración en el dispositivo móvil. No puede instalar un perfil de configuración con ajustes para un dispositivo supervisado en un dispositivo en modo de control básico.
Delete configuration profile	El perfil de configuración se elimina del dispositivo móvil. El perfil puede aparecer en la lista de perfiles de configuración instalados en el dispositivo durante varios minutos después de que se haya eliminado.
Install app	Se instala la aplicación especificada en el dispositivo móvil.
Update app	Se actualiza la aplicación especificada en el dispositivo móvil.
Delete app	Se elimina la aplicación especificada del dispositivo móvil.
OS update (supervised only)	Las actualizaciones del sistema operativo se programan en el dispositivo móvil de acuerdo con la configuración de actualización especificada. Es posible que este comando no se ejecute si un dispositivo no tiene suficiente espacio de almacenamiento o la versión del sistema operativo especificado no está disponible para el dispositivo seleccionado. Recomendamos especificar la versión más reciente disponible del sistema operativo.
Change roaming settings	Se habilita o deshabilita el roaming de datos y de voz.
Set Bluetooth state (supervised only)	Bluetooth está habilitado o deshabilitado en el dispositivo móvil. Este comando solo es compatible con dispositivos supervisados que ejecutan iOS 11.3 o posterior.
Enable Lost Mode (supervised only)	El modo perdido se habilita en el dispositivo móvil supervisado y se bloquea el dispositivo. La pantalla del dispositivo muestra un mensaje y un número de teléfono que puede editar. Si envía el comando Habilitar modo perdido a un dispositivo MDM con iOS supervisado sin una tarjeta SIM y este dispositivo se reinicia, el dispositivo no podrá conectarse a Wi-Fi y recibir el comando Deshabilitar modo perdido. Esta es una característica específica de los dispositivos iOS. Para evitar este problema, puede enviar el comando solo a dispositivos con una tarjeta SIM o insertar una tarjeta SIM en el dispositivo bloqueado para permitirle recibir el comando Deshabilitar modo perdido a través de la red móvil.
Locate device (Lost Mode only)	Se obtiene la ubicación del dispositivo móvil. Para ver la ubicación del dispositivo en Yandex.Maps, vaya a la sección **Asset management** → **Mobile** → **Devices**. Luego, elija un dispositivo y seleccione **Command history** → **Locate device** → **Device coordinates** → **View on map**. Después de hacer clic en **View on map**, las coordenadas del dispositivo se transfieren a Yandex.Maps y el dispositivo se muestra en un mapa.

Comando	Resultado
Sound alarm (Lost Mode only)	Se reproduce un sonido en el dispositivo móvil perdido.
Disable Lost Mode (supervised only)	El modo perdido se deshabilita en el dispositivo móvil y se desbloquea el dispositivo.

Permisos para la ejecución de comandos

Se requieren derechos y permisos especiales para ejecutar comandos de Kaspersky Endpoint Security para Android. Mientras se ejecuta el Asistente de configuración inicial, Kaspersky Endpoint Security para Android le pide al usuario que otorgue a la aplicación todos los permisos y derechos necesarios. El usuario puede omitir estos pasos o deshabilitar estos permisos más adelante en la configuración del dispositivo. Si este es el caso, será imposible ejecutar comandos.

En dispositivos con Android 10 o posterior, el usuario debe otorgar el permiso "Todo el tiempo" para acceder a la ubicación. En dispositivos con Android 11 o posterior, el usuario también debe otorgar el permiso "Mientras se usa la aplicación" para acceder a la cámara. De lo contrario, los comandos de antirrobo no funcionarán. Se notificará al usuario esta limitación y se le volverá a pedir que otorgue el nivel requerido de los permisos. Si el usuario selecciona la opción "Solo esta vez" para el permiso de la cámara, la aplicación considerará el permiso como otorgado. Se recomienda comunicarse con el usuario directamente si se vuelve a pedir el permiso de la cámara.

Enviar comandos

Para enviar un comando al dispositivo móvil del usuario:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.
2. En la lista de dispositivos que se abre, seleccione un dispositivo al que desee enviar un comando.

   Puede seleccionar varios dispositivos.

3. Haga clic en **Send command**.
4. En la ventana **Send command** que se abre, en el campo **Command**, seleccione un comando.
5. Configure el comando que desea enviar.
6. Haga clic en **Send**.

   Puede ver y cancelar comandos en el **Command history**.

El comando se envía a los dispositivos seleccionados.

Ver los estados de los comandos en el historial de comandos

La aplicación guarda información sobre todos los comandos que se enviaron a dispositivos móviles en el historial de comandos. El historial de comandos contiene información acerca de la fecha y hora en que se envió cada comando al dispositivo móvil, sus estados y las descripciones detalladas de los resultados. Por ejemplo, cuando un comando falla, el historial muestra la causa del error.

Los comandos enviados a los dispositivos móviles pueden tener los siguientes estados:

- *Enviado*

  El comando se envió al dispositivo móvil.

- *Ejecutado*

  La ejecución del comando se realizó correctamente.

- *Error*

  Error al ejecutar el comando.

- *Cancelando*

  El comando se está eliminando de la cola de comandos enviados al dispositivo móvil.

- *Cancelado*

  El comando se eliminó correctamente de la cola de comandos enviados al dispositivo móvil.

La aplicación mantiene un historial de comandos para cada dispositivo móvil.

Para ver el historial de comandos, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Mobile** → **Devices**.

2. En la lista de dispositivos móviles, seleccione aquel para el que desee ver el historial de comandos.

3. Haga clic en **Command history**.

   Se abre la ventana **Command history**. Las secciones de la ventana **Command history** corresponden a los comandos que pueden enviarse al dispositivo móvil.

4. Seleccione las secciones que contengan los comandos que necesita y vea información acerca de cómo se envían y ejecutan los comandos.

Administrar la aplicación a través de soluciones EMM de terceros (solo para Android)

Puede usar Kaspersky Endpoint Security para Android sin los sistemas de administración de Kaspersky. Utilice las soluciones de otros proveedores de servicios EMM (Enterprise Mobility Management) para instalar y administrar Kaspersky Endpoint Security para Android. Kaspersky participa en la Comunidad AppConfig para garantizar que la aplicación opere con las soluciones EMM de otras empresas.

Además, puede usar una solución EMM de terceros únicamente para desplegar Kaspersky Endpoint Security para Android y, después del despliegue, administrar los dispositivos en Kaspersky Next Expert View (on-premise).

Si Kaspersky Endpoint Security para Android se despliega mediante una solución EMM de terceros, no puede administrar la aplicación en Kaspersky Endpoint Security Cloud, pero puede hacerlo en la consola EMM, Kaspersky Next Expert View (on-premise) o Kaspersky Security Center Cloud Console.

Las siguientes soluciones EMM admiten el uso de la aplicación Kaspersky Endpoint Security para Android:

- VMware AirWatch
- MobileIron
- IBM Maas360
- Microsoft Intune
- SOTI MobiControl

Puede realizar las siguientes acciones en la Consola EMM:

- Implemente la aplicación en un perfil de trabajo de Android creado por una solución de EMM de terceros.
- Activar la aplicación.
- Establecer la configuración de la aplicación:
  - Habilitar la protección contra sitios web maliciosos y de phishing en Internet.
  - Configure los ajustes para conectar el dispositivo a Kaspersky Security Center.
  - Configure los ajustes del Antimalware.
  - Configure la programación para ejecutar un análisis de malware en el dispositivo.
  - Permita la detección de adware y aplicaciones que pueden ser utilizados para dañar su dispositivo o sus datos personales.
  - Configure la programación para actualizaciones de la base de datos de la aplicación.

Primeros pasos

Actualmente, Kaspersky Endpoint Security para Android no está disponible en Google Play.

Para implementar Kaspersky Endpoint Security para Android en los dispositivos de los usuarios, debe agregar la aplicación a la tienda de aplicaciones de EMM mediante el archivo de instalación APK del sitio web de Kaspersky. Para obtener más información sobre el funcionamiento con aplicaciones en Consola EMM, visite el *sitio web del Soporte Técnico del proveedor de servicios EMM*.

Kaspersky Endpoint Security para Android se implementa en un perfil de trabajo de Android creado por una solución de EMM de terceros. La aplicación se aísla de los datos personales del usuario y protege solo datos corporativos en el perfil de trabajo.

Recomendamos proteger la aplicación Kaspersky Endpoint Security para Android para que no la eliminen las herramientas de EMM Console.

Cómo instalar la aplicación

Si desea administrar dispositivos en una consola de EMM de terceros, puede distribuir la aplicación utilizando el archivo APK del sitio web de Kaspersky.

Para que la aplicación funcione, se requieren los siguientes permisos:

- Permiso de almacenamiento para acceder a los archivos cuando se ejecuta el Antimalware (solo para Android 6 o versiones posteriores).
- Permiso telefónico para identificar el dispositivo, por ejemplo, al activar la aplicación.
- Permiso de administrador del dispositivo para las principales funciones de protección, como Antirrobo y Control de aplicaciones.
- Solicitud para agregar Kaspersky Endpoint Security para Android a la lista de aplicaciones que se abren al iniciarse el sistema operativo en ciertos dispositivos HUAWEI, Meizu y Xiaomi. Si la solicitud Añadir no se muestra, manualmente agregue Kaspersky Endpoint Security para Android a la lista de aplicaciones de inicio. La solicitud no se puede mostrar si la aplicación de seguridad no se instala en el perfil de trabajo.

Puede conceder los permisos requeridos en la Consola EMM antes de instalar la aplicación Kaspersky Endpoint Security para Android. Para obtener más información sobre la concesión de permisos en la Consola EMM, visite el *sitio web del soporte técnico del proveedor de servicios EMM*. También puede conceder los permisos mientras completa el Asistente de configuración inicial de Kaspersky Endpoint Security para Android en el dispositivo.

Kaspersky Endpoint Security para Android se instalará en el perfil de trabajo de Android creado por la solución de EMM de terceros. Luego, la aplicación se actualizará desde el sitio web de Kaspersky o desde HUAWEI AppGallery, Samsung Galaxy Store, RuStore o Xiaomi GetApps.

Para el funcionamiento de la Protección web, también debe configurar un servidor proxy en la configuración de Google Chrome mediante AppConfig a través del sistema de EMM de terceros:

- Modo de la configuración del servidor proxy: manual.
- Dirección y puerto del servidor proxy: 127.0.0.1:3128.
- Protocolo SPDY: desactivado.
- Compresión de datos a través de servidor proxy: desactivado.

Proteger dispositivos en Internet

Para proteger los datos personales de un usuario del dispositivo móvil en Internet, habilite Protección web. El componente Protección web bloquea los sitios web maliciosos que distribuyen un código malicioso y los sitios web de phishing diseñados para robar sus datos confidenciales y acceder a sus cuentas financieras. Protección Web usa el servicio en la nube Kaspersky Security Network para analizar sitios web antes de que los abra.

Para que el componente Protección web funcione, se deben cumplir las siguientes condiciones:

- Se configura el servidor proxy en la configuración del navegador:

  `ProxyMode = "fixed_servers"`

  `ProxyServer = "127.0.0.1:3128"`

  `DisableSpdy = true`

  `DataCompressionProxyEnabled = false`

  La configuración del servidor proxy puede variar según la versión de Google Chrome. Para obtener más información sobre la configuración de Google Chrome, visite el sitio web del proyecto de Chromium.

  Después de que la aplicación Kaspersky Endpoint Security para Android se elimina del dispositivo móvil, reinicie la configuración del servidor proxy.

- Los usuarios del dispositivo aceptan la Política de privacidad y la Declaración de protección web en el Asistente de configuración inicial o en la configuración de la aplicación.

  El administrador puede aceptar la Declaración de protección web en Kaspersky Next Expert View (on-premise).

- Protección web está habilitada en la configuración de la aplicación:

  `EnableWebFilter = True`, `EnableWebFilterLock = True`.

- El uso de KSN está activado en la configuración de la aplicación: `UseKsnMode = Recommended` o `UseKsnMode = Extended`.

Si los dispositivos de los usuarios están conectados a Kaspersky Security Center, habilite Protección web en la directiva de grupo. Además, puede aceptar la Declaración de protección web en Kaspersky Next Expert View (on-premise).

Después de habilitar Protección web en la aplicación Kaspersky Endpoint Security para Android y configurar Google Chrome, verifique la protección contra amenazas web. Para verificar la protección, puede usar el archivo de prueba EICAR.

Cómo activar la aplicación

Se envía la información sobre la licencia al dispositivo móvil junto con la otra configuración en el archivo de configuración.

Si la aplicación no se activa en un plazo de 30 días después de su instalación en el dispositivo móvil, la licencia de prueba vence. Cuando caduca la licencia de prueba, se deshabilitan todas las funciones de Kaspersky Endpoint Security para Android.

Cuando caduca la licencia comercial, la aplicación sigue funcionando de manera limitada (por ejemplo, las actualizaciones de la base de datos de Kaspersky Endpoint Security para Android no están disponibles). Para continuar usando la funcionalidad completa de la aplicación, debe renovar su licencia comercial.

Para activar Kaspersky Endpoint Security para Android:

1. En Console EMM, abra la configuración de la aplicación Kaspersky Endpoint Security para Android.
2. En el campo `LicenseActivationCode`, escriba el código de activación de la aplicación.

   Para activar la aplicación en un dispositivo, debe tener acceso a servidores de activación de Kaspersky.

Cómo conectar un dispositivo a Kaspersky Security Center

Después de instalar Kaspersky Endpoint Security para Android en un dispositivo móvil, puede conectar el dispositivo a Kaspersky Security Center. Los datos necesarios para conectar el dispositivo a Kaspersky Security Center se envían al dispositivo móvil junto con los demás ajustes que figuran en el archivo de configuración. Después de conectar el dispositivo a Kaspersky Security Center, puede utilizar directivas de grupo para establecer de forma centralizada la configuración de la aplicación. También puede recibir informes y estadísticas sobre el rendimiento de Kaspersky Endpoint Security para Android.

Antes de conectar dispositivos a Kaspersky Security Center, asegúrese de que se cumplan las siguientes condiciones:

- El complemento Kaspersky Mobile Devices Protection and Management está instalado en el host de Kaspersky Next Expert View (on-premise).
- El puerto para conectar dispositivos móviles esté abierto en las propiedades del Servidor de administración.
- Se creó un certificado para dispositivos móviles para identificar al usuario del dispositivo móvil en las propiedades del Servidor de administración de Kaspersky Security Center.

Antes de conectar los dispositivos a Kaspersky Security Center, recomendamos hacer lo siguiente:

- Si desea crear directivas para dispositivos móviles, cree un grupo de administración diferente para dispositivos móviles. Las soluciones de EMM de terceros solo admiten el modo de funcionamiento del dispositivo personal.
- Si desea mover dispositivos móviles de manera automática a un grupo de administración diferente, cree una regla para mover dispositivos automáticamente desde la carpeta **Unassigned devices**.
- Si desea configurar Kaspersky Endpoint Security para Android de manera centralizada, cree una política de grupo.

Para conectar un dispositivo a Kaspersky Security Center:

1. En Console EMM, abra la configuración de la aplicación Kaspersky Endpoint Security para Android.
2. En el campo `KscServer`, escriba el nombre DNS o la dirección IP del Servidor de administración de Kaspersky Security Center. El puerto predeterminado es 13292.
3. Si no desea que las notificaciones de Kaspersky Endpoint Security para Android distraigan al usuario, deshabilite las notificaciones de la aplicación. Para hacerlo, configure `DisableNotification = True`.

   Después de conectarse, la aplicación muestra todas las notificaciones. Puede deshabilitar ciertas notificaciones de la aplicación en la configuración de la directiva.

No deshabilite las notificaciones de la aplicación si no utiliza Kaspersky Security Center. Esto podría hacer que un usuario no reciba notificaciones sobre la expiración de la licencia. Como resultado, la aplicación dejará de cumplir su función.

Una vez configurada la conexión, Kaspersky Endpoint Security para Android muestra una notificación que le solicita que conceda los siguientes derechos y permisos adicionales:

- Permiso para usar la cámara para la operación antirrobo (comando **Take photos**).
- Permiso para usar la ubicación para la operación antirrobo (comando **Locate device**).
- Derechos de administrador del dispositivo (propietario del perfil de trabajo de Android) para el funcionamiento de las siguientes funciones de la aplicación:
  - Configuración de Wi-Fi.
  - Restricción del uso de la cámara, Bluetooth y Wi-Fi.

Debido a las características específicas de un perfil de trabajo de Android de terceros, las funciones Antirrobo no están disponibles en la aplicación y el Control de aplicaciones no puede bloquear aplicaciones por su categoría.

Cuando el usuario otorga los derechos y permisos necesarios, el dispositivo se conecta a Kaspersky Security Center. Si no se creó una regla para mover dispositivos automáticamente a un grupo de administración, el dispositivo se agregará automáticamente a la carpeta **Unassigned devices**. Si se creó una regla para mover dispositivos automáticamente a un grupo de administración, el dispositivo se agregará automáticamente al grupo especificado.

Kaspersky Endpoint Security proporciona el siguiente formato de nombre de dispositivo: Modelo del dispositivo [ID de dispositivo, correo electrónico].

También puede agregar una etiqueta al nombre del dispositivo. Esto hace que sea más fácil encontrar y ordenar dispositivos en Kaspersky Security Center.

Para agregar la etiqueta al nombre del dispositivo:

1. En Console EMM, abra la configuración de la aplicación Kaspersky Endpoint Security para Android.
2. En el campo `KscDeviceNameTag`, seleccione los siguientes valores:
   - `{DeviceSerialNumber}`: Número de serie del dispositivo.
   - `{DeviceUid}`: Identificador único del dispositivo (UDID).
   - `{DeviceAssetNumber}`: Número de activo del dispositivo. Este número se crea internamente desde dentro de su organización.

Recomendamos utilizar únicamente estos valores.

Puede agregar algunos valores (por ejemplo, `{DeviceSerialNumber} {DeviceUid}`). La etiqueta se agregará al nombre del dispositivo en Kaspersky Security Center. Un espacio separa la etiqueta del nombre del dispositivo. Por ejemplo, si el nombre del dispositivo es `Google Pixel 2 a10c6b75f7b31de9 22:7D:78:9E:C5:1E`, la etiqueta UDID es `22:7D:78:9E:C5:1E`.

Una vez que el dispositivo está conectado a Kaspersky Security Center, la configuración de la aplicación se modifica de acuerdo con la directiva de grupo. Kaspersky Endpoint Security para Android ignora la configuración de la aplicación del archivo de configuración que se configuró en la Consola EMM. Puede configurar todas las secciones de la directiva excepto las siguientes:

- **Anti-Theft**
- **Screen unlock settings**
- La pestaña **App use** de la sección **App Control**
- **Corporate container on devices**
- **Samsung Knox settings**

Debido al método utilizado para implementar un perfil de trabajo de terceros, no puede aplicar la configuración de directiva de grupo desde la sección **Corporate container on devices**. Esta configuración solo se puede aplicar si contenedor corporativo se creó utilizando Kaspersky Security Center.

Modo silencioso

Un usuario del dispositivo Android puede desactivar todas las notificaciones de Kaspersky Endpoint Security para Android en la configuración de la barra de notificaciones. Si las notificaciones están deshabilitadas, el usuario no supervisa el funcionamiento de la aplicación y es posible que no vea información importante (por ejemplo, información en tiempo real sobre amenazas). En este caso, para averiguar el estado de funcionamiento de la aplicación, el usuario debe abrir Kaspersky Endpoint Security para Android.

Si no desea que el usuario del dispositivo móvil se distraiga con las notificaciones de Kaspersky Endpoint Security para Android, puede deshabilitar ciertas notificaciones.

Kaspersky Endpoint Security utiliza las siguientes herramientas para mostrar el estado de protección del dispositivo:

- **Notificación del estado de protección**. Esta notificación está anclada a la barra de notificaciones. La notificación del estado de protección no se puede eliminar. Muestra el estado de protección del dispositivo (por ejemplo,) y el número de problemas, si los hubiera. Puede presionar el estado de protección del dispositivo y ver la lista de problemas en la aplicación.
- **Notificaciones de la app**. Estas notificaciones informan al usuario del dispositivo sobre la aplicación (por ejemplo, detección de amenazas).
- **Mensajes emergentes**. Los mensajes emergentes requieren una acción del usuario del dispositivo (por ejemplo, qué hacer cuando se detecta una amenaza).

Los ajustes del modo silencioso se envían al dispositivo móvil junto con los demás ajustes en el archivo de configuración. Establezca el parámetro `DisableNotification` en `True`.

Si el dispositivo está conectado a Kaspersky Security Center, puede habilitar el modo silencioso solo en la directiva de grupo.

Archivo AppConfig

Se genera un archivo de configuración para configurar la aplicación en una consola EMM. Los ajustes de la aplicación en el archivo de configuración se presentan en la siguiente tabla.

Configuración de archivos

Clave de la configuración	Descripción	Tipo	Valor	Valor predeterminado
`LicenseActivationCode`	Código de activación de la aplicación	String	Código de activación de la app que consiste en 20 letras y números latinos. Para activar la aplicación mediante un código de activación, necesita acceso a Internet para conectarse con los servidores de activación de Kaspersky. Si deja el campo en blanco, la aplicación se activará con una licencia de prueba. La licencia de evaluación es válida durante 30 días. Cuando caduca la licencia de evaluación, se desactivan todas las funciones de la aplicación móvil Kaspersky Endpoint Security para Android. Para continuar usando la aplicación, debe adquirir la versión comercial.	
`EulaAcceptanceConfirmationV1`	<License Agreement link>	Choice	`Accepted`: Confirmo que he leído completamente, comprendo y acepto los términos y las condiciones de este Contrato de licencia de usuario final. `Declined`: No acepto los términos y las condiciones de este Contrato de licencia de usuario final (EULA). Para aceptar los términos y las condiciones del EULA para todos los dispositivos móviles, necesita acceder a Internet a fin de conectarse a los servidores de Kaspersky. Si elige `Declined`, la aplicación le pedirá al usuario que acepte los términos y las condiciones del EULA. Los usuarios del dispositivo móvil pueden aceptar las condiciones en el Asistente de configuración inicial.	

Clave de la configuración	Descripción	Tipo	Valor	Valor predeterminado
`EulaAcceptanceCodeV1`	Código de Contrato de licencia	String	Utilice `EulaAcceptanceCodeV1` si desea aceptar un único Contrato de licencia de usuario final (EULA). Utilice `EulaAcceptanceCodesV2` si desea aceptar varios EULA al mismo tiempo. El campo `EulaAcceptanceCodesV2` debe contener una lista de códigos EULA separados por punto y coma: `"<EULAid1>;<EULAid2>;<EULAid3>;..."`. El código del Contrato de licencia está incluido en el Contrato de licencia de usuario final. *Para conocer el código del Contrato de licencia:* 1. Copie el vínculo del Contrato de licencia (`EulaAcceptanceConfirmationV1`) de la Consola EMM. 2. Pegue el vínculo en el navegador. Se abrirá el Contrato de licencia de usuario final (EULA). 3. Lea los términos y las condiciones de este EULA y busque el código del Contrato de licencia. Para aceptar los términos y las condiciones de los EULA para todos los dispositivos móviles, debe acceder a Internet a fin de conectarse a los servidores de Kaspersky. Si deja los campos en blanco, la aplicación le pedirá al usuario que acepte los términos y las condiciones de los EULA. El usuario del dispositivo móvil puede aceptar las condiciones en el Asistente de configuración inicial. Si especifica los valores de ambos campos, se aceptarán los términos y las condiciones de todos los EULA especificados en ellos.	
`EulaAcceptanceCodesV2`	Códigos de Contrato de licencia	Cadena		
`KscServer`	Dirección y puerto del servidor de administración de Kaspersky Security Center	String	Nombre DNS o dirección IP del servidor de administración de Kaspersky Security Center y número de puerto. Ingrese la dirección como se indica a continuación: `<server address>:<port>`. Si ingresa la dirección del servidor sin especificar el puerto, la aplicación utilizará el puerto predeterminado 13292.	`<server address>:13292`
`DisableNotification`	Deshabilite las notificaciones de la aplicación antes de conectarse a Kaspersky Security Center	Boolean	`True`: Kaspersky Endpoint Security para Android oculta todas las notificaciones hasta que el dispositivo se conecta con Kaspersky Security Center. Después de conectarse, la aplicación muestra todas las notificaciones. Puede deshabilitar ciertas notificaciones de la aplicación en la configuración de la directiva. No deshabilite las notificaciones de la aplicación si no utiliza Kaspersky Security Center. Esto podría hacer que un usuario no vea las notificaciones sobre la expiración de la licencia. En este caso, la aplicación dejaría de funcionar. `False` – Kaspersky Endpoint Security para Android muestra todas las notificaciones de la aplicación.	`False`

Clave de la configuración	Descripción	Tipo	Valor	Valor predeterminado
`ScanScheduleType`	Modo de ejecución de análisis	Choice	`AfterUpdate`: inicia un análisis de malware después de una actualización de la base de datos. La aplicación actualiza las bases de datos antimalware según la programación definida (`UpdateScheduleType`). `Daily`: inicia un análisis de malware una vez al día. Configure el tiempo de inicio de análisis (`ScanScheduleTime`). `Weekly`: inicia un análisis de malware una vez por semana. Seleccione el día de la semana para iniciar un análisis de malware (`ScanScheduleDay`) y configurar el tiempo (`ScanScheduleTime`). `Off`: se deshabilita el inicio automático de un análisis de malware. Independientemente del valor configurado, el usuario del dispositivo puede iniciar manualmente un análisis de malware.	`AfterUpdate`
`ScanScheduleDay`	Día del análisis	Choice	`Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday` Puede seleccionar solo un valor para este parámetro.	`Monday`
`ScanScheduleTime`	Hora del análisis	String	El tiempo se puede indicar en formato de 24 horas (por ejemplo, 13:00) o en formato de 12 horas (por ejemplo, 10:30 p. m.).	`8:00`
`ScanScheduleLock`	Bloquee la configuración del modo de ejecución de análisis	Boolean	`True`: el usuario no puede acceder a la configuración del modo de ejecución del análisis de malware en la configuración de la aplicación. `False`: el usuario puede configurar el modo de ejecución del análisis de malware y, por ejemplo, deshabilitar el inicio automático de un análisis de malware.	`True`
`ScanActionOnThreatFound`	Acción al detectar amenazas (análisis de malware)	Choice	`Quarantine` – La aplicación pone objetos detectados en cuarentena. La cuarentena almacena los archivos como archivos comprimidos para que no puedan causar daños al dispositivo. El filtro de llamadas y mensajes de texto le permite eliminar o restaurar los archivos que se movieron a la cuarentena. `Delete` – La aplicación elimina el archivo detectado. `Skip` – La aplicación deja los objetos detectados sin alterar. Si las amenazas se han omitido, Kaspersky Endpoint Security para Android le advertirá al usuario sobre problemas en la protección del dispositivo. Cuando hay un intento de acceder a un objeto en el dispositivo (por ejemplo un intento de copiar o abrirlo), la aplicación bloquea el acceso al objeto. `AskUser` – La aplicación solicita al usuario seleccionar una acción para cada objeto detectado: omitir, poner en cuarentena o eliminar. Cuando se detectan varios objetos, el usuario puede aplicar una acción seleccionada a todos los objetos. Se registra la información sobre amenazas detectadas y las acciones tomadas sobre ellas en informes de la aplicación.	`Cuarentena`

Clave de la configuración	Descripción	Tipo	Valor	Valor predeterminado
`ScanLock`	Bloquee la configuración de análisis	Boolean	`True` – El usuario no puede acceder a la siguiente configuración de análisis en la configuración de la aplicación: el tipo de archivos para analizar, análisis de archivos y la acción que se tomará cuando se detecta una amenaza. `False` – El usuario puede establecer la configuración de análisis y, por ejemplo, seleccionar la acción `Skip` para amenazas detectadas.	`True`
`ScanAndProtectionAdwareRiskware`	Bloquear adware, marcadores automáticos y aplicaciones que los delincuentes pueden utilizar para dañar el dispositivo y los datos del usuario	Boolean	`True`: La aplicación detecta el adware y otras aplicaciones que los delincuentes pueden utilizar para dañar el dispositivo y los datos del usuario. `False`: La aplicación omite el adware y otras aplicaciones que los delincuentes pueden utilizar para dañar el dispositivo y los datos del usuario.	`True`
`ProtectionMode`	Modo de protección en tiempo real	Choice	`Recommended` – La aplicación analiza solo nuevas aplicaciones una vez inmediatamente después de que se han instalado, así como archivos desde la carpeta Descargas. `Extended` – La aplicación analiza todos los archivos que el usuario abre, modifica, copia, ejecuta y guarda en el dispositivo. La aplicación también analiza aplicaciones y archivos nuevos desde la carpeta Descargas. `Disabled` – La protección en tiempo real está deshabilitada.	`Recomendado`
`UseKsnMode`	Modo de Kaspersky Security Network	Choice	`Recommended`: la aplicación intercambia datos con Kaspersky Security Network (KSN). Kaspersky Endpoint Security para Android usa KSN para la protección en tiempo real del dispositivo contra amenazas (Protección en la nube) y el funcionamiento de Protección web en Internet. `Extended`: la aplicación intercambia datos con Kaspersky Security Network y también envía al laboratorio de virus determinadas estadísticas de rendimiento de Kaspersky Endpoint Security para Android. Esta información permite hacer un seguimiento de las amenazas en tiempo real. Los servicios de KSN no obtienen, procesan o almacenan datos personales. `Disabled`: la aplicación no usa datos desde Kaspersky Security Network. No puede habilitar la Protección web `(EnableWebFilter)`. El componente Protección en la nube no está disponible para el Antimalware.	`Recomendado`

Clave de la configuración	Descripción	Tipo	Valor	Valor predeterminado
`ProtectionActionOnThreatFound`	Acción al detectar una amenaza (Protección en tiempo real)	Choice	`Quarantine` – La aplicación pone objetos detectados en cuarentena. La cuarentena almacena los archivos como archivos comprimidos para que no puedan causar daños al dispositivo. La cuarentena le permite eliminar o restaurar los archivos que se movieron al almacenamiento aislado. `Delete` – La aplicación elimina el archivo detectado. `Skip` – La aplicación deja los objetos detectados sin alterar. Si las amenazas se han omitido, Kaspersky Endpoint Security para Android le advertirá al usuario sobre problemas en la protección del dispositivo. Cuando se produce un intento de acceder a un objeto en el dispositivo (por ejemplo, un intento de copiar o abrirlo), la aplicación bloquea el acceso al objeto. Se registra la información sobre amenazas detectadas y las acciones tomadas sobre ellas en informes de la aplicación.	`Cuarentena`
`ProtectionLock`	Bloquee el ajuste de la configuración de la protección en tiempo real	Boolean	`True` – El usuario no puede acceder a la siguiente configuración de la protección en tiempo real en la configuración de la aplicación: modo de protección en tiempo real, tipos de archivos para analizar, y la acción que se tomará cuando se detecta una amenaza. `False` – El usuario puede ajustar la configuración de la protección en tiempo real y, por ejemplo, seleccionar la acción `Skip` para amenazas detectadas.	`True`
`UpdateScheduleType`	Modo de ejecución de actualización de Bases de datos	Choice	`Daily`: examina nuevas bases de datos antimalware y las descarga a los dispositivos una vez al día. Configure el tiempo del inicio de actualización de la base de datos `(UpdateScheduleTime)`. `Weekly`: examina nuevas bases de datos antimalware y las descarga a dispositivos una vez por semana. Seleccione el día de la semana para iniciar una actualización de la base de datos `(UpdateScheduleDay)` y configurar el tiempo `(UpdateScheduleTime)`. `Off`: se deshabilita la actualización automática de bases de datos antimalware. Independientemente del valor establecido, el usuario puede actualizar manualmente una base de datos antimalware.	`A diario`
`UpdateScheduleDay`	Día para iniciar una actualización de la base de datos	Choice	`Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday` Puede seleccionar solo un valor para este parámetro.	`Monday`
`UpdateScheduleTime`	Tiempo para iniciar la actualización de la base de datos	String	El tiempo se puede indicar en formato de 24 horas (por ejemplo, 13:00) o en formato de 12 horas (por ejemplo, 10:30 p. m.).	`8:00`
`UpdateScheduleLock`	Bloquee la configuración del modo de ejecución de actualización de la base de datos	Boolean	`True` – El usuario no puede acceder a la configuración del modo de ejecución de actualización de la base de datos en la configuración de la aplicación. `False`: el usuario puede configurar el modo de ejecución de actualización de la base de datos y, por ejemplo, deshabilitar el inicio automático de las actualizaciones de la base de datos antimalware.	`True`

Clave de la configuración	Descripción	Tipo	Valor	Valor predeterminado
`AllowUpdateInRoaming`	Actualización de bases de datos en roaming	Boolean	`True`: la aplicación descarga bases de datos antimalware si el dispositivo está en modo roaming. La aplicación descarga bases de datos antimalware según la programación definida (`UpdateScheduleType`). `False`: la aplicación descarga bases de datos antimalware solo si el dispositivo está conectado a la red doméstica.	`False`

`EnableWebFilter`	Protección web	Boolean	`True`: La aplicación usa el componente Protección web para bloquear sitios web maliciosos y de phishing en Internet.
			Protección web en dispositivos Android solo es compatible con Google Chrome, el navegador HUAWEI, Samsung Internet y Yandex Browser.
			Solo se analiza el dominio del sitio web. Si se trata de un dominio malicioso o de phishing, Protección web bloquea la amenaza. Si el dominio no está clasificado como malicioso o como phishing, la URL específica no se bloquea.
			`False` – Se deshabilita la protección contra sitios web phishing y maliciosos.
			Para que el componente Protección web funcione, se deben cumplir las siguientes condiciones:
			• Los usuarios del dispositivo aceptan la Política de privacidad y la Declaración de protección web en el Asistente de configuración inicial o en la configuración de la aplicación.
			• En los dispositivos corporativos, Kaspersky Endpoint Security para Android está habilitado como función de Accesibilidad.
			• En los dispositivos con un contenedor corporativo, se configura un servidor proxy en la configuración del navegador:
			`ProxyMode = "fixed_servers"`
			`ProxyServer = "127.0.0.1:3128"`
			`DisableSpdy = true`
			`DataCompressionProxyEnabled = false`
			La configuración del servidor proxy puede variar según la versión del navegador. Después de que la aplicación Kaspersky Endpoint Security para Android se elimina del dispositivo móvil, reinicie la configuración del servidor proxy.
			• El uso de KSN está activado en la configuración de la aplicación: `UseKsnMode = Recommended` o `UseKsnMode = Extended`.
			• Se recomienda seleccionar Google Chrome, HUAWEI Browser, Samsung Internet Browser o Yandex Browser como navegador predeterminado en la configuración del sistema operativo.
				`False`

`EnableWebFilterLock`	Bloquee la configuración de Protección web	Boolean	`True` – El usuario no puede acceder a la configuración de la Protección web en la configuración de la aplicación. `False`: El usuario puede ajustar la configuración de Protección web y, por ejemplo, deshabilitar la protección contra sitios web maliciosos y de phishing en Internet.	`True`

Clave de la configuración	Descripción	Tipo	Valor	Valor predeterminado
`UpdateServer`	Dirección del servidor fuente de actualizaciones de la base de datos	String	Dirección del servidor que aloja las actualizaciones de la base de datos, por ejemplo, `http://update.server.com`. Si deja el campo en blanco, Kaspersky Endpoint Security para Android usa los servidores de actualización de la base de datos de Kaspersky.	
`AllowGoogleAnalytics`	Enviar datos a los servicios de Google Analytics para Firebase, Firebase Performance Monitoring y Crashlytics	Boolean	`True`: la aplicación envía automáticamente los datos de funcionamiento de Kaspersky Endpoint Security para Android a los servicios de Google Analytics for Firebase, Firebase Performance Monitoring y Crashlytics Estos datos son necesarios para mejorar el funcionamiento de la aplicación y analizar la satisfacción del usuario. Los datos se transfieren a los servicios de Google Analytics para Firebase, Firebase Performance Monitoring y Crashlytics a través de una conexión segura. El acceso a los datos y su protección están regulados por los correspondientes términos de uso de los servicios de Google Analytics para Firebase, Firebase Performance Monitoring y Crashlytics. `False`: se deshabilita el envío de datos a los servicios de Google Analytics para Firebase, Firebase Performance Monitoring y Crashlytics.	`True`
`KscDeviceNameTag`	Etiqueta de nombre de dispositivo para Kaspersky Security Center	String	La etiqueta se agregará al nombre del dispositivo en Kaspersky Security Center. Un espacio separa la etiqueta del nombre del dispositivo. Esto hace que sea más fácil encontrar y ordenar dispositivos en Kaspersky Security Center. • `{DeviceSerialNumber}`: Número de serie del dispositivo. • `{DeviceUid}`: Identificador único del dispositivo (UDID). • `{DeviceAssetNumber}`: Número de activo del dispositivo. Este número se crea internamente dentro de su organización. Puede agregar algunos valores (por ejemplo, `{DeviceSerialNumber} {DeviceUid}`). Recomendamos utilizar únicamente estos valores.	
`KscGroup`	Nombre del grupo de dispositivos	String	Puede especificar grupos de dispositivos en una consola EMM. Cuando un dispositivo se conecta a Kaspersky Security Center, se añadirá automáticamente a una subcarpeta de la carpeta de dispositivos No asignados. El nombre de la subcarpeta coincidirá con el nombre del grupo especificado en este parámetro. Puede crear reglas para mover dispositivos automáticamente de las subcarpetas de la carpeta Dispositivos no asignados a grupos de administración en la sección **Discovery & deployment** > **Deployment & assignment** > **Moving rules**. Si deja el campo en blanco, el dispositivo se agregará automáticamente a la raíz de la carpeta **Unassigned devices**.	`KES10`

Clave de la configuración	Descripción	Tipo	Valor	Valor predeterminado
`KscCorporateEmail`	Correo electrónico corporativo del usuario	Cadena	Puede especificar las direcciones de correo electrónico corporativo de los usuarios en una consola EMM. Estos correos electrónicos se visualizarán en Kaspersky Security Center. La cadena debe ser una dirección de correo electrónico válida. Otros valores no se tienen en cuenta.	
`KscDeviceName`	Nombre del dispositivo en Kaspersky Security Center	Cadena	Puede especificar el nombre de dispositivo que se muestra en Kaspersky Security Center. El valor especificado reemplazará por completo el nombre del dispositivo. Se ignorará el valor establecido en la configuración `KscDeviceNameTag`. Si deja el campo en blanco, el nombre del dispositivo se generará según el formato especificado en la directiva de grupo de Kaspersky Security Center.	

Participación en Kaspersky Security Network

Para proteger dispositivos móviles con mayor eficacia, Kaspersky Endpoint Security para Android y Kaspersky Protection para iOS utilizan datos adquiridos de usuarios de todo el mundo. Kaspersky Security Network está diseñado para procesar esos datos.

Kaspersky Security Network (KSN) es una infraestructura de servicios en la nube que brinda acceso a la base de conocimiento de Kaspersky, que contiene información sobre la reputación de los archivos, recursos web y software. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas de las aplicaciones de Kaspersky frente a amenazas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de falsas alarmas.

Su participación en Kaspersky Security Network ayuda a Kaspersky a reunir información en tiempo real sobre los tipos y las fuentes de las amenazas nuevas, a desarrollar métodos para neutralizarlas y a reducir las falsas alarmas generadas por Kaspersky Endpoint Security para Android y Kaspersky Protection para iOS. Participar en Kaspersky Security Network también le permite acceder a estadísticas de reputación de aplicaciones y sitios web.

Cuando participa en Kaspersky Security Network, algunas estadísticas se obtienen mientras Kaspersky Endpoint Security para Android y Kaspersky Protection para iOS se están ejecutando y se envían automáticamente a Kaspersky. Esta información permite hacer un seguimiento de las amenazas en tiempo real. Los archivos o las partes de los archivos que los intrusos podrían usar para dañar el equipo o el contenido del usuario también se pueden enviar a Kaspersky para realizar exámenes adicionales.

El uso de Kaspersky Security Network se requiere para el funcionamiento de Kaspersky Endpoint Security para Android y Kaspersky Protection para iOS.

Los siguientes componentes de la aplicación utilizan el servicio en la nube de Kaspersky Security Network:

- Los componentes Antimalware, Protección web, Control web y Control de apps en la aplicación Kaspersky Endpoint Security para Android.
- El componente Protección web en la aplicación Kaspersky Protection para iOS.

La negativa a utilizar KSN reduce el nivel de protección del dispositivo, lo cual puede llevar a la infección del dispositivo y la pérdida de datos. Para empezar a usar Kaspersky Security Network, deberá aceptar los términos del Contrato de licencia de usuario final al instalar la aplicación. El Contrato de licencia de usuario final detalla los datos que Kaspersky Endpoint Security para Android y Kaspersky Protection para iOS transmiten a Kaspersky Security Network.

Para mejorar el rendimiento de la aplicación, también podrá proporcionar datos estadísticos a Kaspersky Security Network. Proporcionar a KSN la información indicada anteriormente es de carácter voluntario. Para empezar a usar Kaspersky Security Network, debe aceptar los términos de un contrato especial: la Declaración de Kaspersky Security Network. Puede dejar de participar en Kaspersky Security Network en cualquier momento. La Declaración de Kaspersky Security Network describe los tipos de datos que Kaspersky Endpoint Security para Android y Kaspersky Protection para iOS transmiten a Kaspersky Security Network. Puede usar los servicios de Kaspersky Security Network si el plazo de licencia de la solución integrada no caducó y la clave no se colocó en la lista de claves rechazadas.

La función de actualizaciones (incluido el suministro de actualizaciones de las firmas antimalware y de la base de código) y la función de KSN pueden dejar de estar disponibles en el software en el territorio de EE. UU.

Intercambio de información con Kaspersky Security Network

Intercambio de información en Kaspersky Endpoint Security para Android

Para mejorar la protección en tiempo real, Kaspersky Endpoint Security para Android utiliza el servicio en la nube de Kaspersky Security Network para los siguientes componentes:

- **Antimalware**. La aplicación obtiene acceso a la base de conocimientos de Kaspersky para consultar por la reputación de los archivos y aplicaciones. La aplicación realiza un análisis para detectar amenazas cuya información aún no se agregó a las bases de datos antimalware, pero que ya está disponible en KSN. El servicio en la nube de Kaspersky Security Network proporciona la funcionalidad Antimalware y reduce la posibilidad de falsas alarmas.
- **Protección web y Control web.** La aplicación usa datos recibidos de KSN para analizar sitios web antes de que se abran. La aplicación también determina la categoría del sitio web para controlar el acceso a Internet de usuarios según listas de categorías permitidas y bloqueadas (por ejemplo, la categoría "Internet communication").
- **Control de aplicaciones**. La aplicación determina la categoría de la aplicación para restringir el inicio de las que no cumplan con los requisitos de seguridad corporativa según listas de categorías permitidas y bloqueadas (por ejemplo, la categoría "Games").

La información sobre los tipos de datos enviados a Kaspersky cuando se utiliza KSN durante el funcionamiento de Antimalware y Control de aplicaciones está disponible en el Contrato de licencia de usuario final. Al aceptar los términos y las condiciones del Contrato de licencia, acepta transferir esta información.

La información sobre los tipos de datos enviados a Kaspersky cuando se usa KSN durante el funcionamiento de Protección web y Control web está disponible en la Declaración sobre el procesamiento de datos para Protección web. Al aceptar los términos y las condiciones de la Declaración, acepta transferir esta información.

Para obtener más información acerca de la provisión de datos a KSN, consulte la sección Provisión de datos en Kaspersky Endpoint Security para Android.

El envío de datos a KSN es voluntario. Si lo desea, puede deshabilitar el intercambio de datos con KSN.

Intercambio de información en Kaspersky Protection para iOS

Para mejorar la protección en tiempo real, Kaspersky Protection para iOS utiliza el servicio en la nube de Kaspersky Security Network para los siguientes componentes:

- **Protección web**. La aplicación usa datos recibidos de KSN para analizar sitios web antes de que se abran.

La información sobre los tipos de datos enviados a Kaspersky cuando se utiliza KSN durante el funcionamiento de Protección web está disponible en el Contrato de licencia de usuario final. Al aceptar los términos y las condiciones del Contrato de licencia, acepta transferir esta información.

Para obtener más información acerca de la provisión de datos a KSN, consulte la sección Provisión de datos en Kaspersky Protection para iOS.

El envío de datos a KSN es voluntario. Si lo desea, puede deshabilitar el intercambio de datos con KSN.

Envío de estadísticas a KSN desde aplicaciones de Android o iOS

Con el fin de identificar amenazas emergentes de seguridad de la información, amenazas de intrusión y amenazas difíciles de detectar (junto con sus respectivas fuentes), y de mejorar la protección de la información almacenada y procesada en un dispositivo, puede ampliar su participación en Kaspersky Security Network.

Para intercambiar datos con KSN con el propósito de mejorar el rendimiento de la aplicación, se deben cumplir las condiciones siguientes:

- Usted o el usuario del dispositivo debe leer y aceptar los términos de la Declaración de Kaspersky Security Network. Si elige que los usuarios acepten la Declaración, se les pedirá mediante una notificación en la pantalla principal de la aplicación que acepten los términos de la Declaración. Los usuarios también pueden aceptar las declaraciones en la sección **Acerca de la aplicación** en la configuración de Kaspersky Endpoint Security para Android o Kaspersky Protection para iOS.

- Debe configurar la política de grupos para permitir que se envíen estadísticas a KSN.

Podrá optar por no enviar datos estadísticos a Kaspersky Security Network en cualquier momento. En la Declaración de Kaspersky Security Network encontrará información sobre el tipo de datos estadísticos enviados a Kaspersky al usar KSN durante el funcionamiento de las aplicaciones móviles.

El envío de datos a KSN es voluntario. Si lo desea, puede deshabilitar el intercambio de datos con KSN.

Habilitación y deshabilitación del uso de Kaspersky Security Network

Para el funcionamiento de los componentes de Kaspersky Endpoint Security para Android y Kaspersky Protection para iOS que utilizan Kaspersky Security Network, la aplicación envía solicitudes a los servicios en la nube. Las solicitudes contienen los datos descritos en las secciones Provisión de datos en Kaspersky Endpoint Security para Android y Provisión de datos en Kaspersky Protection para iOS, respectivamente.

Si se deshabilita el uso de Kaspersky Security Network en el dispositivo, los componentes Antimalware, Protección web, Control web y Control de aplicaciones se deshabilitan automáticamente.

Para habilitar o deshabilitar el uso de Kaspersky Security Network para dispositivos Android, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **Android** y vaya a la sección **KES for Android settings**.
4. En la tarjeta **Kaspersky Security Network**, haga clic en **Settings**.

   Se abre la ventana **Kaspersky Security Network**.
5. Habilite el interruptor **Kaspersky Security Network** para los siguientes componentes: Antimalware, Protección web, Control web y Control de aplicaciones.
6. En la sección **KSN Proxy**, seleccione la casilla **Switch to using public Kaspersky Security Network servers if KSN Proxy is not available** si es necesario.
7. Haga clic en **Aceptar**.
8. En la tarjeta **Sending additional data**, haga clic en **Settings**.
9. En la sección **Sending data to Kaspersky Security Network**, seleccione la casilla **Allow sending statistics to Kaspersky Security Network** para enviar datos a Kaspersky.

   Estos datos ayudarán a que la aplicación Kaspersky Endpoint Security para Android responda con mayor rapidez a amenazas, mejore el rendimiento de componentes de protección y disminuya la posibilidad de falsas alarmas.
10. En la sección **Sending data for marketing purposes**, seleccione la casilla **Allow data processing to help improve the quality, appearance, and performance of the app** a fin de mejorar la calidad, la apariencia y el rendimiento del Software, los productos, los servicios y la infraestructura del Titular de los derechos al analizar la experiencia de los usuarios, las funciones que utilizan y el estado y la configuración del dispositivo.

11. Seleccione quién debe aceptar las Declaraciones:

    - Si selecciona **Statements are accepted by administrator**, se le pedirá que acepte las declaraciones en la ventana que se abre.

    - Si selecciona **Statements are accepted by users**, se le pedirá al usuario del dispositivo que las acepte.

12. Haga clic en **Aceptar**.

13. Haga clic en el botón **Save** para guardar los cambios que realizó.

    La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Para habilitar o deshabilitar el uso de Kaspersky Security Network para dispositivos iOS:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **iOS** y vaya a la sección **KP for iOS settings**.

4. Habilite el interruptor de la tarjeta **Kaspersky Security Network** para el componente Protección web.

5. En la tarjeta **Sending additional data**, haga clic en **Settings**.

6. En la sección **Sending data to Kaspersky Security Network**, seleccione la casilla **Allow sending statistics to Kaspersky Security Network** para enviar datos a Kaspersky.

   Estos datos ayudarán a que la aplicación Kaspersky Endpoint Security para iOS responda con mayor rapidez a amenazas, mejore el rendimiento de componentes de protección y disminuya la posibilidad de falsas alarmas.

7. Seleccione quién debe aceptar las Declaraciones:

    - Si selecciona **Statements are accepted by administrator**, se le pedirá que acepte las declaraciones en la ventana que se abre.

    - Si selecciona **Statements are accepted by users**, se le pedirá al usuario del dispositivo que las acepte.

8. Haga clic en **Aceptar**.

9. Haga clic en el botón **Save** para guardar los cambios que realizó.

   La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Uso de Kaspersky Private Security Network

Kaspersky Private Security Network (en lo sucesivo, denominado *KPSN)* es una solución que otorga acceso a las bases de datos de reputación de Kaspersky Security Network (KSN), sin enviar datos a Kaspersky Security Network desde los dispositivos de los usuarios.

Una base de datos de reputación de objetos (archivos o URL) se almacena en el servidor de Kaspersky Private Security Network, pero no en los servidores de Kaspersky Security Network. Las bases de datos de reputación de KPSN se almacenan dentro de la red corporativa y son administradas por el administrador de la empresa.

Cuando KPSN está habilitado, Kaspersky Endpoint Security para Android no envía ningún dato estadístico a KSN desde los dispositivos de los usuarios.

KPSN solo se aplica a los dispositivos Android administrados por Kaspersky Endpoint Security para Android. Kaspersky Protection para iOS continúa enviando datos estadísticos a KSN desde los dispositivos de los usuarios.

Para habilitar el uso de KPSN a través de Kaspersky Security Center:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), haga clic en el nombre del Servidor de administración.
2. En la ventana de propiedades del Servidor de administración que se abre, en la pestaña **General**, seleccione la sección **KSN settings**.
3. Cambie el botón de alternancia **Use Kaspersky Private Security Network Enabled** a la posición Habilitado.
4. Haga clic en el botón **Select file with KSN Proxy settings** y luego busque un archivo de configuración que tenga la extensión PKCS7 o PEM (proporcionado por Kaspersky).
5. Haga clic en **Abrir**.
6. Si definió la configuración del servidor proxy en las propiedades del Servidor de administración, pero la arquitectura de su red requiere que use KPSN directamente, habilite la opción **Ignore proxy server settings when connecting to KPSN**. De lo contrario, las solicitudes de las aplicaciones administradas no pueden llegar a la KPSN.
7. Haga clic en el botón **Save** para guardar los cambios que realizó.

Después de descargar la configuración, la interfaz muestra el nombre y los contactos del proveedor, así como la fecha de creación del archivo con la configuración de la KPSN. La configuración de KPSN se aplica a los dispositivos móviles.

Cuando cambia a KPSN, Control de apps no es compatible con las categorías de aplicaciones disponibles cuando usa KSN. La categorización de aplicaciones estará disponible si elige volver a KSN.

Si los dispositivos móviles están conectados a Kaspersky Security Center a través de la puerta de enlace de conexión, el proxy de KSN no funciona. En este caso, deshabilite el interruptor **Enable KSN Proxy on Administration Server Enabled** en la sección **KSN Proxy** de la ventana de propiedades del Servidor de administración. Para obtener información detallada sobre cómo habilitar y deshabilitar el uso del proxy de KSN, consulte la Ayuda de Kaspersky Security Center.

Samsung Knox

Samsung Knox es una solución móvil para configurar y desplegar dispositivos móviles Samsung que utilizan el sistema operativo Android. Para obtener más información sobre Samsung Knox, visite el sitio web del servicio de soporte técnico de Samsung.

Instalación de Kaspersky Endpoint Security para Android a través de Knox Mobile Enrollment

Knox Mobile Enrollment (KME) es parte de la solución móvil de Samsung Knox. Se utiliza para la instalación por lotes y la configuración inicial de aplicaciones en dispositivos Samsung nuevos.

La instalación de Kaspersky Endpoint Security para Android mediante Knox Mobile Enrollment consiste en los siguientes pasos:

1. **Crear un perfil de Knox con la aplicación Kaspersky Endpoint Security para Android**
2. **Agregar dispositivos a Knox Mobile Enrollment**
3. **Instalar la aplicación Kaspersky Endpoint Security para Android en los dispositivos móviles del usuario**

Para obtener más información sobre el uso de Knox Mobile Enrollment, consulte la Guía del usuario de Knox Mobile Enrollment.

El despliegue a través de Knox Mobile Enrollment solo es posible para dispositivos Samsung compatibles.

Crear un perfil de Knox

Un *perfil Knox* es un perfil que contiene vínculos a aplicaciones para una rápida instalación y configuración inicial en dispositivos móviles.

Para crear un perfil Knox, siga estos pasos:

1. Inicie sesión en la consola Samsung Knox → **Knox Mobile Enrollment**.
2. Seleccione la sección **Perfiles**.
3. Haga clic en **Acciones** > **Crear perfil**.

   Se inicia el asistente Crear nuevo perfil.
4. Seleccione **Android Enterprise** como tipo de perfil.
5. En la ventana **Detalles del perfil empresarial de Android** que se abre, especifique la siguiente configuración:
   a. En la sección **Información básica**, ingrese información general sobre el perfil de Knox: **Nombre de perfil** y **Descripción**.
   b. En la sección **Información de EMM**, en el campo **Elija su EMM**, seleccione **Otro**.

c. En el campo **APK del agente de EMM**, ingrese la ruta al archivo de instalación de APK.

El archivo de instalación de Kaspersky Endpoint Security para Android se incluye en el kit de distribución de MDM básico en Kaspersky Next Expert View (on-premise). Primero, descargue el archivo de instalación APK. Luego, coloque el archivo de instalación APK en el Servidor web de Kaspersky Security Center o en otro servidor que sea accesible para descargar desde el dispositivo.

6. Haga clic en **Continuar**.

7. En la ventana **Configuración del perfil empresarial de Android** que se abre, especifique la siguiente configuración:

a. En la sección **Configuración de EMM**, ingrese la configuración para conectar el dispositivo a Kaspersky Security Center en el campo **Datos JSON personalizados (según lo definido por EMM)** en el siguiente formato:

b. `{"serverAddress":"myServer.domain.com","serverPort":"12345","vsrv":"virtualServerID",GROUP","eulas":"cmFuZG9tYmFzZTY0c3RyaW5n"}`.

Los siguientes campos del archivo JSON ahora son compatibles:

- `serverAddress`: la dirección de Kaspersky Security Center.
- `serverPort`: el número del puerto para la sincronización del dispositivo móvil con el Servidor de administración a través de la dirección especificada.
- `vsrv` (opcional): el Servidor de administración virtual.
- `groupName` (opcional): el nombre del subgrupo del grupo No asignado.
- `eulas` (opcional): la lista de EULA aceptados (una matriz de identificadores binarios, de 16 bytes).

> El parámetro `connectionString` ya no es compatible con KME (Knox Mobile Enrollment).

c. Para instalar Kaspersky Endpoint Security para Android mediante la Knox Mobile Enrollment, el usuario del dispositivo móvil debe aceptar las condiciones del Contrato de licencia de Samsung. Puede ver los términos del Contrato de licencia de Samsung en la sección **Política de privacidad, EULA y Condiciones de servicio**. También puede agregar otros documentos legales de su empresa que sean necesarios para desplegar un perfil de Knox haciendo clic en el botón **Agregar contrato legal**.

8. Haga clic en el botón **Guardar**.

Por lo tanto, se agregará el nuevo perfil de Knox con la aplicación Kaspersky Endpoint Security para Android a la lista en la consola KME.

Agregar dispositivos a Knox Mobile Enrollment

Los dispositivos se pueden agregar en la consola Knox Mobile Enrollment (KME) de los siguientes modos:

- El proveedor automáticamente agrega dispositivos a la consola KME después de que los dispositivos se compran.
- El administrador instala la aplicación Knox Deployment desde Google Play en su dispositivo móvil y migra el perfil Knox a los dispositivos de los usuarios mediante Bluetooth, Wi-Fi Direct o un código QR.

Una vez que el dispositivo se restablezca a los ajustes de fábrica, se instalará el perfil Knox. Después de la instalación del perfil de Knox, el dispositivo se agregará automáticamente a la consola KME.

Agregar un dispositivo a través de la aplicación Knox Deployment

Si no compró su dispositivo Samsung a un proveedor oficial, puede agregar el dispositivo a Knox Mobile Enrollment mediante Bluetooth, Wi-Fi Direct o un código QR. Esto requerirá el dispositivo móvil del administrador que será usado para entregar perfiles de Knox a los dispositivos móviles de los usuarios.

Para agregar dispositivos usando la aplicación Knox Deployment, se deben cumplir las siguientes condiciones:

- Según el modo de entrega seleccionado, se debe habilitar Bluetooth o Wi-Fi en los dispositivos móviles.
- Los dispositivos móviles deben estar conectados a Internet.

Para entregar un perfil de Knox usando la aplicación Knox Deployment, siga estos pasos:

1. Instale la aplicación Knox Deployment desde Google Play en el dispositivo móvil principal del administrador.
2. Abra la aplicación Knox Deployment.
3. Ingrese las credenciales de su cuenta Samsung para iniciar sesión.
4. En la ventana **Knox Deployment**, ajuste la configuración para instalar un perfil de Knox:
   a. En la sección **Servicios de Knox**, seleccione **Knox Mobile Enrollment**.
   b. Seleccione el perfil de Knox deseado de la lista.
   c. Seleccione el **modo de despliegue**:
      - **Bluetooth**. Establezca la duración de la conexión Bluetooth y especifique si la conexión Bluetooth es automática o manual.

        Al usar Bluetooth, puede agregar un perfil de Knox a varios dispositivos al mismo tiempo.
      - **Wi-Fi Direct**. Especifique si la conexión Wi-Fi Direct es automática o manual. Luego, siga las instrucciones en la pantalla.
   d. Toque **Iniciar despliegue**.
5. En el dispositivo receptor, dibuje un signo más (+) en la ventana de **bienvenida** para iniciar el despliegue.
6. En el menú **Knox Deployment** que se abre, seleccione si desea usar Bluetooth o Wi-Fi Direct para inscribir un dispositivo:
   a. Si seleccionó **Bluetooth**, apruebe la solicitud de emparejamiento que aparece en el dispositivo principal. Luego, el dispositivo receptor descarga el perfil. Siga las instrucciones en la pantalla.

      Una vez que se haya instalado el perfil de Knox, el nuevo dispositivo se agregará con la etiqueta **Bluetooth** a la consola KME.

b. Si seleccionó **Wi-Fi Direct**, siga las instrucciones en pantalla.

Después de instalar el perfil de Knox, el nuevo dispositivo se agregará con la etiqueta **Wi-Fi** a la consola KME.

7. Cuando el dispositivo receptor esté configurado, toque **Finalizar despliegue** en el dispositivo principal para completar la inscripción.

Una vez que el dispositivo se restablezca a los ajustes de fábrica, se instalará el perfil Knox.

Para entregar un perfil Knox mediante un código QR, siga estos pasos:

1. En el dispositivo receptor, dibuje un signo más (+) en la ventana de **bienvenida** para iniciar el despliegue.
2. En el menú **Knox Deployment** que se abre, seleccione **Código QR**.
3. En la Consola de KME, seleccione el perfil deseado en la sección **Perfiles**.
4. Si no hay un código QR junto al nombre del perfil, abra la configuración del perfil y haga clic en el botón **Agregar un código QR** en la segunda página.
5. Siga las instrucciones en pantalla y guarde el perfil.

   El código QR generado aparece cerca del nombre del perfil.
6. Escanee un código QR desde la Consola de KME con la cámara del dispositivo Android del usuario con la versión Android 10 o posterior.

   Después de que se instale el perfil Knox, se agregará el dispositivo nuevo con la etiqueta **Código QR** a la Consola de KME.

Una vez que el dispositivo se restablezca a los ajustes de fábrica, se instalará el perfil Knox.

Agregar un dispositivo a través del proveedor

Los proveedores oficiales de dispositivos Samsung pueden registrarse en Samsung Knox. Para ver la lista de proveedores oficiales, visite el sitio web del servicio de soporte técnico de Samsung. El proveedor automáticamente agrega los dispositivos en la consola de KME para su cuenta de Samsung inmediatamente después de que los dispositivos se compran. Para que el proveedor agregue los dispositivos, debe registrar al proveedor en la consola KME para su cuenta de Samsung. Necesitará un ID de revendedor para agregar al proveedor de dispositivos Samsung en la Consola de KME. Para recibir el ID del revendedor, debe enviar una solicitud al proveedor. En la solicitud, especifique su ID del cliente Knox.

Para ver su ID de cliente Knox, siga estos pasos:

1. Inicie sesión en la consola Samsung Knox → **Knox Mobile Enrollment**.
2. Seleccione la sección **Revendedores**.
3. Su ID se muestra en el campo **ID de cliente Knox**.

Después de que reciba una respuesta del proveedor con el ID del revendedor, registre al proveedor en la consola KME. Antes del registro del proveedor, puede crear un perfil Knox de modo que el perfil se pueda implementar automáticamente al agregar dispositivos nuevos.

Registrar a un proveedor oficial en la consola KME:

1. Inicie sesión en la consola Samsung Knox → **Knox Mobile Enrollment**.
2. Seleccione la sección **Revendedores**.
3. Haga clic en el botón **Registrar revendedor**.

   Se abre la ventana para registrar al proveedor del dispositivo.
4. En el campo **ID de revendedor**, ingrese el ID recibido del proveedor oficial de dispositivos de Samsung.
5. Si creó un perfil Knox, seleccione el perfil Knox en la ventana de registro del proveedor.

   Cuando agrega dispositivos nuevos, el perfil Knox se instala en forma automática.

   Para obtener más información sobre cómo configurar otros ajustes, consulte el sitio web del servicio de soporte técnico de Samsung.
6. Haga clic en **Aceptar**.

El proveedor de dispositivos de Samsung se agregará a la lista de proveedores en la Consola de KME.

Luego de que se compran dispositivos nuevos al proveedor oficial, Kaspersky Endpoint Security para Android se instalará automáticamente en los dispositivos después de que estos se conecten a Internet. Para obtener más información sobre el uso de Knox Mobile Enrollment, consulte la Guía del usuario de Knox Mobile Enrollment. Si ya tiene una lista de dispositivos en la Consola de KME, agregue el perfil Knox con la aplicación de Knox al dispositivo.

Instalar la aplicación

Antes de instalar Kaspersky Endpoint Security para Android, emita un certificado para dispositivos móviles para los usuarios de dispositivos móviles en Kaspersky Next Expert View (on-premise). Se requiere un certificado para dispositivos móviles para identificar al usuario del dispositivo móvil en Kaspersky Next Expert View (on-premise).

Para entregar un perfil Knox a dispositivos, siga estos pasos:

1. Inicie sesión en la consola Samsung Knox → **Knox Mobile Enrollment**.
2. Seleccione **Dispositivos** → **Todos los dispositivos**.
3. Seleccione los dispositivos en los cuales desea instalar el perfil Knox.

   Se abre la ventana **Información del dispositivo**.
4. En la lista **Perfiles**, seleccione el perfil Knox con Kaspersky Endpoint Security para Android.
5. En el campo **Etiquetas**, escriba etiquetas para agrupar y poner etiqueta a dispositivos, y para la optimización de búsqueda en la consola KME.
6. Ingrese las credenciales de la cuenta de usuario del dispositivo en los campos **Contraseña** e **ID de usuario**.

   Se requieren credenciales de cuenta para recibir un certificado para dispositivos móviles. El ID de usuario y la contraseña deben coincidir con las credenciales de la cuenta de usuario en Kaspersky Security Center (**Nombre** y **Contraseña** en propiedades de la cuenta de usuario).

Para recibir un certificado móvil solo con una contraseña y sin un nombre de usuario, ingrese el valor "DO_NOT_USE_LOGIN" en el campo **ID de usuario**. Kaspersky Endpoint Security para Android no utilizará el nombre de usuario para solicitar un certificado.

7. Seleccione el perfil Knox para los dispositivos restantes.
8. Haga clic en el botón **Guardar**.

Una vez que el dispositivo se restablezca a los ajustes de fábrica, se instalará el perfil Knox.

Después de iniciar la instalación del perfil Knox, el archivo de instalación APK se descargará en forma automática en el dispositivo móvil. Se inicia la instalación de Kaspersky Endpoint Security para Android automáticamente. No se requiere ninguna configuración adicional de la aplicación. Una vez que se haya realizado la configuración inicial del dispositivo y se haya instalado la aplicación, la sincronización con Kaspersky Security Center se realizará automáticamente. El dispositivo móvil se agregará a Kaspersky Next Expert View (on-premise).

Configurar Knox

Esta sección contiene información sobre cómo trabajar con Knox en dispositivos Samsung.

Knox solo está disponible en dispositivos Samsung que ejecutan Android 6 o versiones posteriores.

Configurar una VPN en KNOX

Para conectar de forma segura un dispositivo Android a Internet y proteger la transferencia de datos, puede configurar los ajustes de la VPN (red privada virtual).

La configuración de VPN solo es posible para dispositivos Samsung que ejecutan Android 11 o versiones anteriores.

Los siguientes requisitos se deben tener en cuenta cuando se utiliza una red privada virtual:

- La aplicación que usa la conexión VPN debe estar permitida en la configuración del **Firewall**.
- Las opciones de la VPN configuradas en la directiva no pueden aplicarse a las aplicaciones del sistema. La conexión VPN para las aplicaciones del sistema debe configurarse manualmente.
- Para algunas aplicaciones que utilizan una conexión VPN, se deben configurar opciones adicionales en el primer inicio. Para configurar opciones, una conexión VPN debe estar permitida en las opciones de la aplicación.

Para configurar la VPN en un dispositivo móvil del usuario:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **Android** y vaya a la sección **Samsung Knox settings**.

4. En la tarjeta **VPN**, haga clic en **Settings**.

   Se abre la ventana **VPN**.

5. Habilite la configuración con el interruptor **VPN**.

6. Especifique la siguiente configuración para la VPN:

   - Ajustes de la sección **Network**:

     - En el campo **Network name**, escriba el nombre del túnel VPN.

     - En la lista desplegable **Protocol**, seleccione el tipo de conexión VPN:

       - **IPSec Xauth PSK**. Un protocolo de túnel entre puertas de enlace que permite al usuario del dispositivo móvil establecer una conexión segura con el servidor VPN por medio de la utilidad de autenticación Xauth.

       - **L2TP IPSec PSK**. Un protocolo de túnel entre puertas de enlace que permite al usuario del dispositivo móvil establecer una conexión segura con el servidor VPN mediante el protocolo IKE usando una clave predefinida. Este protocolo está seleccionado de manera predeterminada.

       - **PPTP**. Un protocolo de túnel punto a punto que permite al usuario del dispositivo móvil establecer una conexión segura con el servidor VPN creando un túnel especial en una red estándar sin protección.

     - En el campo **Dirección del servidor**, escriba el nombre de la red o la dirección IP del servidor VPN.

   - Ajustes de la sección **Protocol settings**:

     - En la lista **DNS search domain(s)**, escriba el dominio de búsqueda DNS que se agregará automáticamente al nombre del servidor DNS.

       Puede especificar varios dominios DNS separándolos con espacios en blanco.

     - En el campo **DNS server(s)**, escriba el nombre completo del dominio o de la dirección IP del servidor DNS.

       Se pueden especificar varios servidores DNS separados con espacios en blanco.

     - En el campo **Routing**, escriba el rango de direcciones IP dentro del cual se intercambia información a través de la conexión VPN.

       > Si el rango de direcciones IP no está especificado en el campo **Routing**, todo el tráfico de Internet pasa a través de la conexión VPN.

7. Además, configure los siguientes parámetros:

   - Para los protocolos **IPSec Xauth PSK** y **L2TP IPSec PSK**:

     - En el campo **IPSec shared key**, escriba la contraseña de la clave de seguridad preestablecida IPSec.

     - En el campo **IPSec ID**, escriba el nombre del usuario del dispositivo móvil.

- Para el protocolo **L2TP IPSec PSK**, además puede especificar la contraseña para la clave L2TP en el campo **L2TP key**.
- Para la red **PPTP**, seleccione la casilla **Use SSL connection** para que la aplicación utilice el método MPPE (Microsoft Point-to-Point Encryption) de cifrado de datos para proteger la transmisión de información cuando el dispositivo móvil se conecta al servidor VPN.

8. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Configurar un buzón de correo de Exchange en Knox

Para trabajar con el calendario, el correo y los contactos corporativos en el dispositivo móvil, puede ajustar la configuración del buzón de correo de Exchange para la aplicación de correo electrónico estándar de Samsung.

Un buzón de correo de Exchange solo se puede configurar para dispositivos Samsung con Android 9 o versiones anteriores.

Para configurar un buzón de correo de Exchange en el dispositivo móvil de un usuario, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Seleccione **Android** y vaya a la sección **Samsung Knox settings**.
4. En la tarjeta **Exchange ActiveSync**, haga clic en **Settings**.

   Se abre la ventana **Exchange ActiveSync**.
5. Habilite la configuración con el interruptor **Exchange ActiveSync**.
6. En el campo **Server address**, escriba la dirección IP o el nombre DNS del servidor que aloja al servidor de correo.
7. En el campo **Domain name**, escriba el nombre de dominio del usuario del dispositivo móvil en la red corporativa.
8. En la lista desplegable **Synchronization interval**, seleccione el intervalo que desee para la sincronización del dispositivo móvil con el servidor Microsoft Exchange.
9. Para usar el protocolo SSL (Secure Sockets Layer) de transporte de datos, seleccione la casilla **Use SSL connection**. El protocolo SSL utiliza cifrado y autenticación basada en certificados para la transferencia de datos segura. Esta casilla está marcada por defecto.

10. Para usar certificados digitales para proteger la transferencia de datos entre el dispositivo móvil y el servidor Microsoft Exchange, seleccione la casilla **Verify server certificate**. Se verifica que el certificado del servidor se haya emitido a partir del certificado raíz de confianza. Esta casilla está marcada por defecto.

11. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Configurar una APN en Knox

APN solo se puede configurar para dispositivos Samsung.

Debe insertar una tarjeta SIM para poder utilizar un punto de acceso en el dispositivo móvil del usuario. La operadora de telefonía móvil proporciona la configuración de punto de acceso. Si la configuración del punto de acceso es incorrecta, es posible que genere cargos adicionales de datos móviles.

Para configurar el nombre del punto de acceso (APN) del dispositivo móvil de un usuario, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **Android** y vaya a la sección **Samsung Knox settings**.

4. En la tarjeta **APN settings**, haga clic en **Settings**.

   Se abre la ventana **APN settings**.

5. Habilite la configuración con el interruptor **APN settings**.

   El interruptor de esta tarjeta no habilita ni deshabilita la funcionalidad correspondiente en los dispositivos. Habilitar el interruptor le permite utilizar configuraciones personalizadas. Deshabilitar el interruptor le permite usar la configuración predeterminada.

6. Especifique la siguiente configuración del punto de acceso para conectar al usuario al servicio de datos:

   - En la lista desplegable **APN type**, seleccione el tipo de punto de acceso (APN) para la transmisión de datos en una red móvil GPRS/3G/4G:

     - **Internet**. Conexión del dispositivo móvil del usuario a Internet.

     - **MMS**. Intercambio de mensajes multimedia MMS.

     - **Internet and MMS**. Conexión a Internet e intercambio de mensajes multimedia. Este es el valor predeterminado.

   - En el campo **APN name**, especifique el nombre del punto de acceso.

- En el campo **MCC**, ingrese el código de país de móvil (MCC).
- En el campo **MNC**, ingrese el código de operador de móvil (MNC).

7. Si seleccionó **MMS** o **Internet and MMS** como el tipo de punto de acceso, especifique las siguientes opciones adicionales del servidor de MMS en la sección **MMS server**:
   - En el campo **MMS server name**, especifique el nombre de dominio completo del servidor de la empresa de telefonía móvil que se utiliza para intercambiar MMS (por ejemplo, `mms.mobile.com`).
   - En el campo **MMS proxy server address**, especifique el nombre de la red o la dirección IP del servidor proxy.
   - En el campo **MMS proxy server port**, especifique el número de puerto del servidor de la empresa de telefonía móvil que se utiliza para intercambiar MMS.
8. En la sección **Authentication**, especifique la siguiente configuración de autenticación:
   - En la lista desplegable **Authentication type**, seleccione el tipo de autenticación del usuario del dispositivo móvil que se utiliza en el servidor de la empresa de telefonía móvil para acceder a la red. De forma predeterminada, no se requiere la autenticación del usuario. Están disponibles los siguientes tipos:
     - **None**. No se requiere autenticación de usuario para acceder a la red móvil.
     - **PAP** (Password Authentication Protocol). Un protocolo de autenticación que utiliza contraseñas como texto no cifrado.
     - **CHAP** (Challenge Handshake Authentication Protocol). Un protocolo de autenticación de solicitud-respuesta que utiliza hashing MD5 estándar para cifrar la respuesta.
     - **Concurrently**. Uso combinado de los protocolos CHAP y PAP.
   - En el campo **User name**, escriba el nombre usuario para la autorización en la red móvil.
   - En el campo **Password**, escriba la contraseña para la autorización del usuario en la red móvil.
9. En la sección **Network**, especifique la siguiente configuración de la red:
   - En el campo **Network name**, escriba el nombre de la red.
   - En el campo **Server address**, especifique el nombre de la red del servidor de la empresa de telefonía móvil a través del cual se accede a los servicios de transmisión de datos.
10. En la sección **Proxy server**, especifique la siguiente configuración del servidor proxy:
    - Seleccione la casilla **Use a proxy server** para habilitar el uso de un servidor proxy. Esta casilla está desactivada por defecto.
    - En el campo **Proxy server address**, especifique el nombre de la red o la dirección IP del servidor proxy de la empresa de telefonía móvil que se utiliza para acceder a la red. Este campo está disponible solo si la casilla **Use a proxy server** está marcada.
    - En el campo **Proxy server port**, especifique el número de puerto del servidor proxy de la empresa de telefonía móvil que se utiliza para acceder a la red. Este campo está disponible solo si la casilla **Use a proxy server** está marcada.

11. Haga clic en **Aceptar**.

12. Haga clic en el botón **Save** para guardar los cambios que realizó.

    La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Configurar un firewall en Knox

Configure las opciones del firewall para controlar las conexiones a la red en el dispositivo móvil del usuario.

El firewall solo se puede configurar para dispositivos Samsung que operan en los siguientes modos:

- dispositivo corporativo
- dispositivo personal con Android 15 o anterior
- dispositivo con contenedor corporativo con Android 15 o anterior

Para configurar el firewall en el dispositivo móvil de un usuario, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

2. En la ventana de propiedades de la directiva, seleccione **Application settings**.

3. Seleccione **Android** y vaya a la sección **Samsung Knox settings**.

4. En la tarjeta **Firewall**, haga clic en **Settings**.

   Se abre la ventana **Firewall**.

5. Habilite la configuración con el interruptor **Firewall**.

6. En la lista desplegable **Internet access**, seleccione el modo Firewall. Según el modo de funcionamiento, el firewall supervisa las conexiones establecidas por el dispositivo móvil del usuario:

   - Si desea permitir las conexiones entrantes y salientes de todas las aplicaciones instaladas, seleccione **Allow for all apps**. Este modo está seleccionado de forma predeterminada.
   - Si desea bloquear toda la actividad de la red, excepto varias aplicaciones especificadas, seleccione **Allow for listed apps**.

7. Si seleccionó **Allow for listed apps** como el modo del firewall, cree una lista de aplicaciones para las que se permite toda la actividad de red:

   a. En la sección **Apps with internet access**, haga clic en **Add**.

      Se abre la ventana **Add app**.

   b. En el campo **App name**, escriba el nombre de una aplicación móvil.

c. En el campo **Package name**, escriba el nombre del sistema del paquete de la aplicación móvil (por ejemplo, `com.mobileapp.example`).

d. Haga clic en **Agregar**.

La nueva aplicación para la que se deshabilita el firewall aparece en la lista.

Puede modificar o eliminar redes aplicaciones móviles en la lista con los botones **Edit** y **Delete** que se encuentran en la parte superior de la lista.

8. Haga clic en **Aceptar**.

9. Haga clic en el botón **Save** para guardar los cambios que realizó.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con Kaspersky Security Center.

Uso de la aplicación Kaspersky Endpoint Security para Android

Esta sección de Ayuda describe las funciones y operaciones que están disponibles para los usuarios de la app Kaspersky Endpoint Security para Android.

Los artículos de esta sección incluyen todas las opciones que pueden estar visibles o disponibles en un dispositivo móvil. El diseño y el comportamiento de la aplicación se establecen en función del sistema de administración remota implementado y de cómo el administrador configure su dispositivo según los requisitos de seguridad corporativa. Es posible que algunas de las funciones y opciones que se describen en esta sección no se apliquen a su experiencia real con la aplicación. Si tiene alguna pregunta sobre la aplicación instalada en un dispositivo específico, comuníquese con su administrador.

Funciones de la aplicación

Kaspersky Endpoint Security ofrece las siguientes funciones clave.

Protección contra virus y otro software malicioso

La aplicación utiliza el componente Antimalware para proteger el dispositivo contra virus y otro malware.

El componente Antimalware realiza las siguientes funciones:

- Analiza el dispositivo completo, las aplicaciones instaladas o las carpetas seleccionadas en busca de amenazas
- Protege el dispositivo en tiempo real
- Analiza las aplicaciones recién instaladas antes de que se inicien por primera vez
- Actualiza las bases de datos antimalware

Si una aplicación que recopila la información y la envía para procesarse se instala en un dispositivo móvil, Kaspersky Endpoint Security para Android puede clasificarla como software malicioso.

Protección de datos de dispositivos robados o perdidos

El componente Antirrobo protege los datos contra el acceso no autorizado y ayuda a localizar el dispositivo en caso de pérdida o robo.

El componente Antirrobo permite realizar las siguientes operaciones de manera remota:

- Bloquear dispositivo.

  Para impedir que un atacante pueda desbloquear el dispositivo, Kaspersky Endpoint Security debe estar habilitado como un servicio de accesibilidad en dispositivos móviles con Android 7 o versiones posteriores.

- Activar una alarma sonora en el dispositivo, incluso si el sonido del dispositivo está deshabilitado.
- Obtener las coordenadas de la ubicación del dispositivo.
- Borrar los datos almacenados en el dispositivo.
- Restablecer ajustes de fábrica.
- Tomar, de forma secreta, una foto de la persona que está utilizando el dispositivo.

Para habilitar operaciones antirrobo, Kaspersky Endpoint Security debe estar habilitado como administrador del dispositivo. Si no concediera derechos de administrador del dispositivo durante la configuración inicial de aplicaciones, puede conceder derechos de administrador a Kaspersky Endpoint Security mediante la notificación apropiada o en la configuración del dispositivo (**Configuración de Android** → **Seguridad** → **Administradores del dispositivo**).

Protección contra amenazas en línea

El componente Protección web ofrece protección contra amenazas en línea.

El componente Protección web bloquea los sitios web maliciosos que distribuyen un código malicioso y los sitios web de phishing diseñados para robar sus datos confidenciales y acceder a sus cuentas financieras. Protección web analiza los sitios web antes de abrirlos mediante el servicio en la nube de Kaspersky Security Network. Más información.

Control de apps

De acuerdo a los requisitos de seguridad corporativa, el *administrador del sistema de administración remota* (en adelante "administrador") crea listas de las aplicaciones recomendadas, prohibidas y requeridas. El componente Control de aplicaciones se utiliza para instalar aplicaciones recomendadas y requeridas, para actualizarlas y para eliminar aplicaciones prohibidas.

El componente Control de apps permite instalar aplicaciones recomendadas y requeridas en el dispositivo por medio de un vínculo directo al paquete de distribución o de un vínculo a Google Play. El componente Control de aplicaciones permite eliminar aplicaciones prohibidas que infrinjan los requisitos de seguridad corporativa.

Kaspersky Endpoint Security debe estar habilitado como un servicio de accesibilidad para garantizar el correcto funcionamiento de Control de apps. Si no habilitó este servicio durante el Asistente de configuración inicial de la aplicación, puede habilitar Kaspersky Endpoint Security como un servicio de accesibilidad mediante la notificación correspondiente o en la configuración del dispositivo (**Configuración de Android** → **Accesibilidad** → **Servicios**).

Control de cumplimiento

El componente Control de cumplimiento revisa de forma automática si el dispositivo cumple los requisitos de seguridad corporativa. Si el dispositivo no cumple con los requisitos corporativos de seguridad, la aplicación muestra una notificación con la siguiente información:

- Motivo de la falta de cumplimiento (por ejemplo, se detectaron aplicaciones prohibidas en el dispositivo o las bases de datos antimalware están desactualizadas).
- Período de tiempo en el cual debe eliminar el incumplimiento (por ejemplo, 24 horas).
- Acción que se llevará a cabo en el dispositivo si no se elimina el incumplimiento dentro del período de tiempo especificado (por ejemplo, se bloqueará el dispositivo).
- Acción realizada para solucionar el incumplimiento con los requisitos de seguridad corporativa del dispositivo.

Ventana principal de un vistazo

La apariencia de la ventana principal apenas difiere según las diferentes resoluciones de pantalla.

La ventana principal muestra el estado de protección general del dispositivo. El estado determina el color de la ventana:

- Verde indica que la protección del dispositivo es óptima.
- Rojo indica problemas graves respecto de la seguridad del dispositivo.

En la ventana principal de la aplicación, también puede hacer lo siguiente:

- Ver notificaciones haciendo clic en el botón, en la esquina superior derecha. Estas notificaciones tendrán información sobre problemas de seguridad, problemas en el funcionamiento de la aplicación, el cumplimiento de requisitos corporativos de seguridad y su licencia.
- Navegue entre la ventana principal y la configuración de la aplicación con los botones ubicados en la parte inferior.

Icono de la barra de estado

Al finalizar el asistente en el primer inicio, el icono de Kaspersky Endpoint Security aparece en la barra de estado.

El icono refleja el funcionamiento de la aplicación y ofrece acceso a la ventana principal de Kaspersky Endpoint Security.

El icono señala el funcionamiento de Kaspersky Endpoint Security y refleja el estado de protección del dispositivo:

: el dispositivo está protegido.

: hay problemas con la protección (por ejemplo, las bases de datos antimalware están desactualizadas o una aplicación recién instalada no se analizó).

Análisis del dispositivo

El componente Antimalware tiene varias limitaciones:

- Cuando el componente Antimalware se está ejecutando, una amenaza detectada en la memoria externa del dispositivo (por ejemplo, una tarjeta SD) no se puede neutralizar automáticamente en el contenedor corporativo. Kaspersky Endpoint Security para Android no tiene el acceso a la memoria externa en el contenedor corporativo. La información sobre los objetos detectados se muestra en las notificaciones de la aplicación. Para neutralizar objetos detectados en la memoria externa, los archivos de objeto se tienen que eliminar manualmente y se debe reiniciar el análisis del dispositivo.

- Debido a limitaciones técnicas, Kaspersky Endpoint Security para Android no puede analizar archivos con un tamaño de 2 GB o más. Durante un análisis, la app omite dichos archivos sin notificarle que se omitieron.

- En dispositivos con Android 11 o versiones posteriores, la aplicación Kaspersky Endpoint Security para Android no puede analizar las carpetas "Android/data" ni "Android/obb" ni detectar malware en ellas debido a limitaciones técnicas.

Para iniciar un análisis del dispositivo:

1. En la ventana principal de Kaspersky Endpoint Security, toque **Settings** → **App settings** → **Anti-Malware** → **Start scan**.

2. Seleccione el alcance del análisis del dispositivo:

   - **Analizar todo el dispositivo**. La aplicación analiza el sistema de archivos completo del dispositivo.

   - **Analizar aplicaciones instaladas**. La aplicación solo analiza las aplicaciones instaladas.

- **Análisis personalizado**. La aplicación analiza la carpeta seleccionada o un archivo individual. Puede seleccionar un objeto individual (carpeta o archivo) o una de las particiones siguientes de la memoria del dispositivo:

  - **Memoria del dispositivo**. Memoria de todo el dispositivo a la que se puede acceder para lectura. Esto también incluye la partición de la memoria del sistema que almacena archivos del sistema operativo.

  - **Memoria interna**. Partición de la memoria del dispositivo destinada a la instalación de aplicaciones y al almacenamiento de contenidos multimedia, documentos y otros archivos.

  - **Memoria externa**. Memoria de la tarjeta SD externa. Si no hay ninguna tarjeta SD externa instalada, esta opción está oculta.

Es posible que el administrador restrinja el acceso a la configuración del análisis de malware.

Para configurar el análisis de malware, siga estos pasos:

1. En la ventana principal de Kaspersky Endpoint Security, toque **Settings** → **App settings** → **Anti-Malware** → **Scan settings**.

2. Si desea que la aplicación detecte adware y aplicaciones que podrían ser utilizadas por atacantes para dañar su dispositivo o sus datos cuando la aplicación realiza un análisis, active el interruptor **Adware, programas de marcado y otros**.

3. Toque **Acción al detectar una amenaza** y seleccione la acción que realiza la aplicación predeterminada:

   - **Cuarentena**

     La cuarentena almacena los archivos como archivos comprimidos para que no puedan causar daños al dispositivo. El filtro de llamadas y mensajes de texto le permite eliminar o restaurar los archivos que se movieron a la cuarentena.

   - **Preguntar al usuario**

     La aplicación le solicita que seleccione una acción para cada objeto detectado: omitir, poner en cuarentena o eliminar. Cuando se detectan varios objetos, puede aplicar una acción seleccionada a todos los objetos.

   - **Eliminar**

     Los Objetos detectados se eliminarán automáticamente. No se requieren más acciones. Antes de eliminar un objeto, Kaspersky Endpoint Security mostrará una notificación temporal para indicar la detección del objeto.

   - **Omitir**

     Si se han omitido los objetos detectados, Kaspersky Endpoint Security le advierte sobre problemas en la protección del dispositivo. Para cada amenaza omitida, la aplicación le proporciona acciones que puede realizar para eliminar la amenaza. La lista de objetos omitidos puede cambiar, por ejemplo, si se eliminó o movió un archivo malicioso. Para recibir una lista actualizada de amenazas, ejecute un análisis completo del dispositivo. Para garantizar la protección fiable de sus datos, elimine todos los objetos detectados.

Se registra la información sobre amenazas detectadas y las acciones realizadas al respecto en los informes de la aplicación (**Settings** → **Reports**). Puede elegir mostrar informes sobre las operaciones del componente Antimalware.

Ejecución de un análisis programado

El componente Antimalware tiene varias limitaciones:

- Cuando el componente Antimalware se está ejecutando, una amenaza detectada en la memoria externa del dispositivo (por ejemplo, una tarjeta SD) no se puede neutralizar automáticamente en el contenedor corporativo. Kaspersky Endpoint Security para Android no tiene el acceso a la memoria externa en el contenedor corporativo. La información sobre los objetos detectados se muestra en las notificaciones de la aplicación. Para neutralizar objetos detectados en la memoria externa, los archivos de objeto se tienen que eliminar manualmente y se debe reiniciar el análisis del dispositivo.

- Debido a limitaciones técnicas, Kaspersky Endpoint Security para Android no puede analizar archivos con un tamaño de 2 GB o más. Durante un análisis, la app omite dichos archivos sin notificarle que se omitieron.

- En dispositivos con Android 11 o versiones posteriores, la aplicación Kaspersky Endpoint Security para Android no puede analizar las carpetas "Android/data" ni "Android/obb" ni detectar malware en ellas debido a limitaciones técnicas.

Para configurar la programación del análisis completo del dispositivo:

1. En la ventana principal de Kaspersky Endpoint Security, toque **Settings** → **App settings** → **Anti-Malware** → **Scan settings**.

2. Toque **Programación** y seleccione la frecuencia de análisis completo:

   - **Semanal**
   - **A diario**
   - **Deshabilitado**
   - **Tras actualizar la base de datos**

3. Toque **Día de inicio** y seleccione el día de la semana en que desea que comience el análisis completo.

4. Toque **Hora de inicio** y seleccione la hora para comenzar el análisis completo.

El análisis completo del dispositivo se iniciará según la programación.

Si el dispositivo está en modo de ahorro de batería, la aplicación puede realizar esta tarea más tarde de lo especificado. Para garantizar una respuesta oportuna de los dispositivos Android a los comandos del administrador, habilite el uso de Firebase Cloud Messaging.

Cambio del modo de Protección

La protección en tiempo real permite detectar amenazas en los archivos que se abren y analizar aplicaciones mientras se instalan en el dispositivo. Las bases de datos antimalware y el servicio en la nube de Kaspersky Security Network (Protección en la nube) se utilizan para garantizar la seguridad de manera automática.

Para cambiar el modo de Protección del dispositivo:

1. En la ventana principal de Kaspersky Endpoint Security, toque **Settings** → **App settings** → **Anti-Malware** → **Real-time protection mode**.

2. Seleccione el modo de Protección del dispositivo:

   - **Deshabilitado**. La protección está desactivada.

   - **Recomendado**. El componente Antimalware analiza solo las aplicaciones instaladas y los archivos de la carpeta Descargas. El componente Antimalware analiza las nuevas aplicaciones en cuanto se instalan.

   - **Extendido**. El antimalware analiza todos los archivos del dispositivo en busca de objetos maliciosos cuando se realiza cualquier operación con ellos (por ejemplo, cuando se guardan, mueven o modifican). El componente Antimalware también analiza las nuevas aplicaciones en cuanto se instalan.

La información sobre el modo de protección actual se muestra debajo de la descripción del componente.

Es posible que el administrador restrinja el acceso a la configuración de protección en tiempo real.

Para habilitar Protección en la nube (KSN):

1. En la ventana principal de Kaspersky Endpoint Security, toque **Settings** → **App settings** → **Anti-Malware**.

2. Active el interruptor de **Protección en la nube (KSN)**.

   El interruptor de **Protección en la nube (KSN)** administra el uso de Kaspersky Security Network solo para la protección en tiempo real de un dispositivo. Si la casilla no está seleccionada, Kaspersky Endpoint Security sigue utilizando KSN para el funcionamiento de otros componentes de la aplicación.

Como resultado, la aplicación obtiene acceso a la base de conocimientos en línea de Kaspersky sobre la reputación de archivos y aplicaciones. El análisis busca amenazas cuya información aún no se ha agregado a las bases de datos antimalware, pero que ya está disponible en KSN. El servicio en la nube de Kaspersky Security Network garantiza el funcionamiento completo del antimalware y reduce la probabilidad de falsas alarmas. Solo el administrador puede deshabilitar por completo el uso de Kaspersky Security Network.

Para configurar Protección en tiempo real:

1. En la ventana principal de Kaspersky Endpoint Security, toque **Settings** → **App settings** → **Anti-Malware** → **Scan settings**.

2. Si desea que la aplicación detecte adware y aplicaciones que podrían ser utilizadas por atacantes para dañar su dispositivo o sus datos cuando la aplicación realiza un análisis, active el interruptor **Adware, programas de marcado y otros**.

3. Toque **Acción al detectar una amenaza** y seleccione la acción que realiza la aplicación predeterminada:

   - **Cuarentena**

     La cuarentena almacena los archivos como archivos comprimidos para que no puedan causar daños al dispositivo. La cuarentena le permite eliminar o restaurar los archivos que se movieron al almacenamiento aislado.

- **Preguntar al usuario**

  La aplicación le solicita que seleccione una acción para cada objeto detectado: omitir, poner en cuarentena o eliminar. Cuando se detectan varios objetos, puede aplicar una acción seleccionada a todos los objetos.

- **Eliminar**

  Los Objetos detectados se eliminarán automáticamente. No se requieren más acciones. Antes de eliminar un objeto, Kaspersky Endpoint Security mostrará una notificación temporal para indicar la detección del objeto.

- **Omitir**

  Si se han omitido los objetos detectados, Kaspersky Endpoint Security le advierte sobre problemas en la protección del dispositivo. Para cada amenaza omitida, la aplicación le proporciona acciones que puede realizar para eliminar la amenaza. La lista de objetos omitidos puede cambiar, por ejemplo, si se eliminó o movió un archivo malicioso. Para recibir una lista actualizada de amenazas, ejecute un análisis completo del dispositivo. Para garantizar la protección fiable de sus datos, elimine todos los objetos detectados.

Se registra la información sobre amenazas detectadas y las acciones realizadas al respecto en los informes de la aplicación (**Settings** → **Reports**). Puede elegir mostrar informes sobre las operaciones del componente Antimalware.

Actualizaciones de las bases de datos antimalware

Para actualizar las bases de datos antimalware de la aplicación:

En la ventana principal de Kaspersky Endpoint Security, toque **Settings** → **App settings** → **Anti-Malware** → **Start database update**.

Cuando usa Kaspersky Endpoint Security para Android, puede encontrar el problema **Se bloqueó el nombre de dominio del servicio de Kaspersky**, lo que significa que los problemas de red impiden que la aplicación llegue a los servicios de Kaspersky. Esto puede afectar las funciones de protección antimalware y poner en riesgo sus datos. Cambiar la configuración de la conexión podría solucionar el problema.

Esta sección solo brinda instrucciones generales. Consulte la guía del usuario proporcionada por el fabricante del dispositivo para obtener instrucciones específicas.

Para cambiar la configuración de la conexión:

1. Vaya a **Configuración** en el dispositivo.
2. Abra la configuración de conexión.
3. Vaya a la sección **DNS privado**.
4. Seleccione **Nombre de host del proveedor de DNS privado** y, a continuación, escriba un nombre de DNS. Por ejemplo, puede escribir "dns.google" para usar el servidor DNS público de Google.
5. Guarde los cambios.

La configuración de conexión se actualiza.

Actualización de bases de datos programada

La aplicación puede actualizar automáticamente las bases de datos antimalware según la programación que especifique.

Para configurar la programación de actualización:

1. En la ventana principal de Kaspersky Endpoint Security, toque **Settings** → **App settings** → **Anti-Malware** → **Database update settings**.
2. Toque **Programación** y seleccione la frecuencia de actualización:
   - **Semanal**
   - **A diario**
   - **Deshabilitado**
3. Toque **Día de inicio** y seleccione el día de la semana en que desea realizar la actualización.
4. Toque **Hora de inicio** y seleccione la hora para comenzar la actualización.

Las actualizaciones de las bases de datos antimalware se iniciarán según la programación.

Si el dispositivo está en modo de ahorro de batería, la aplicación puede realizar esta tarea más tarde de lo especificado. Para garantizar una respuesta oportuna de los dispositivos Android a los comandos del administrador, habilite el uso de Firebase Cloud Messaging.

La función de actualizaciones (incluido el suministro de actualizaciones de las firmas antimalware y de la base de código) y la función de KSN pueden dejar de estar disponibles en el software en el territorio de EE. UU.

Qué hacer en caso de pérdida o robo del dispositivo

Si pierde o le roban el dispositivo, comuníquese con el administrador del sistema. El administrador puede ejecutar comandos antirrobo en su dispositivo de forma remota, según los requisitos de seguridad corporativa.

Si se envía el comando Restablecer ajustes de fábrica al dispositivo, se perderá el control sobre este y los demás comandos antirrobo no funcionarán.

Protección web

Deben cumplirse las siguientes condiciones para habilitar Protección web:

- Se debe configurar Kaspersky Endpoint Security para Android como un Servicio de accesibilidad.

  Si la aplicación Kaspersky Endpoint Security para Android en un dispositivo corporativo no está habilitada como servicio de funciones de accesibilidad, la protección web solo es compatible con el navegador Google Chrome y solo verifica el dominio de un sitio web. Para permitir que otros navegadores (Samsung Internet, Yandex Browser y HUAWEI Browser) admitan la protección web, habilite Kaspersky Endpoint Security como servicio de funciones de accesibilidad. Esto también habilitará el funcionamiento de la función Pestañas personalizadas.

- Se debe aceptar la Declaración con respecto al procesamiento de datos para el uso de la Protección web (Declaración de Protección web). Kaspersky Endpoint Security usa Kaspersky Security Network (KSN) para analizar sitios web. La Declaración de Protección web contiene los términos del intercambio de datos con KSN.

  Su administrador puede aceptar la Declaración de Protección web en su nombre en Kaspersky Security Center. En este caso, no necesita realizar ninguna acción.

  Si su administrador no aceptó la Declaración de Protección web y le envió la solicitud para hacerlo, debe leer y aceptar la Declaración de Protección web en la configuración de la aplicación.

  Si su administrador no ha aceptado la Declaración de Protección web, la Protección web no está disponible.

- En algunos dispositivos, se deben otorgar los siguientes permisos:

  - **Ejecutar en segundo plano**
  - **Mostrar ventanas emergentes mientras se ejecuta en segundo plano**
  - **Mostrar ventana emergente**
  - **Ignorar la optimización de la batería**

En Yandex Browser y Samsung Internet, las URL maliciosas y de phishing pueden permanecer desbloqueadas. Esto se debe a que solo se realiza el análisis del dominio del sitio web. Si se trata de un dominio malicioso o de phishing, Protección web bloquea la amenaza. Si el dominio no está clasificado como malicioso o como phishing, la URL específica no se bloquea.

Protección web en dispositivos Android solo es compatible con Google Chrome, el navegador HUAWEI, Samsung Internet y Yandex Browser.

La función Pestañas personalizadas es compatible con Google Chrome, el navegador HUAWEI y Samsung Internet.

Para usar la protección web en Telegram, desactive la apertura de enlaces en el navegador integrado de Telegram en la configuración de Telegram.

La Protección web para HUAWEI Browser, Samsung Internet y Yandex Browser no bloquea sitios en un dispositivo móvil si se utiliza un contenedor corporativo y la Protección web está habilitada solo para el contenedor corporativo.

Para usar la protección web en todo momento mientras navega por la web, establezca Google Chrome, HUAWEI Browser, Samsung Internet o Yandex Browser como navegador predeterminado.

Para establecer un navegador admitido como navegador predeterminado y usar la Protección web para analizar los sitios web en todo momento:

1. En la ventana principal de Kaspersky Endpoint Security, toque **Settings** → **App settings** → **Web Protection**.
2. Active el interruptor de **Protección web**.
3. Toque **Establecer navegador predeterminado**.

   Este botón se muestra cuando la protección web está habilitada y no se ha establecido un navegador compatible como navegador predeterminado.

   Se inicia el asistente de selección del navegador predeterminado.
4. Siga las instrucciones del asistente.

El asistente establece Google Chrome, HUAWEI Browser o Samsung Internet como navegador predeterminado. La protección web analiza continuamente los sitios web mientras navega por la web.

Análisis de notificaciones de servicios de mensajería instantánea

Kaspersky Endpoint Security para Android puede detectar URL maliciosas y de phishing en las notificaciones de Telegram, WhatsApp, la aplicación de SMS predeterminada y otras aplicaciones de servicio de mensajería instantánea habituales. Solo se pueden analizar las URL expresadas como texto directamente en el texto de la notificación. Las direcciones URL incrustadas en marcas no se analizan.

Deben cumplirse las siguientes condiciones para habilitar el análisis de notificaciones:

- La Protección web debe estar habilitada.
- La visualización de notificaciones debe estar permitida para los servicios de mensajería instantánea deseados. Kaspersky Endpoint Security para Android analiza únicamente las notificaciones que pueden mostrarse en la pantalla del dispositivo.
- En los dispositivos Google Pixel y Vivo, se debe conceder el permiso "Conversaciones" a Kaspersky Endpoint Security en la configuración de acceso a notificaciones.

Para permitir el acceso a las notificaciones de manera que la aplicación pueda analizarlas:

1. En la ventana principal de Kaspersky Endpoint Security, toque **Settings** → **App settings** → **Web Protection**.
2. Active el interruptor **Bloquee notificaciones que contengan URL maliciosas y de phishing**.

   Se abre la ventana **Acceso de notificación requerido**.
3. Toque **Continuar**.

   Se abre la sección de configuración correspondiente.
4. Active el interruptor de Kaspersky Endpoint Security.
5. En el cuadro de diálogo que se abre, permita que la aplicación lea todas sus notificaciones.
6. Vuelva a Kaspersky Endpoint Security.

La aplicación analiza ahora las notificaciones para detectar URL maliciosas y de phishing. Si se encuentra una URL peligrosa, la notificación se bloquea y aparece una pantalla de bloqueo con información sobre la notificación bloqueada.

Si Kaspersky Endpoint Security para Android no está habilitada como función de Accesibilidad, la aplicación envía una notificación push sobre las URL peligrosas detectadas en lugar de mostrar una pantalla de bloqueo. Tras tocar la notificación push, aparece una pantalla con información sobre la notificación bloqueada.

Obtener certificado

Para obtener un certificado para acceder a los recursos de la red corporativa:

1. En la ventana principal de Kaspersky Endpoint Security, toque **Settings** → **App settings** → **Additional** → **Get certificate**.
2. Especifique sus credenciales de la cuenta de la red corporativa. El nombre de usuario debe especificarse en uno de los siguientes formatos:

   - `userPrincipalName@DNSDomainName`
   - `sAMAccountName`
   - `sAMADomain\sAMAccountName`

   Para obtener más información sobre estos atributos, visite el sitio web de documentación técnica de Microsoft. Para obtener más detalles, puede comunicarse con su administrador.
3. Si recibió una contraseña de un solo uso del administrador, seleccione la casilla **Contraseña de un solo uso** y escríbala.

   Se inicia el Asistente de instalación de certificados.
4. Siga las instrucciones del asistente.

Sincronizar con Kaspersky Security Center

La sincronización del dispositivo móvil con el sistema de administración remota de Kaspersky Security Center es necesaria para proteger y configurar el dispositivo de acuerdo con los requisitos de seguridad corporativa. El dispositivo se sincroniza con Kaspersky Security Center automáticamente, pero también se puede iniciar la sincronización de forma manual. Después de la primera sincronización, el dispositivo se agrega a la lista de dispositivos móviles administrados mediante Kaspersky Security Center. El administrador puede configurar su dispositivo de acuerdo con los requisitos de seguridad corporativa.

La configuración de sincronización se puede ajustar durante la ejecución del asistente de configuración inicial o en la configuración de Kaspersky Endpoint Security. Pídale al administrador del sistema que le proporcione los valores de sincronización.

Modifique la configuración de sincronización del dispositivo con el sistema de administración remota de Kaspersky Security Center únicamente si el administrador se lo indica.

Para sincronizar el dispositivo con Kaspersky Security Center:

1. En la ventana principal de Kaspersky Endpoint Security, toque **Settings** → **App settings** → **Synchronization**.
2. En la sección **Configuración de sincronización** especifique los valores de la siguiente configuración:
   - **Servidor**
   - **Puerto**
   - **Grupo**
   - **Correo electrónico corporativo**

   El administrador puede ocultar la configuración de sincronización.
3. Toque **Sincronizar**.

Activación de la aplicación Kaspersky Endpoint Security para Android sin Kaspersky Security Center

En la mayoría de los casos, el administrador activa la aplicación Kaspersky Endpoint Security para Android que está instalada en su dispositivo de forma centralizada en el sistema de administración remota de Kaspersky Security Center. Si su dispositivo no está conectado a Kaspersky Security Center, puede ingresar el código de activación manualmente. Para obtener el código de activación, comuníquese con el administrador.

Active la aplicación manualmente solo cuando se lo indique el administrador.

Para ingresar el código de activación:

1. En el mensaje que dice que su licencia caducará pronto o que ya caducó, y que su dispositivo no está conectado al Servidor de administración, toque **Activar**.
2. En la ventana de activación, ingrese el código de activación que le dio el administrador y toque **Activar**.
3. Si el código de activación es correcto, se muestra una notificación que indica que la aplicación se activó, junto con la fecha de caducidad de la licencia.

La aplicación Kaspersky Endpoint Security para Android en su dispositivo está activada.

Instalar y usar certificados de correo y VPN en el dispositivo

El administrador puede especificar que los certificados de correo y VPN se instalen en el dispositivo. En dispositivos corporativos o dispositivos con un contenedor corporativo, dichos certificados se instalan automáticamente.

Se instala un certificado de correo en el dispositivo solo si su administrador primero configura los ajustes de Exchange ActiveSync.

Un certificado VPN también se puede instalar en un almacén de certificados de confianza de un espacio personal, además del contenedor corporativo, y cualquier aplicación puede utilizarlo. Recibirá una notificación y deberá instalar un certificado VPN manualmente siguiendo las instrucciones a continuación.

Para instalar manualmente un certificado VPN en el dispositivo, siga estos pasos:

1. Abra Kaspersky Endpoint Security para Android.
2. Toque **Notifications**.
3. En la notificación sobre el certificado, toque **Install**.

   Se abre una ventana con la contraseña del certificado.
4. Recuerde o escriba la contraseña y toque **Aceptar**.
5. Cuando se le solicite, ingrese la contraseña del certificado y toque **Aceptar**.
6. Toque **Aceptar** para confirmar la instalación del certificado.

El certificado VPN se instalará en el dispositivo.

Habilitación de la accesibilidad en Android 13 o posterior

En Android 13 o posterior, los servicios de accesibilidad están restringidos para las aplicaciones no descargadas desde Google Play o HUAWEI AppGallery. Debe permitir manualmente los servicios de accesibilidad si descargó Kaspersky Endpoint Security para Android desde el servidor de Kaspersky Security Center o el sitio web de Kaspersky.

Si actualiza la aplicación Kaspersky Endpoint Security para Android mediante un paquete de instalación de Kaspersky Security Center o un archivo APK del sitio web de Kaspersky, los servicios de accesibilidad se deshabilitarán. Debe volver a habilitar manualmente los servicios de accesibilidad.

La accesibilidad se utiliza para los siguientes fines:

- Verificar los sitios web y las aplicaciones en Kaspersky Security Network
- Bloquear el dispositivo en caso de robo
- Mostrar advertencias
- Bloquear la cámara cuando está restringida por el administrador

Para habilitar la accesibilidad de Kaspersky Endpoint Security:

1. Abra la página **Accesibilidad** en la configuración del dispositivo y busque Kaspersky Endpoint Security.
2. Active el interruptor de Kaspersky Endpoint Security. En el cuadro de diálogo que indica que los servicios de accesibilidad están restringidos, toque **Aceptar**.

   Ahora puede dar a Kaspersky Endpoint Security acceso a la configuración restringida.
3. Abra la página de información de Kaspersky Endpoint Security en la configuración del dispositivo. Por ejemplo, vaya a **Configuración** > **Aplicaciones** y busque la aplicación en la lista de aplicaciones.
4. En la página de información de Kaspersky Endpoint Security, toque ⋮ en la esquina superior derecha y seleccione **Permitir configuración restringida**.

   Kaspersky Endpoint Security ahora tiene acceso a la configuración restringida.
5. Vuelva a la página **Accesibilidad** en la configuración del dispositivo y busque Kaspersky Endpoint Security.
6. Active el interruptor de **Kaspersky Endpoint Security**. En el cuadro de diálogo que se abre, permita que la aplicación tenga control total de su dispositivo.

Los servicios de accesibilidad están ahora habilitados para Kaspersky Endpoint Security.

Habilitación de la accesibilidad de la aplicación en Android 13 o posterior

Para habilitar la accesibilidad de Kaspersky Endpoint Security:

1. En el cuadro de diálogo donde se le pide que active los servicios de accesibilidad, toque **Activar**.

   Se abre la página **Accesibilidad** en la configuración del dispositivo.

2. Active el interruptor de Kaspersky Endpoint Security. En el cuadro de diálogo que indica que los servicios de accesibilidad están restringidos, toque **Aceptar**.

   Ahora puede dar a Kaspersky Endpoint Security acceso a la configuración restringida.

3. Abra la página de información de Kaspersky Endpoint Security en la configuración del dispositivo. Por ejemplo, vaya a **Configuración** > **Aplicaciones** y busque la aplicación en la lista de aplicaciones.

4. En la página de información de Kaspersky Endpoint Security, toque ⋮ en la esquina superior derecha y seleccione **Permitir configuración restringida**.

   Kaspersky Endpoint Security ahora tiene acceso a la configuración restringida.

5. Vuelva a la aplicación y, en el cuadro de diálogo donde se le pide que active los servicios de accesibilidad, toque **Activar**.

   Se abre la página **Accesibilidad** en la configuración del dispositivo.

6. Active el interruptor de **Kaspersky Endpoint Security**. En el cuadro de diálogo que se abre, permita que la aplicación tenga control total de su dispositivo.

Los servicios de accesibilidad están ahora habilitados para Kaspersky Endpoint Security.

Actualización de la aplicación

Kaspersky Endpoint Security se puede actualizar de las siguientes maneras:

- Uso manual del sitio web de Kaspersky. Puede descargar la versión nueva de la aplicación desde el sitio web de Kaspersky e instalarla en el dispositivo.
- Con la ayuda de un administrador. El administrador puede actualizar de manera remota la versión de la aplicación en su dispositivo mediante el sistema de administración remota de Kaspersky Security Center.

Actualización de la aplicación desde el sitio web de Kaspersky

Para actualizar la aplicación desde el sitio web de Kaspersky:

1. Vaya al sitio web de Kaspersky.
2. Busque Kaspersky Security para dispositivos móviles en el sitio web.

3. Toque **Mostrar descargas**.
4. Seleccione una versión de la aplicación y toque **Descargar**.
5. Abra el archivo APK descargado y siga las instrucciones en pantalla.

Kaspersky Endpoint Security para Android se actualizó.

Actualización de la aplicación mediante Kaspersky Security Center

Actualizar la aplicación mediante Kaspersky Security Center consiste en los pasos siguientes:

1. El administrador envía a su dispositivo móvil el paquete de distribución de la aplicación cuya versión cumple con los requisitos de seguridad corporativa.

   Se muestra un mensaje para instalar Kaspersky Endpoint Security en su dispositivo.
2. Acepte los términos y condiciones de actualización.

   La versión nueva de la aplicación se instalará en su dispositivo. La aplicación no requiere configuración adicional después de la actualización.

La función de actualizaciones (incluido el suministro de actualizaciones de las firmas antimalware y de la base de código) y la función de KSN pueden dejar de estar disponibles en el software en el territorio de EE. UU.

Eliminación de la aplicación

El administrador puede bloquear que elimine la aplicación por su cuenta. Si es así, no puede eliminar Kaspersky Endpoint Security.

Kaspersky Endpoint Security se puede eliminar de las siguientes maneras:

- Manualmente en la configuración del dispositivo.
- Con la ayuda de un administrador. El administrador puede eliminar de manera remota la aplicación de su dispositivo mediante el sistema de administración remota de Kaspersky Security Center.

En los dispositivos corporativos, solo el administrador puede eliminar Kaspersky Endpoint Security para Android al restablecer los ajustes de fábrica del dispositivo.

Eliminación en la configuración del dispositivo

La aplicación se puede eliminar mediante el procedimiento estándar de la plataforma Android. Para eliminar la aplicación, los derechos del administrador para Kaspersky Endpoint Security deben estar deshabilitados en la configuración de seguridad del dispositivo.

En dispositivos con Android 7 o versiones posteriores, si el administrador ha bloqueado la eliminación, el dispositivo se bloqueará si se realiza un intento de eliminar la aplicación en la configuración de Android. Para desbloquear el dispositivo, contacte a su administrador.

Eliminación mediante Kaspersky Security Center

La eliminación de la aplicación mediante Kaspersky Security Center consiste en los siguientes pasos:

1. El administrador envía el comando de eliminación de la aplicación a su dispositivo móvil.

   Su dispositivo móvil muestra un mensaje para confirmar la eliminación de Kaspersky Endpoint Security.

2. Confirme la eliminación de la aplicación.

   La aplicación se eliminará de su dispositivo.

Aplicaciones con el icono de un maletín

Las aplicaciones marcadas con un ícono de maletín (aplicaciones corporativas) se almacenan en su dispositivo en el contenedor corporativo. El *contenedor corporativo* es un entorno seguro del dispositivo en el que el administrador puede administrar las cuentas y aplicaciones sin restringir sus capacidades de trabajar con datos personales.

Un contenedor corporativo permite almacenar los datos corporativos y personales por separado. Esto mantiene la confidencialidad de los datos corporativos y los protege contra malware. Cuando se crea un contenedor corporativo en el dispositivo, se instalan las siguientes aplicaciones corporativas automáticamente en el contenedor corporativo: Google Play Market, Google Chrome, Descargas, Kaspersky Endpoint Security para Android y otras.

Aplicación Knox



Ícono de Knox

La aplicación de Knox abre un contenedor Knox en su dispositivo. Un *contenedor de Knox* es un entorno seguro en su dispositivo que tiene su propio escritorio, panel de inicio, aplicaciones y widgets. El administrador puede administrar aplicaciones y cuentas en un contenedor Knox sin restringir sus capacidades de trabajar con datos personales.

Un contenedor Knox permite almacenar los datos corporativos y personales por separado. Esto mantiene la confidencialidad de los datos corporativos y los protege contra malware.

En un contenedor Knox, puede acceder a su buzón de correo de la empresa, a la información de contacto de los empleados de la empresa, al almacenamiento de archivos y a otras aplicaciones.

Para obtener más información sobre cómo trabajar con Knox, visite el sitio web del Servicio de soporte técnico de Samsung.

Usar la aplicación Kaspersky Protection para iOS

Esta sección de Ayuda describe las funciones y operaciones que están disponibles para los usuarios de la aplicación Kaspersky Protection para iOS.

Los artículos de esta sección incluyen todas las opciones que pueden estar visibles o disponibles en un dispositivo móvil. El diseño y el comportamiento de la aplicación se establecen en función del sistema de administración remota implementado y de cómo el administrador configure su dispositivo según los requisitos de seguridad corporativa. Es posible que algunas de las funciones y opciones que se describen en esta sección no se apliquen a su experiencia real con la aplicación. Si tiene alguna pregunta sobre la aplicación instalada en un dispositivo específico, comuníquese con su administrador.

Funciones de la aplicación

Kaspersky Protection para iOS ofrece las siguientes funciones clave.

Protección contra amenazas en línea

El componente Protección web ofrece protección contra amenazas en línea.

El componente Protección web bloquea los sitios web maliciosos que distribuyen un código malicioso y los sitios web de phishing diseñados para robar sus datos confidenciales y acceder a sus cuentas financieras. Protección web analiza los sitios web antes de abrirlos mediante el servicio en la nube de Kaspersky Security Network.

Solo se analiza el dominio del sitio web. Si se trata de un dominio malicioso o de phishing, Protección web bloquea la amenaza. Si el dominio no está clasificado como malicioso o como phishing, la URL específica no se bloquea.

La Protección web también supervisa la actividad de red de las aplicaciones y todo el tráfico del sistema en su dispositivo.

Para que la Protección web funcione, debe permitir que la aplicación agregue una configuración de VPN.

Detección de jailbreak

Cuando Kaspersky Protection para iOS detecta un jailbreak, muestra un mensaje crítico e informa a su administrador sobre el problema.

Una liberación permite evadir las funciones de seguridad del sistema operativo, por lo que no se puede garantizar la seguridad de su dispositivo y pueden surgir varios problemas, incluidos los siguientes:

- Vulnerabilidades de seguridad
- Problemas de estabilidad
- Interrupción de los servicios de Apple
- Posibles fallas y bloqueos
- Reducción de la duración de la batería
- Imposibilidad de aplicar las actualizaciones de iOS

Instalar la aplicación

Puede instalar la aplicación Kaspersky Protection para iOS mediante un vínculo o un código QR generado para usted por el administrador en la consola de administración. Recibirá esta información en un correo electrónico.

Para instalar la aplicación Kaspersky Protection para iOS, siga estos pasos:

1. Busque el mensaje de correo electrónico con la invitación del administrador para conectar su dispositivo al sistema de administración remota de Kaspersky Security Center.
2. Vaya a la App Store de una de las siguientes maneras:
   - Presione **Conectar dispositivo** en el mensaje si lo está leyendo en el dispositivo iOS en el que desea instalar la aplicación.
   - Escanee el código QR con el dispositivo iOS en el que desea instalar la aplicación si está leyendo el mensaje en una computadora.

   El vínculo de invitación es válido durante 24 horas. Si no logra instalar la aplicación a tiempo, comuníquese con su administrador para obtener una nueva invitación.
3. En la página web que se abre, presione **Descargar en la App Store**.
4. Descargue e instale la aplicación desde la App Store siguiendo el procedimiento de instalación de aplicaciones estándar en la plataforma iOS.

La aplicación Kaspersky Protection para iOS se instala en su dispositivo. Para proteger el dispositivo, activa la aplicación. Si su dispositivo no está conectado a Kaspersky Security Center, puede activar la aplicación manualmente con el código de activación proporcionado por su administrador.

Activación de la aplicación

Para activar la aplicación Kaspersky Protection para iOS, siga estos pasos:

1. Inicie la aplicación en su dispositivo.
2. Acepte los contratos y las declaraciones seleccionando las casillas **End User License Agreement** y **Products and Services Privacy Policy**.

   O bien, puede aceptar la **Kaspersky Security Network Statement** para permitir el envío de estadísticas a Kaspersky Security Network. Esto mejora el rendimiento de la aplicación y garantiza su funcionamiento ininterrumpido.
3. Pulse **Next**. La aplicación se conecta al sistema de administración remota de Kaspersky Security Center y obtiene la información de la licencia.
4. Permita que la aplicación agregue una configuración de VPN. La aplicación utiliza la configuración de la VPN para comprobar los sitios web en busca de phishing y proteger su dispositivo de las amenazas web.
5. Permita que la aplicación envíe notificaciones automáticas. La aplicación utiliza notificaciones para informarle los problemas de seguridad y su licencia.

Se activa la aplicación Kaspersky Protection para iOS en su dispositivo.

Activar la aplicación con un código de activación

Cuando instala la aplicación Kaspersky Protection para iOS en su dispositivo, la aplicación se conecta al sistema de administración remota de Kaspersky Security Center y obtiene la información de la licencia de forma automática. Si su dispositivo no está conectado a Kaspersky Security Center, puede ingresar el código de activación manualmente. Para obtener el código de activación, comuníquese con el administrador.

Active la aplicación manualmente solo cuando se lo indique el administrador.

Para ingresar el código de activación:

1. En el mensaje que indica que la aplicación no está activada, toque **Activate the app**.
2. En la ventana de activación, ingrese el código de activación que le dio el administrador y toque **Activate**.

   Si el código de activación es correcto, se muestra una notificación que indica que la aplicación se activó, junto con la fecha de caducidad de la licencia.

Se activa la aplicación Kaspersky Protection para iOS en su dispositivo.

Ventana principal de un vistazo

La apariencia de la ventana principal apenas difiere según las diferentes resoluciones de pantalla.

La ventana principal muestra lo siguiente:

- Estado general de la protección de su dispositivo.
- Mensajes que indican el estado de los componentes de la aplicación y los problemas de protección.

Hay tres tipos de mensajes:

- Resaltados en verde. Mensajes de estado que informan que la protección está activa en el área especificada.
- Resaltados en amarillo. Mensajes de información sobre eventos que pueden afectar la seguridad del dispositivo.
- Resaltados en rojo. Mensajes críticos que informan sobre eventos de importancia crítica para la seguridad del dispositivo.

Puede tocar un mensaje para ver los detalles.

Actualización de la aplicación

Puede descargar la última versión de la aplicación Kaspersky Protection para iOS desde la App Store e instalarla en su dispositivo siguiendo el procedimiento de actualización estándar en la plataforma iOS. También puede activar las actualizaciones automáticas. La aplicación no requiere ninguna configuración adicional después de la actualización.

Para actualizar la aplicación deben cumplirse las siguientes condiciones:

- Debe tener un Apple ID.
- El dispositivo debe estar vinculado a su Apple ID.
- El dispositivo debe estar conectado a Internet.

Para obtener más información sobre la creación de un Apple ID, la vinculación del dispositivo con su Apple ID o el funcionamiento de la App Store, consulte el sitio web de soporte de Apple.

La función de actualizaciones (incluido el suministro de actualizaciones de las firmas antimalware y de la base de código) y la función de KSN pueden dejar de estar disponibles en el software en el territorio de EE. UU.

Usar el diagnóstico para solucionar problemas

Si tiene problemas con Kaspersky Protection para iOS, los especialistas del Servicio de soporte técnico de Kaspersky pueden pedirle que les envíe un *archivo con información de diagnóstico*. Este archivo permite a los especialistas del Servicio de soporte técnico rastrear las causas de los problemas en el funcionamiento de la aplicación.

Para compartir un archivo con información de diagnóstico, el diagnóstico debe estar habilitado en Kaspersky Protection para iOS.

Le recomendamos que habilite el diagnóstico solo si se lo solicita un especialista del Servicio de soporte técnico de Kaspersky.

Guardar información de diagnóstico puede afectar la velocidad de su conexión a Internet y el rendimiento de su dispositivo, Kaspersky Protection para iOS y otras aplicaciones.

Puede eliminar el archivo con la información de diagnóstico manualmente en la aplicación Archivos.

Para habilitar el diagnóstico, siga estos pasos:

1. En la ventana principal, toque ⓘ.
2. En la ventana **About the App** que se abre, toque **Diagnostics**.
3. En la ventana **Diagnostics** que se abre, habilite el diagnóstico mediante el interruptor **Diagnostics**.
4. Acepte la Declaración de soporte. La Declaración de soporte describe qué datos se guardan en el archivo con información de diagnóstico.
5. Toque **OK**.

   Se habilita el diagnóstico en su dispositivo. Los datos sobre el funcionamiento de Kaspersky Protection para iOS ahora se guardarán en un archivo con información de diagnóstico. Si tiene algún problema, puede compartir este archivo con un especialista del Servicio de soporte técnico de Kaspersky.

Eliminación de la aplicación

Para eliminar la aplicación Kaspersky Protection para iOS, siga el procedimiento estándar en la plataforma iOS:

1. En la pantalla de inicio, mantenga pulsado el ícono de la aplicación.
2. Elimine la aplicación.

La aplicación Kaspersky Protection para iOS se elimina de su dispositivo.

Licenciamiento de la aplicación

Esta sección proporciona información sobre los términos generales relacionados con la licencia de MDM básico en Kaspersky Next Expert View (on-premise).

Acerca del Contrato de licencia de usuario final

El *Contrato de licencia de usuario final* (EULA) es un contrato obligatorio entre usted y AO Kaspersky Lab en el que se estipulan los términos y condiciones para utilizar el MDM básico en Kaspersky Next Expert View (on-premise).

Le recomendamos que lea detenidamente los Términos y condiciones del EULA antes de utilizar el MDM básico en Kaspersky Next Expert View (on-premise).

Puede consultar los Términos y condiciones del EULA de las siguientes maneras:

- Durante la instalación de componentes del MDM básico en Kaspersky Next Expert View (on-premise).
- Al leer el archivo license.txt incluido en el archivo comprimido de extracción automática del kit de distribución para instalar la aplicación Kaspersky Endpoint Security para Android.
- En la sección **Acerca de la aplicación** en Kaspersky Endpoint Security para Android.
- En la sección **About the App** → **Agreements and Statements** en Kaspersky Protection para iOS.
- En la sección **Avanzado** → **Contratos de licencia aceptados** en las propiedades del Servidor de administración. Esta función está disponible en la versión 12.1 de Kaspersky Security Center y versiones posteriores.
- En la sección **General** → **End User License Agreements** en las propiedades del Servidor de administración de Kaspersky Next Expert View (on-premise).
- En el paso 4 del proceso de conexión de dispositivos móviles a Kaspersky Next Expert View (on-premise), si se seleccionó **Administrator** en el paso 3. Se le pedirá al administrador que acepte el EULA.
- Durante la instalación de la aplicación, si se seleccionó **Users** en el paso 3 del proceso de conexión de dispositivos móviles a Kaspersky Next Expert View (on-premise). Se le pedirá al usuario del dispositivo móvil que acepte el EULA.

Al confirmar que acepta el Contrato de licencia de usuario final (EULA) al instalar los componentes del MDM básico en Kaspersky Next Expert View (on-premise), usted acepta los Términos y condiciones del Contrato de licencia de usuario final. Si no acepta los términos del Contrato de licencia de usuario final, debe cancelar la instalación de los componentes del MDM básico en Kaspersky Next Expert View (on-premise) y abstenerse de utilizarlos.

Acerca de la licencia

Una *licencia* otorga el derecho a usar el MDM básico en Kaspersky Next Expert View (on-premise) por un tiempo limitado según los términos del Contrato de licencia firmado (Contrato de licencia de usuario final).

El alcance de los servicios y el período de validez dependen de la licencia con la que se usa la solución.

Con una licencia que no proporciona funcionalidad ampliada, solo está disponible la configuración de protección básica del dispositivo en el complemento Kaspersky Mobile Devices Protection and Management.

Se proporcionan los siguientes tipos de licencia:

- *Prueba*

  Una licencia gratuita para probar el MDM básico en Kaspersky Next Expert View (on-premise).

  Una licencia de prueba es válida durante 30 días. Cuando la licencia de prueba caduque, las aplicaciones móviles Kaspersky Endpoint Security para Android o Kaspersky Protection para iOS dejarán de realizar la mayoría de sus funciones excepto la sincronización con el Servidor de administración. Para continuar usando las aplicaciones, debe adquirir una licencia comercial.

- *Comercial*

  Una licencia paga.

  Cuando la licencia comercial caduca, las aplicaciones móviles siguen funcionando, pero con la funcionalidad limitada.

  En el modo de funcionalidad limitada, los siguientes componentes están disponibles según la aplicación.

  - Aplicación Kaspersky Endpoint Security para Android:

    - Antimalware. Se encuentran disponibles la protección en tiempo real y el análisis de malware del dispositivo, pero las actualizaciones de la base de datos antimalware no están disponibles.
    - Antirrobo. Solo está disponible el envío de comandos a los dispositivos móviles.
    - Sincronización con el Servidor de administración.

    Kaspersky Endpoint Security para Android deja de intercambiar información con Kaspersky Security Network, Google Analytics para Firebase, Firebase Performance Monitoring y Crashlytics si la clave de Kaspersky se bloquea, si la licencia de prueba caduca o si falta una licencia (el código de activación se elimina de la directiva).

  - Aplicación de Kaspersky Protection para iOS:

    - Sincronización con el Servidor de administración.

    Kaspersky Protection para iOS deja de intercambiar información con Kaspersky Security Network si una licencia de prueba caduca o si falta una licencia (el código de activación se elimina de la directiva).

  Los componentes restantes de las aplicaciones móviles no están disponibles para el usuario del dispositivo y no puede configurar los ajustes de la directiva.

  Para seguir usando la funcionalidad completa de las aplicaciones y configurar los ajustes de la directiva, debe renovar su licencia comercial. Para garantizar una protección ininterrumpida de los dispositivos de sus usuarios contra todas las amenazas de seguridad, recomendamos renovar el plazo de la licencia o comprar una nueva licencia antes de que caduque la actual.

Ver información de la licencia

El complemento Kaspersky Mobile Devices Protection and Management le permite ver la siguiente información acerca de la licencia actual:

- Clave de la licencia
- Número de dispositivos en los que se puede usar la clave de licencia
- Tipo de licencia
- Fecha y hora de caducidad de la licencia
- Cantidad de días por transcurrir antes de que caduque la licencia
- El tipo de funcionalidad disponible bajo la licencia actual

Para ver información sobre la licencia actual, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (on-premise), seleccione **Asset management** → **Policies**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
2. En la ventana de propiedades de la directiva, seleccione **Application settings**.
3. Haga clic en **License**.

Se abre la ventana **License** que contiene información sobre la licencia.

Acerca de la suscripción

La suscripción para el MDM básico en Kaspersky Next Expert View (on-premise) es una solicitud para usar la aplicación móvil con los parámetros seleccionados (fecha de caducidad de la suscripción, cantidad de dispositivos móviles protegidos). Puede solicitar la suscripción para el MDM básico en Kaspersky Next Expert View (on-premise) a su proveedor de servicios (por ejemplo, su ISP). La suscripción se puede renovar de forma manual o automática, o bien se puede cancelar. Puede administrar la suscripción en el sitio web del proveedor de servicios.

La suscripción puede ser limitada, por ejemplo de un año, o ilimitada, es decir, sin fecha de caducidad. Para que el MDM básico en Kaspersky Next Expert View (on-premise) siga funcionando después de que caduque el plazo de la suscripción limitada, debe renovar la suscripción. La suscripción ilimitada se renueva automáticamente siempre que se realice el correspondiente pago al proveedor de servicios.

Si la suscripción es limitada, al caducar se podría ofrecer al usuario un período de gracia para renovarla, y durante ese período la aplicación seguirá funcionando. La disponibilidad y la duración de tal período de gracia son a discreción del proveedor de servicios.

Para usar el MDM básico en Kaspersky Next Expert View (on-premise) con suscripción, debe aplicar el código de activación recibido del proveedor de servicios. Tras aplicar el código de activación, se instala la clave de la licencia para utilizar la aplicación en la modalidad de suscripción.

Cada proveedor de servicios puede tener sus propias opciones de administración de suscripciones. Algunos podrían no ofrecer un período de gracia de renovación de la suscripción durante el que las aplicaciones conserven su funcionalidad.

Los códigos de activación comprados bajo suscripción no se pueden utilizar para activar versiones anteriores del MDM básico en Kaspersky Next Expert View (on-premise).

Acerca de la clave de licencia

Una *clave de licencia* es una secuencia de bits que puede aplicar para activar y usar la solución integrada MDM básico en Kaspersky Next Expert View (on-premise) de conformidad con los términos del Contrato de licencia de usuario final. Las claves de licencia son generadas por los especialistas de Kaspersky.

Puede agregar una clave de licencia para la aplicación móvil mediante un archivo de clave o un código de activación:

- Si su organización implementó el software Kaspersky Security Center, debe aplicar el fichero llave y distribuirlo entre las aplicaciones móviles Android. La clave de licencia se muestra en la interfaz de Kaspersky Security Center y en la interfaz de la aplicación móvil Android como una secuencia alfanumérica única.

  Después de agregar claves de licencia, las puede sustituir por otras.

  No puede activar la aplicación Kaspersky Protection para iOS con un archivo de clave.

- Si su organización no utiliza Kaspersky Security Center, debe compartir el código de activación con el usuario. El usuario ingresa este código de activación en la aplicación móvil de Android o iOS. La clave de licencia se muestra en la interfaz de la aplicación móvil como una secuencia alfanumérica única.

Kaspersky puede bloquear la clave de licencia, por ejemplo, en caso de incumplimiento de las condiciones del Contrato de licencia de usuario final. Si la clave de licencia está bloqueada, las aplicaciones móviles dejan de realizar todas sus funciones excepto la sincronización con el Servidor de administración. Para continuar usando las aplicaciones, deberá agregar una clave de licencia diferente.

Acerca del código de activación

El *código de activación* es una secuencia única de 20 caracteres alfanuméricos. Usted ingresa un código de activación para agregar una clave que activa la aplicación móvil Kaspersky Endpoint Security para Android o Kaspersky Protection para iOS. Recibirá el código de activación en la dirección de correo electrónico que especificó después de adquirir la solución integrada MDM básico en Kaspersky Next Expert View (on-premise) o de solicitar la versión de prueba de MDM básico en Kaspersky Next Expert View (on-premise).

Para activar la aplicación móvil mediante un código de activación, necesita acceso a Internet para conectarse con los servidores de activación de Kaspersky.

Si ha perdido el código de activación tras haber activado la aplicación, se puede restaurar. Es posible que necesite el código de activación, por ejemplo para registrarse en Kaspersky CompanyAccount. Para restaurar el código de activación, póngase en contacto con el Servicio de soporte técnico de Kaspersky.

Acerca del archivo de clave

Un *fichero llave* es un archivo con la extensión .key que le proporcionará Kaspersky. El objetivo del fichero llave es agregar una clave que active la aplicación Kaspersky Endpoint Security para Android.

No puede activar la aplicación Kaspersky Protection para iOS con un archivo de clave.

Recibirá un archivo de clave en la dirección de correo electrónico que proporcionó cuando compró la solución integrada MDM básico en Kaspersky Next Expert View (on-premise) o cuando solicitó su versión de prueba.

Para activar la aplicación con un fichero llave no hace falta conectarse a los servidores de activación de Kaspersky.

Puede restaurar un archivo de clave si se ha eliminado accidentalmente. Es posible que necesite un fichero llave para registrar una Kaspersky CompanyAccount, por ejemplo.

Para recuperar el archivo de clave, realice cualquiera de las siguientes acciones:

- Póngase en contacto con el vendedor de la licencia.
- Use su código de activación para recibir un archivo de clave a través del sitio web de Kaspersky.

Provisión de datos en Kaspersky Endpoint Security para Android

El MDM básico en Kaspersky Next Expert View (on-premise) cumple con el Reglamento general de protección de datos (RGPD).

Para instalar la aplicación, usted o el usuario del dispositivo deben leer y aceptar los términos del Contrato de licencia de usuario final. Además, puede configurar una política para aceptar las declaraciones enumeradas a continuación de forma global, para todos los usuarios. De lo contrario, los usuarios recibirán una notificación en la pantalla principal de la aplicación para aceptar las siguientes declaraciones con respecto al procesamiento de los datos personales del usuario:

- Declaración de Kaspersky Security Network
- Declaración sobre el tratamiento de datos para Protección web
- Declaración sobre el procesamiento de datos para propósitos de marketing

Si elige aceptar las declaraciones de forma global, las versiones de las declaraciones aceptadas a través de Kaspersky Security Center deben coincidir con las versiones ya aceptadas por los usuarios. De lo contrario, se les informará a los usuarios sobre el problema y se les pedirá que acepten la versión de una declaración que coincida con la versión aceptada globalmente por el administrador. El estado del dispositivo en el complemento Kaspersky Mobile Devices Protection and Management también cambiará a *Advertencia*.

El usuario puede aceptar las condiciones de una declaración o rechazarlas en cualquier momento en la sección **Acerca de la aplicación** en la configuración de Kaspersky Endpoint Security para Android.

Intercambio de información con Kaspersky Security Network

Para mejorar la protección en tiempo real, Kaspersky Endpoint Security para Android utiliza el servicio en la nube de Kaspersky Security Network para el funcionamiento de los siguientes componentes:

- **Antimalware**. La aplicación obtiene acceso a la base de conocimientos en línea de Kaspersky para consultar por la reputación de los archivos y aplicaciones. El análisis busca amenazas cuya información aún no se ha agregado a las bases de datos antimalware, pero que ya está disponible en KSN. El servicio en la nube de Kaspersky Security Network garantiza el funcionamiento completo del antimalware y reduce la probabilidad de falsas alarmas.
- **Protección web y Control web.** La aplicación usa datos recibidos de KSN para analizar sitios web antes de que se abran. La aplicación también determina la categoría del sitio web para controlar el acceso a Internet de usuarios según listas de categorías permitidas y bloqueadas (por ejemplo, la categoría "Comunicación por Internet").
- **Control de aplicaciones**. La aplicación determina la categoría de la aplicación para restringir el inicio de las que no cumplan con los requisitos de seguridad corporativa según listas de categorías permitidas y bloqueadas (por ejemplo, la categoría "juegos").

La información sobre los tipos de datos enviados a Kaspersky cuando se utiliza KSN durante el funcionamiento de Antimalware y Control de aplicaciones está disponible en el Contrato de licencia de usuario final. Al aceptar los términos y las condiciones del Contrato de licencia, acepta transferir esta información.

La información sobre los tipos de datos enviados a Kaspersky cuando se usa KSN durante el funcionamiento de Protección web está disponible en la Declaración sobre el procesamiento de datos para Protección web. Al aceptar los términos y las condiciones de la Declaración, acepta transferir esta información.

Encontrará información sobre el tipo de datos estadísticos enviados a Kaspersky al usar KSN durante el funcionamiento de la aplicación móvil Kaspersky Endpoint Security para Android en la Declaración de Kaspersky Security Network. Al aceptar los términos y las condiciones de la Declaración, acepta transferir esta información.

Divulgación de datos según el Contrato de licencia de usuario final

Cuando el Código de activación se utiliza para activar el Software, a fin de verificar el uso legítimo del Software, el Usuario final acepta proporcionar periódicamente al Titular de los derechos la siguiente información:

- formato de los datos en la solicitud a la infraestructura del Titular de los derechos; dirección IPv4 del servicio web a la cual se accedió; tamaño del contenido de la solicitud a la infraestructura del Titular de derechos; ID de protocolo; código de activación del software; tipo de compresión de datos; ID de Software; conjunto de ID del Software que se pueden activar en el dispositivo del usuario; localización del Software; versión completa del Software; ID de dispositivo único; fecha y hora en el dispositivo del usuario; ID de instalación de Software (PCID); versión del SO, número de compilación del SO, número de actualización del SO, edición del SO, información ampliada sobre la edición del SO; modelo de dispositivo; familia de sistemas operativos; formato de los datos en la solicitud a la infraestructura del Titular de los derechos; tipo de suma de comprobación para el objeto que se está procesando; encabezado de licencia de Software; ID de un centro de activación regional; fecha y hora de creación de la clave de licencia del Software; ID de licencia de Software; ID del modelo de información utilizado para proporcionar la licencia del Software; fecha y hora de caducidad de la licencia de Software; estado actual de la clave de licencia del Software; tipo de licencia de Software utilizada; tipo de licencia utilizada para activar el Software; ID de Software derivado de la licencia.

A fin de proteger a la computadora contra las amenazas a la seguridad de la información, el Usuario Final acuerda proporcionarle periódicamente al Titular del Derecho la siguiente información:

- tipo de suma de comprobación para el objeto que se está procesando; suma de comprobación del objeto que se está procesando; ID del componente de Software;

- ID del registro activado en las bases de datos antimalware del Software; marca de tiempo del registro activado en las bases de datos antimalware del Software; tipo de registro activado en las bases de datos antimalware del Software; nombre del malware o software legítimo detectado que puede usarse para dañar el dispositivo o los datos del usuario;

- nombre de la tienda desde la que se instaló la aplicación; nombre del paquete de la aplicación; clave pública utilizada para firmar el archivo APK; suma de comprobación del certificado utilizado para firmar el archivo APK; marca de tiempo del certificado digital;

- versión completa del Software; ID de actualización de Software; tipo de Software instalado; identificador de configuración; resultado de la acción del Software; código de error;

- números que se obtienen del archivo APK de la aplicación de Android de acuerdo con ciertas reglas matemáticas y que no permiten la restauración del contenido del archivo original; estos datos no contienen nombres de archivos, rutas de archivos, direcciones, números de teléfono u otra información personal de los usuarios.

Si Usted utiliza los servidores de actualización del Titular de los derechos para descargar las Actualizaciones, el Usuario final, para aumentar la eficiencia del procedimiento de actualización, acepta proporcionar periódicamente al Titular de los derechos la siguiente información:

- ID de Software derivado de la licencia; versión completa del Software; ID de licencia de Software; tipo de licencia de Software utilizada; ID de instalación de Software (PCID); ID del inicio de la actualización del Software; dirección web que se está procesando.

El Titular del derecho también puede utilizar dicha información para recibir información estadística sobre la distribución y el uso del software.

La información recibida es protegida por Kaspersky de acuerdo con los requisitos establecidos por ley. La información recibida original se guarda en forma cifrada y se destruye a medida que se acumula (dos veces por año) o a petición del Usuario. Las estadísticas generales se almacenan indefinidamente.

Divulgación de datos según la declaración de Kaspersky Security Network

El uso de KSN podría aumentar la eficacia de la protección proporcionada por el Software contra amenazas de seguridad de red y de la información.

Si usa una licencia para 5 o más nodos, el Titular de los derechos recibirá y procesará automáticamente los siguientes datos mientras use KSN:

- ID del registro activado en las bases de datos antimalware del Software; registro de hora del registro activado en las bases de datos antimalware del Software; tipo del registro activado en las bases de datos antimalware del Software; fecha y hora del lanzamiento de las bases de datos del Software; versión del SO, número de compilación del SO, número de actualización del SO, edición del SO, información extendida sobre la edición del SO, versión del Service Pack del SO; características de detección; suma de comprobación (MD5) del objeto en procesamiento; nombre del objeto en procesamiento; bandera de indicio de que el objeto en procesamiento es un archivo PE; suma de comprobación (MD5) de la máscara que bloqueó el servicio web; suma de comprobación (SHA256) del objeto en procesamiento; tamaño del objeto en procesamiento; código de tipo del objeto; decisión del Software sobre el objeto en procesamiento; ruta al objeto en procesamiento; código de directorio; versión del componente del Software; versión de las estadísticas en envío; dirección accedida del servicio web (URL, IP); tipo de cliente usado para acceder al servicio web; dirección IPv4 del servicio web accedida; dirección IPv6 del servicio web accedida; dirección web del origen de la solicitud del servicio web (referer); dirección web en procesamiento.

- Información acerca de objetos analizados (versión de la aplicación de AndroidManifest.xml; decisión del Software sobre la aplicación; método utilizado para obtener la decisión del Software sobre la aplicación; nombre del paquete de instalación de la tienda; nombre del paquete de AndroidManifest.xml; categoría de Google SafetyNet; marca que indique si SafetyNet está habilitado en el dispositivo; valor de SHA256 de la respuesta de Google SafetyNet; esquema de firma del APK para el certificado APK; código de la versión del Software instalado; número de serie del certificado usado para firmar el archivo APK; nombre del archivo APK en instalación; ruta al archivo APK en instalación; emisor del certificado usado para firmar el archivo APK; clave pública usada para firmar el archivo APK; suma de comprobación del certificado usado para firmar el archivo APK; fecha y hora de caducidad del certificado; fecha y hora de emisión del certificado; versión de las estadísticas en envío; algoritmo para calcular la huella dactilar del certificado digital, hash MD5 del archivo APK instalado; hash MD5 del archivo DEX ubicado en el archivo APK; permisos otorgados dinámicamente por la aplicación; versión de software de terceros; marca que indica si la aplicación es el servicio de mensajería SMS predeterminado; marca que indica si la aplicación tiene derechos del Administrador del dispositivo; marca que indica si la aplicación está en el catálogo del sistema; marca que indica si la aplicación usa servicios de accesibilidad).

- Información acerca de todos los objetos y actividades potencialmente maliciosos (contendido fragmentado del objeto procesado; fecha y hora de caducidad del certificado; fecha y hora de emisión del certificado; ID de la clave del keystore usado para el cifrado; protocolo usado para intercambiar datos con el KSN; orden de los fragmentos en el objeto procesado; datos del registro interno, generados por el módulo del Software antimalware para un objeto procesado; nombre del emisor del certificado; clave pública del certificado; algoritmo de cálculo de la clave pública del certificado; número de serie del certificado; fecha y hora de la firma del objeto; configuración y nombre del propietario del certificado; huella dactilar del certificado digital del objeto analizado y algoritmo de hashing; fecha y hora de la última modificación del objeto procesado; fecha y hora de creación de un objeto procesado; objetos y sus partes procesados; descripción de un objeto en proceso según se lo define en las propiedades del objeto; formato del objeto procesado; suma de comprobación para el objeto procesado; suma de comprobación (MD5) del objeto procesado; nombre del objeto procesado; suma de comprobación (SHA256) del objeto procesado; tamaño del objeto procesado; nombre del proveedor del Software; decisión del Software sobre el objeto procesado; versión del objeto procesado; origen de la decisión tomada para el objeto procesado; suma de comprobación del objeto procesado; nombre de la aplicación principal; ruta al objeto procesado; información acerca de los resultados de la comprobación de la firma del archivo; clave de sesión de acceso; algoritmo de cifrado para la clave de sesión de acceso; tiempo de almacenamiento para el objeto procesado; algoritmo para el cálculo de la huella dactilar del certificado digital).

- Tipo de compilación, por ejemplo, "usuario" o "eng"; nombre completo del producto; fabricante del producto/hardware; se pueden instalar aplicaciones de clima por fuera de Google Play; estado del servicio de la nube para la verificación de las aplicaciones de Google; estado del servicio de la nube para la verificación de las aplicaciones de Google instaladas a través de ADB; clave de desarrollo actual o "REL" para compilaciones de producción; número de compilación incremental; cadena de caracteres de versión visible para el usuario; nombre del dispositivo del usuario; ID de compilación del Software visible para el usuario; huella digital del firmware; ID del firmware; bandera de indicio de que el rooting del dispositivo está activo; sistema operativo nombre del Software; tipo de licencia de Software utilizada.

- Información acerca de la calidad de los servicios de KSN (protocolo usado para intercambiar datos con KSN; ID del servicio de KSN que accede el Software; fecha y hora en que se dejaron de recibir estadísticas; número de conexiones de KSN tomadas de la caché; número de solicitudes para las que se encontró una respuesta en la base de datos de solicitudes local; número de conexiones de KSN sin éxito; número de transacciones de KSN sin éxito; distribución temporal de solicitudes a KSN canceladas; distribución temporal de conexiones de KSN sin éxito; distribución temporal de transacciones de KSN sin éxito; distribución temporal de conexiones de KSN exitosas; distribución temporal de transacciones de KSN exitosas; distribución temporal de solicitudes a KSN exitosas; distribución temporal de solicitudes a KSN pausadas; número de conexiones de KSN nuevas; número de solicitudes a KSN sin éxito causadas por errores de enrutamiento; número de solicitudes sin éxito causadas por la inhabilitación de KSN en la configuración del Software; número de solicitudes a KSN sin éxito causadas por problemas de red; número de conexiones a KSN exitosas; número de transacciones de KSN exitosas; número total de solicitudes a KSN; fecha y hora en que se comenzaron a recibir las estadísticas).

- ID del dispositivo; versión completa del Software; ID de actualización del Software; ID de instalación del Software (PCID); tipo de Software instalado.

- Altura de la pantalla del dispositivo; ancho de la pantalla del dispositivo; información sobre la aplicación superpuesta: hash MD5 del archivo APK; información sobre la aplicación superpuesta: hash MD5 del archivo classes.dex; información sobre la aplicación superpuesta: nombre del archivo APK; información sobre la aplicación superpuesta: ruta del archivo APK sin el nombre del archivo; altura de la superposición; información sobre el Software superpuesto: hash MD5 del archivo APK; información sobre la aplicación superpuesta: hash MD5 del archivo classes.dex; información sobre la aplicación superpuesta: nombre del archivo APK; información sobre la aplicación superpuesta: ruta del archivo APK sin el nombre del archivo; información sobre la aplicación superpuesta: nombre del paquete de la aplicación (para la aplicación superpuesta: si el anuncio se muestra en un escritorio vacío, el valor debe ser "iniciador"); fecha y hora de la superposición; información sobre la aplicación superpuesta: nombre del paquete de la aplicación; ancho de la superposición.

- Configuración del punto de acceso de Wi-Fi en uso (tipo de dispositivo detectado; configuración del DHCP (sumas de comprobación de la puerta de enlace local IPv6, DHCP IPv6, DNS1 IPv6, DNS2 IPv6; suma de comprobación de la extensión del prefijo de red; suma de comprobación de dirección local IPv6); configuración del DHCP (sumas de comprobación de la dirección IP local de la puerta de enlace, DHCP IP, DNS1 IP, DNS2 IP y máscara de subred); marca que indica si existe el dominio DNS; suma de comprobación de la dirección IPv6 local asignada; suma de comprobación de la dirección IPv4 local asignada; marca que indica si el dispositivo está enchufado; tipo de autenticación de red Wi-Fi; lista de redes Wi-Fi disponibles y sus configuraciones; suma de comprobación (MD5 con sal) de la dirección MAC del punto de acceso; suma de comprobación (SHA256 con sal) de la dirección MAC del punto de acceso; tipos de conexión admitidos por el punto de acceso de Wi-Fi; tipo de cifrado de la red Wi-Fi; hora local del inicio y finalización de la conexión a la red Wi-Fi; ID de la red Wi-Fi basada en la dirección MAC del punto de acceso; ID de la red Wi-Fi basada en el nombre de la red Wi-Fi; ID de la red Wi-Fi basada en el nombre de la red Wi-Fi y la dirección MAC del punto de acceso; potencia de la señal de Wi-Fi; nombre de la red Wi-Fi; serie de protocolos de acceso que admite esta configuración; protocolo de autenticación usado para una conexión WPA-EAP; protocolo de autenticación interno; serie de cifrados de grupo que admite esta configuración; serie de protocolos de administración de claves que admite esta configuración; categoría de privacidad final de la red en el Software; categoría de seguridad final de la red en el Software; serie de cifrados en bloque para WPA que admite esta configuración; serie de protocolos de seguridad que admite esta configuración).

- fecha y hora de instalación del Software; fecha de activación del Software; identificador de la organización asociada a través de la cual se realizó el pedido de licencia de Software; ID de Software derivado de la licencia; número de serie de la clave de licencia del Software; localización del Software; mensaje que indica si la participación en KSN está habilitada; ID del Software con licencia; ID de licencia de Software; ID del SO; versión de bits del sistema operativo.

Además, a fin de alcanzar el propósito declarado de aumentar la eficacia de la protección que proporciona el Software, es posible que el Titular del Derecho reciba objetos que los intrusos podrían aprovechar para dañar la Computadora y representar amenazas a la seguridad de la información.

Proporcionar a KSN la información indicada anteriormente es de carácter voluntario. Puede dejar de participar en Kaspersky Security Network en cualquier momento.

Si no se acepta la última versión de la Declaración de Kaspersky Security Network, solo se envían a Kaspersky Security Network las estadísticas enumeradas en la versión aceptada anteriormente.

Divulgación de datos según la declaración sobre el procesamiento de datos para Protección web

De acuerdo con la Declaración de Protección Web, el Titular del derecho procesa los datos para la funcionalidad de Protección Web. El propósito declarado incluye la detección de amenazas web y la determinación de las categorías de sitios web visitados mediante Kaspersky Security Network (KSN).

Con su consentimiento, los siguientes datos se enviarán automáticamente de forma regular al Titular de derechos en virtud de la Declaración de protección web:

- Versión del producto; Identificador único del dispositivo; ID de instalación; Tipo de producto.

- dirección URL de la página, número de puerto, protocolo de la URL, URL, que hace referencia a la información solicitada.

Divulgación de datos según la declaración sobre el procesamiento de información para propósitos de marketing

El Titular del derecho utiliza sistemas de información de terceros para procesar datos. Su procesamiento de datos se rige por declaraciones de privacidad de dichos sistemas de información de terceros. A continuación figuran los servicios que utiliza el Titular del derecho y los datos que estos procesan:

Google Analytics para Firebase

Durante el uso del Software, se enviarán los siguientes datos a Google Analytics para Firebase automáticamente y de manera periódica a fin de alcanzar el propósito declarado:

- información de la aplicación (versión de la aplicación, ID de la aplicación e ID de la aplicación en el servicio de Firebase, ID de instancia en el servicio de Firebase, nombre de la tienda donde se obtuvo la aplicación, marca de tiempo del primer lanzamiento del Software)
- El ID de instalación de la aplicación en el dispositivo y el método de instalación en el dispositivo
- información acerca de la región y localización del idioma
- información acerca de la resolución de la pantalla del dispositivo
- información sobre el usuario que obtiene raíz
- información sobre la configuración de Kaspersky Endpoint Security para Android como una función de accesibilidad
- información sobre las transiciones entre las pantallas de la aplicación, duración de la sesión, inicio y final de una sesión de pantalla, nombre de la pantalla
- información acerca del protocolo utilizado para enviar datos al servicio de Firebase, su versión e ID del método de envío de datos utilizado
- detalles sobre el tipo y los parámetros del evento para el cual se envían los datos
- información acerca de la licencia de la app, su disponibilidad, la cantidad de dispositivos
- información sobre la frecuencia de las actualizaciones de las bases de datos antimalware y sincronización con el Servidor de administración
- información acerca de la Consola de administración (Kaspersky Security Center o sistemas EMM de terceros)
- ID de Android
- ID de publicidad
- información sobre el usuario: categoría de edad y sexo, identificador del país de residencia y lista de intereses
- información sobre el equipo del usuario donde está instalado el Software: nombre del fabricante del equipo, tipo de equipo, modelo, versión y el idioma (configuración regional) del sistema operativo, información sobre la aplicación que se abrió por primera vez en los últimos 7 días y la aplicación se abrió por primera vez hace más de 7 días

  La transmisión de datos a Firebase se realiza a través de un canal seguro. La información sobre cómo se procesan los datos en Firebase está publicada en: https://firebase.google.com/support/privacy.

Firebase Performance Monitoring

Durante el uso del Software, se enviarán los siguientes datos a Firebase Performance Monitoring automáticamente y de manera periódica a fin de lograr el propósito declarado:

- ID de instalación único
- nombre del paquete de la aplicación
- versión del software instalado
- nivel de batería y estado de carga de la batería
- proveedor
- estado en primer o segundo plano de la aplicación
- geografía
- Dirección IP
- código de idioma del dispositivo
- información sobre la conexión de radio/red
- ID de instancia de Software seudónimo
- tamaño de RAM y del disco
- mensaje que indica si el dispositivo está liberado o tiene acceso a los permisos de administración (root)
- fuerza de la señal
- duración de los rastros automatizados
- red y la siguiente información correspondiente: código de respuesta, tamaño de carga en bytes, tiempo de respuesta
- descripción del dispositivo

  La transmisión de datos a Firebase Performance Monitoring se realiza a través de un canal seguro. La información sobre cómo se procesan los datos en Firebase Performance Monitoring está publicada en: https://firebase.google.com/support/privacy.

Crashlytics

Durante el uso del Software, se enviarán los siguientes datos a Crashlytics automáticamente y de manera periódica a fin de lograr el propósito declarado:

- ID del software
- versión del software instalado
- mensaje que indica si el Software estaba en ejecución en segundo plano
- arquitectura de la CPU
- ID de evento único

- fecha y hora del evento
- modelo de dispositivo
- espacio total del disco y cantidad usada actualmente
- nombre y versión del SO
- RAM total y cantidad usada actualmente
- mensaje que indica si el dispositivo tiene acceso a los permisos de administración (root)
- orientación de la pantalla al momento del evento
- fabricante del producto/hardware
- ID de instalación único
- versión de las estadísticas enviadas
- tipo de excepción de Software
- texto del mensaje de error
- marca que indica que la excepción de Software fue provocada por una excepción anidada
- ID de subproceso
- marca que indica si el marco fue el motivo del error de Software
- marca que indica que el subproceso provocó el cierre inesperado del Software
- información sobre la señal que provocó el cierre inesperado del Software: nombre de la señal, código de la señal, dirección de la señal
- para cada cuadro asociado con un subproceso, una excepción o un error: nombre del archivo del cuadro, número de línea del archivo del cuadro, símbolos de depuración, dirección y desplazamiento en la imagen binaria, nombre de visualización de la biblioteca que incluye el cuadro, tipo de cuadro, mensaje que indica si el cuadro fue la causa del error
- ID del SO
- ID del problema asociado con el evento
- información sobre los eventos que ocurrieron antes de que el Software se cerrara inesperadamente: identificador del evento, fecha y hora del evento, tipo y valor del evento
- valores de registro de la CPU
- tipo y valor del evento

  La transmisión de datos a Crashlytics se realiza a través de un canal seguro. La información sobre cómo se procesan los datos en Crashlytics se publica en: https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

Proporcionar la información anterior para procesamiento con fines de marketing es voluntario.

Provisión de datos en Kaspersky Protection para iOS

El MDM básico en Kaspersky Next Expert View (on-premise) cumple con el Reglamento general de protección de datos (RGPD).

Para instalar la aplicación, el usuario de un dispositivo debe leer y aceptar los términos de las siguientes declaraciones acerca del procesamiento de los datos personales del usuario:

- Contrato de licencia de usuario final
- Política de Privacidad de Productos y Servicios

De modo opcional, el usuario puede leer y aceptar los términos de la siguiente declaración:

- Declaración de Kaspersky Security Network
- Declaración de Soporte

El usuario puede ver los términos de estos documentos en cualquier momento, en la sección **About the App** → **Agreements and Statements** dentro de la configuración de Kaspersky Protection para iOS. En esta sección, el usuario también puede aceptar o rechazar los términos de la Declaración de KSN.

Intercambio de información con Kaspersky Security Network

Para mejorar la protección en tiempo real, Kaspersky Protection para iOS utiliza el servicio en la nube de Kaspersky Security Network para el funcionamiento del componente **Protección web**. La aplicación usa datos recibidos de KSN para analizar recursos web antes de que se abran.

La información sobre los tipos de datos enviados a Kaspersky cuando se utiliza KSN durante el funcionamiento de Protección web está disponible en el Contrato de licencia de usuario final. Al aceptar los términos y las condiciones del Contrato de licencia, acepta transferir esta información.

Encontrará información sobre el tipo de datos estadísticos enviados a Kaspersky al usar KSN durante el funcionamiento de la aplicación móvil Kaspersky Protection para iOS en la Declaración de Kaspersky Security Network. Al aceptar los términos y las condiciones de la Declaración, acepta transferir esta información.

Divulgación de datos según el Contrato de licencia de usuario final

Cuando el código de activación se utiliza para activar el Software, a fin de verificar el uso legítimo del Software, el Usuario final acepta proporcionar periódicamente al Titular de los derechos la siguiente información:

- Formato de los datos en la solicitud a la infraestructura del Titular de los derechos; dirección IPv4 del servicio web a la que se accedió; tamaño del contenido de la solicitud a la infraestructura del Titular de los derechos; ID de protocolo; código de activación del Software; tipo de compresión de datos; ID de Software; conjunto de identificadores de Software que se pueden activar en el dispositivo del usuario; localización del Software; versión completa del Software; ID de dispositivo único; fecha y hora en el dispositivo del usuario; ID de instalación de Software (PCID); código de activación del Software utilizado actualmente; versión del SO, número de compilación del SO, número de actualización del SO, edición del SO, información ampliada sobre la edición del SO; modelo de dispositivo; código del operador de telefonía móvil; familia de sistemas operativos; ID de Software derivado de la licencia; lista de acuerdos presentados al usuario por el Software; tipo de acuerdo legal aceptado por el usuario al usar el Software; versión del acuerdo legal aceptado por el usuario al usar el Software; mensaje que indica si el usuario aceptó los términos del acuerdo legal al usar el Software; tipo de suma de comprobación para el objeto que se está procesando; encabezado de licencia de Software; ID de un centro de activación regional; fecha y hora de creación de la clave de licencia del Software; ID de clave de licencia de Software; ID del modelo de información utilizado para proporcionar la clave de licencia del Software; fecha y hora de caducidad de la clave de licencia de Software; estado actual de la clave de licencia del Software; tipo de clave de licencia de Software utilizada; tipo de clave de licencia utilizada para activar el Software; ID de Software derivado de la clave de licencia.

El Titular del Derecho también puede usar dicha información para obtener datos estadísticos sobre la distribución y el uso de Software del Titular de los derechos.

A fin de proteger a la computadora contra las amenazas a la seguridad de la información, el Usuario Final acuerda proporcionarle periódicamente al Titular del Derecho la siguiente información:

- Formato de los datos en la solicitud a la infraestructura del Titular de los derechos; dirección del servicio web a la que se accedió (URL, IP); número de puerto; dirección web del origen de la solicitud de servicio web (referencia).

- Versión completa del Software; ID de actualización de Software; tipo de Software instalado; ID de software; identificador de configuración; resultado de la acción del Software; código de error.

- Dirección web en procesamiento; dirección IPv4 del servicio web a la que se accedió; huella digital del certificado del objeto analizado y algoritmo hash; tipo de certificado; contenido del certificado digital que se está procesando.

Divulgación de datos según la declaración de Kaspersky Security Network

Cuando se acepta la Declaración de KSN, el Titular de los derechos recibe y procesa automáticamente los siguientes datos:

- Información acerca de la calidad de los servicios de KSN (protocolo usado para intercambiar datos con KSN; ID del servicio de KSN que accede el Software; fecha y hora en que se dejaron de recibir estadísticas; número de conexiones de KSN tomadas de la caché; número de solicitudes para las que se encontró una respuesta en la base de datos de solicitudes local; número de conexiones de KSN sin éxito; número de transacciones de KSN sin éxito; distribución temporal de solicitudes a KSN canceladas; distribución temporal de conexiones de KSN sin éxito; distribución temporal de transacciones de KSN sin éxito; distribución temporal de conexiones de KSN exitosas; distribución temporal de transacciones de KSN exitosas; distribución temporal de solicitudes a KSN exitosas; distribución temporal de solicitudes a KSN pausadas; número de conexiones de KSN nuevas; número de solicitudes a KSN sin éxito causadas por errores de enrutamiento; número de solicitudes sin éxito causadas por la inhabilitación de KSN en la configuración del Software; número de solicitudes a KSN sin éxito causadas por problemas de red; número de conexiones a KSN exitosas; número de transacciones de KSN exitosas; número total de solicitudes a KSN; fecha y hora en que se comenzaron a recibir las estadísticas).

- ID del dispositivo; versión completa del Software; ID de actualización del Software; ID de instalación del Software (PCID); tipo de Software instalado.

- Fecha y hora de instalación del Software; fecha de activación del Software; localización del Software; mensaje que indica si la participación en KSN está habilitada; ID del Software con licencia; ID de licencia de Software; ID del SO; versión del sistema operativo instalado en el equipo del usuario; versión de bits del sistema operativo.

Proporcionar a KSN la información indicada anteriormente es de carácter voluntario. Puede dejar de participar en Kaspersky Security Network en cualquier momento.

Provisión de datos según la Declaración de soporte

Cuando el diagnóstico se habilita en Kaspersky Protection para iOS, la aplicación procesa y almacena los siguientes datos personales para que el Servicio de soporte técnico los analice:

- Fecha y hora del evento.

- Códigos HTTP y datos para solicitudes del servidor a los sistemas del Titular de los derechos: cuerpo de la solicitud; URL de solicitud; respuestas del servidor; errores.

- Datos de todas las solicitudes de red: URL de solicitud; estado de control de tráfico.

- Información de licencia: ID de licencia y código de activación; período de validez del paquete de datos de licencia actual; estado actual de la clave de software; modo de funcionamiento después de que caduca la licencia; fecha de activación del Software; fecha de caducidad de la licencia; número de pedido al comprar la licencia.

- Información sobre la conexión con el Servidor de administración: contraseña del certificado; dirección de conexión del Servidor de administración; ID de dispositivo único; datos de los certificados de los usuarios; datos de certificados del Servidor de administración; configuración de Software recibida del Servidor de administración.

- Eventos del sistema: apertura y cierre del Software; notificaciones push del Software.
- Información sobre el funcionamiento del Software y sus módulos.
- Versión del SO; tipo de SO.
- ID de dispositivo; tipo de dispositivo.
- ID de software; ID de idioma del Software; versión del Software; ID de instalación del Software.
- Información acerca de errores del Software.

Proporcionar al Servicio de soporte técnico la información indicada anteriormente es de carácter voluntario.

Contacto con el Servicio de soporte técnico

En esta sección se describen las distintas formas de obtener Servicio de soporte técnico y las condiciones en las que se encuentra disponible.

Cómo obtener servicio de soporte técnico

Si no encuentra una solución a su problema en la documentación del MDM básico en Kaspersky Next Expert View (on-premise) ni en ninguna de las fuentes de información sobre el MDM básico en Kaspersky Next Expert View (on-premise), comuníquese con Soporte técnico. Los especialistas de Soporte técnico responderán todas sus preguntas sobre la instalación y el uso del MDM básico en Kaspersky Next Expert View (on-premise).

Kaspersky brinda soporte para el MDM básico en Kaspersky Next Expert View (on-premise) durante su vida útil (página de vida útil del soporte del producto). Antes de comunicarse con el Servicio de soporte técnico, lea las reglas del soporte técnico.

Para comunicarse con Soporte técnico, puede elegir alguna de estas opciones:

- Visitando el sitio web del Servicio de soporte técnico
- Enviando una solicitud al Servicio de soporte técnico desde el portal de Kaspersky CompanyAccount

Soporte técnico a través de Kaspersky CompanyAccount

Kaspersky CompanyAccount es un portal para las empresas que utilizan las aplicaciones Kaspersky. El portal Kaspersky CompanyAccount está diseñado para facilitar la interacción entre los usuarios y los especialistas de Kaspersky mediante solicitudes en línea. Puede usar Kaspersky CompanyAccount para hacer un seguimiento del estado de sus solicitudes en línea y almacenar un historial de ellas también.

Puede registrar a todos los empleados de su organización en una cuenta única en Kaspersky CompanyAccount. Una cuenta única le permite administrar de forma centralizada las solicitudes electrónicas enviadas por los empleados registrados a Kaspersky y además administrar los privilegios de estos empleados a través de Kaspersky CompanyAccount.

El portal Kaspersky CompanyAccount está disponible en los idiomas siguientes:

- Inglés
- Español
- Italiano
- Alemán

- Polaco
- Portugués
- Ruso
- Francés
- Japonés

Para obtener más información sobre Kaspersky CompanyAccount, visite el sitio web de Soporte técnico.

Fuentes de información acerca de la aplicación

Página web del MDM básico en Kaspersky Next Expert View (on-premise) en el sitio web de Kaspersky

En la página del MDM básico en Kaspersky Next Expert View (on-premise), podrá encontrar información general sobre la aplicación, sus funciones y sus parámetros de funcionamiento.

La página web del MDM básico en Kaspersky Next Expert View (on-premise) proporciona un vínculo a eStore. Donde podrá comprar la aplicación o hacer la renovación.

Página web del MDM básico en Kaspersky Next Expert View (on-premise) en la Base de conocimientos

La *Base de conocimientos* es una sección en el sitio web del Servicio de atención al cliente de Kaspersky.

En la página del MDM básico en Kaspersky Next Expert View (on-premise) en la Base de conocimientos podrá encontrar artículos con información útil, recomendaciones y respuestas a las preguntas más frecuentes sobre la compra, la instalación y el uso de la aplicación.

Los artículos de la Base de conocimientos pueden responder preguntas relacionadas no solo con el MDM básico en Kaspersky Next Expert View (on-premise), sino también con otras aplicaciones de Kaspersky. Además, los artículos de la Base de conocimientos pueden incluir noticias de soporte técnico.

Ayuda

La ayuda de la aplicación incluye archivos de ayuda.

La ayuda en línea de las aplicaciones Kaspersky Endpoint Security para Android y Kaspersky Protection para iOS proporciona información sobre cómo configurar y usar las aplicaciones móviles.

Discusión sobre aplicaciones de Kaspersky en el Foro de asistencia de Kaspersky

Si su pregunta no requiere una respuesta inmediata, puede tratarla con los expertos de Kaspersky y con otros usuarios en nuestro foro.

En el Foro puede ver los temas de debate, dejar sus comentarios y crear nuevos temas de debate.

Glosario

Activación de la aplicación

Habilitar el modo de funcionalidad completa para la aplicación. El usuario puede activar la aplicación durante la instalación o después de ella. Debe tener un código de activación o archivo de clave para activar la aplicación.

Código de activación

Un código que recibe al comprar una licencia para Kaspersky Endpoint Security. Este código se requiere para activar la aplicación.

El código de activación es una secuencia única de veinte letras y números en el formato xxxxx-xxxxx-xxxxx-xxxxx.

Grupo de administración

Conjunto de dispositivos administrados como, por ejemplo, dispositivos móviles agrupados según las funciones que realicen y las aplicaciones instaladas en ellos. Los dispositivos administrados se agrupan para poder gestionarse como si fueran uno. Por ejemplo, los dispositivos móviles que se ejecutan en el mismo sistema operativo se pueden combinar en un grupo de administración. Un grupo puede incluir otros grupos de administración. Es posible crear directivas de grupo y enviar comandos a los dispositivos del grupo.

Servidor de Administración

Componente de Kaspersky Security Center que almacena de manera central la información de todas las aplicaciones Kaspersky instaladas en la red corporativa. También puede utilizarse para administrar estas aplicaciones.

Estación de trabajo del administrador

El equipo en el que se desplegó Kaspersky Next Expert View (on-premise). Mediante la estación de trabajo del administrador, con los complementos de administración móviles instalados, el administrador realiza la administración centralizada de los dispositivos móviles.

Perfil de trabajo de Android

Un perfil autónomo que se puede configurar en un dispositivo Android para garantizar la separación de los datos relacionados con el trabajo de los datos personales. El perfil de trabajo de Android permite a las organizaciones tener el control total de las aplicaciones y los datos de trabajo en un dispositivo, mientras que las aplicaciones y los datos personales del usuario permanecen privados.

Bases de datos antimalware

Bases de datos que contienen información sobre amenazas de seguridad informática que Kaspersky conocía en el momento del lanzamiento de las bases de datos antimalware. Las entradas en las bases de datos antimalware permiten detectar código malicioso en los objetos analizados. Los expertos de Kaspersky crean las bases de datos antimalware y las actualizan cada hora.

Certificado de servicio de Apple Push Notification (APNs)

Certificado firmado por Apple que le permite utilizar Apple Push Notification. A través de Apple Push Notification, un servidor de MDM para iOS y iPadOS puede administrar los dispositivos iOS y iPadOS.

Control básico

Un modo de funcionamiento del dispositivo para dispositivos iOS personales. Este modo de funcionamiento permite realizar la protección y la administración básica de los dispositivos.

Protección básica

Un modo de funcionamiento del dispositivo para dispositivos iOS personales. Este modo de funcionamiento le permite aplicar la protección contra amenazas web y la detección de jailbreak en dispositivos que utilizan Kaspersky Protection para iOS.

Solicitud de firma de certificado

Archivo con la configuración de un Servidor de administración que es aprobado por Kaspersky y luego enviado a Apple para obtener un certificado de APNs.

Control de cumplimiento

Verifica que un dispositivo móvil y Kaspersky Endpoint Security para Android cumplan con los requisitos de seguridad corporativa. Los requisitos de seguridad corporativos regulan el uso de dispositivos. Por ejemplo, la protección en tiempo real debe estar habilitada en el dispositivo, las bases de datos antimalware deben estar actualizadas y la contraseña del dispositivo debe ser lo suficientemente segura. El Control de cumplimiento se basa en la lista de reglas. Una regla de cumplimiento incluye los componentes siguientes:

- Criterio de verificación del dispositivo (por ejemplo, ausencia de aplicaciones prohibidas en el dispositivo)
- Intervalo de tiempo designado para que el usuario solucione el incumplimiento (por ejemplo, 24 horas)
- Acción que se realizará en el dispositivo si el usuario no soluciona el incumplimiento en el plazo determinado (por ejemplo, bloquear el dispositivo)

Contenedor corporativo

El perfil de Android for Work es un entorno seguro del dispositivo del usuario en el que el administrador puede administrar las aplicaciones y cuentas de usuario sin restringir el uso de datos personales por parte del usuario. Cuando se crea un contenedor corporativo en el dispositivo móvil del usuario, se instalan las siguientes aplicaciones corporativas automáticamente en el contenedor corporativo: Google Play Market, Google Chrome, Descargas, Kaspersky Endpoint Security para Android y otras. Las aplicaciones corporativas instaladas en el contenedor corporativo y las notificaciones de estas aplicaciones se marcan con un ícono de maletín. Debe crear una cuenta corporativa de Google separada para la aplicación Google Play. Las aplicaciones instaladas en el contenedor corporativo aparecen en la lista común de aplicaciones.

Dispositivo corporativo

Un modo de funcionamiento del dispositivo para dispositivos Android propiedad de la empresa. Este modo de funcionamiento le permite tener control total sobre todo el dispositivo y configurar un conjunto extendido de configuraciones y funciones de seguridad.

Administrador del dispositivo

Un conjunto de derechos de aplicaciones en un dispositivo Android que permite que la aplicación utilice directivas de gestión de dispositivos. Es necesario implementar todas las funciones de Kaspersky Endpoint Security en los dispositivos Android.

Contrato de licencia de usuario final

El contrato entre usted y Kaspersky AO que estipula los términos bajo los cuales puede usar la aplicación.

Tarea de grupo

Tarea pensada para un grupo de administración y ejecutada en todos los dispositivos gestionados que se incluyen en el grupo.

IMAP

Protocolo para acceder al correo electrónico. En contraste con el protocolo POP3, IMAP proporciona capacidades extendidas para trabajar con buzones de correo, como la administración de carpetas y el manejo de mensajes sin copiar su contenido del servidor de correo. El protocolo IMAP usa el puerto 143.

Paquete de instalación

Conjunto de archivos creados para la instalación remota de una aplicación de Kaspersky mediante el sistema de administración remoto. Se crea un paquete de instalación en función de los archivos dedicados incluidos en el paquete de distribución de la aplicación. El paquete de instalación contiene una serie de opciones necesarias para instalar la aplicación y ejecutarla de inmediato tras la instalación. Los valores de configuración del kit de distribución corresponden a los valores predeterminados de la configuración de la aplicación.

Dispositivo con MDM de iOS

Un dispositivo móvil iOS controlado por el servidor de MDM de iOS.

Servidor de MDM para iOS

Un componente de Kaspersky Endpoint Security que se instala en un dispositivo del cliente y permite la conexión de dispositivos móviles iOS al Servidor de administración y la administración de esos dispositivos móviles iOS mediante el servicio Apple Push Notifications (APNs).

Categorías de Kaspersky

Categorías de datos predefinidas desarrolladas por especialistas de Kaspersky. Las categorías se pueden actualizar durante las actualizaciones de la base de datos de la aplicación. Un encargado de la seguridad no puede modificar ni eliminar categorías predefinidas.

Kaspersky Private Security Network (KPSN)

Kaspersky Private Security Network es una solución que proporciona a los usuarios de dispositivos que tengan instaladas aplicaciones de Kaspersky acceso a las bases de datos de reputación de Kaspersky Security Network y otros datos estadísticos, sin enviar datos desde sus dispositivos a Kaspersky Security Network. Kaspersky Private Security Network está diseñado para clientes corporativos que no pueden participar en Kaspersky Security Network por alguna de las siguientes razones:

- Los dispositivos no están conectados a Internet.
- La transmisión de cualquier dato fuera del país o de la LAN corporativa está prohibida por la ley o las directivas de seguridad corporativas.

Administrador de Kaspersky Security Center

La persona que administra las operaciones de la aplicación a través del sistema centralizado de administración remota de Kaspersky Security Center.

Servidor web de Kaspersky Security Center

Un componente de Kaspersky Security Center que se instala con el Servidor de administración. Web Server está diseñado para la transmisión, a través de una red, de paquetes de instalación independientes, perfiles de administración y archivos desde una carpeta compartida.

Kaspersky Security Network (KSN)

Una infraestructura de servicios en la nube que proporciona acceso a la base de datos de Kaspersky con información constantemente actualizada sobre la reputación de los archivos, recursos web y software. Kaspersky Security Network garantiza respuestas más rápidas de las aplicaciones de Kaspersky frente a amenazas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de falsos positivos.

Servidores de actualización de Kaspersky

Los servidores HTTP en Kaspersky desde los cuales las aplicaciones de Kaspersky descargan actualizaciones de la base de datos y del módulo de la aplicación.

Archivo de clave

Un archivo en formato xxxxxxxx.key que permite el uso de una aplicación de Kaspersky según una licencia de prueba o comercial. La aplicación genera el archivo de clave según el código de activación. Solo puede usar la aplicación cuando tenga un archivo de clave.

Licencia

Un derecho limitado para usar la aplicación concedido por el Contrato de licencia de usuario final.

Período de validez de la licencia

Un período durante el cual tiene acceso a las funciones de la aplicación y el derecho a usar servicios adicionales. Los servicios que puede usar dependen del tipo de licencia.

Malware

Un programa que infecta a otros, agregándoles su código para tener control cuando se ejecutan archivos infectados. La definición simple permite identificar la acción principal realizada por cualquier malware: la infección.

Perfil de administración

Perfil que contiene un conjunto de valores de configuración para conectar dispositivos móviles iOS con el Servidor de Administración. Un perfil de administración permite distribuir perfiles de configuración de iOS en segundo plano mediante el Servidor de MDM para iOS y también recibir información de diagnóstico ampliada sobre los dispositivos móviles. Se debe enviar un vínculo al perfil de administración para que el Servidor de MDM para iOS pueda detectar y conectar el dispositivo móvil iOS del usuario.

Archivo de manifiesto

Un archivo en formato PLIST que contiene un vínculo al archivo de la aplicación (archivo IPA) ubicado en un servidor web. Lo utilizan los dispositivos iOS para localizar, descargar e instalar aplicaciones desde un servidor web.

Complemento de administración móvil

Un componente específico que proporciona la interfaz para administrar dispositivos móviles a través de Kaspersky Next Expert View (on-premise).

Agente de red

Componente de Kaspersky Security Center que permite la interacción entre el Servidor de administración y las aplicaciones de Kaspersky instaladas en un nodo de red específico (estación de trabajo o servidor).

Dispositivo personal

Un modo de funcionamiento del dispositivo para dispositivos Android personales. Este modo de funcionamiento permite realizar la protección y la administración básica de los dispositivos.

Phishing

Tipo de estafa en Internet destinada a obtener el acceso no autorizado a los datos confidenciales de los usuarios.

Directiva

Conjunto de configuración de la aplicación y de aplicaciones móviles de Kaspersky Endpoint Security aplicado a los dispositivos de los grupos de administración o a dispositivos por separado. Pueden aplicarse distintas directivas a distintos grupos de administración. Una directiva incluye la configuración de todas las funciones de las aplicaciones móviles de Kaspersky Endpoint Security.

POP3

Protocolo de red usado por un cliente de correo para recibir mensajes de un servidor de correo.

Servidor proxy

Un servicio de red informática que permite a los usuarios hacer peticiones indirectas a otros servicios de red. Primero, un usuario se conecta a un servidor proxy y solicita un recurso (por ejemplo, un archivo) ubicado en otro servidor. Luego el servidor proxy se conecta al servidor especificado y obtiene dicho recurso o devuelve el recurso de su propio caché (si el proxy tiene un caché propio). En algunos casos, la solicitud del usuario o la respuesta del servidor pueden ser modificadas por el servidor proxy con ciertos propósitos.

Cuarentena

La carpeta a la cual la Aplicación de Kaspersky mueve objetos posiblemente infectados que se han detectado. Los objetos se almacenan en Cuarentena en forma cifrada para evitar cualquier impacto en el equipo.

SSL

Protocolo de cifrado de datos utilizado en Internet y redes locales. El protocolo Capa de sockets seguros (Secure Sockets Layer, SSL) se utiliza en aplicaciones web para crear una conexión segura entre un cliente y servidor.

Paquete de instalación independiente

Archivo de instalación de Kaspersky Endpoint Security para el sistema operativo Android que contiene la configuración de conexión de la aplicación al Servidor de Administración. Se crea sobre la base del paquete de instalación de esta aplicación y es un caso particular de paquete de aplicación móvil.

Suscripción

Permite el uso de la aplicación dentro de los parámetros seleccionados (fecha de caducidad y número de dispositivos). Puede pausar o reanudar su suscripción, renovarla automáticamente o cancelarla.

Dispositivo supervisado

Dispositivo iOS y iPadOS cuya configuración es supervisada por Apple Configurator, un programa de configuración de grupos de dispositivos iOS y iPadOS. Un dispositivo supervisado tiene el estado *supervisado* en Apple Configurator. Cada vez que un dispositivo supervisado se conecta a un equipo, Apple Configurator comprueba la configuración del dispositivo conforme a la configuración de referencia especificada y, si es necesario, la redefine. Un dispositivo supervisado no se puede sincronizar con Apple Configurator instalado en otro equipo.

Cada dispositivo supervisado ofrece más ajustes que se pueden redefinir mediante la directiva de Kaspersky Device Management para iOS que un dispositivo no supervisado. Por ejemplo, puede configurar un servidor proxy HTTP para supervisar el tráfico de Internet en un dispositivo dentro de la red corporativa. De forma predeterminada, ningún dispositivo móvil se supervisa.

Código de desbloqueo

Un código que puede obtener en Kaspersky Security Center. Es necesario desbloquear un dispositivo después de ejecutar los comandos **Bloquear y Localizar**, **Alarma** o **Foto de identificación** y cuando se activa la Autoprotección.

Servidor de administración virtual

Componente de Kaspersky Security Center diseñado para administrar el sistema de protección de la red de una organización cliente.

El Servidor de administración virtual es una clase particular de Servidor de administración secundario. En comparación con un Servidor de administración físico, los servidores de administración virtuales tienen las siguientes restricciones:

- El Servidor de administración virtual puede crearse solamente en un Servidor de administración principal.
- El Servidor de administración virtual usa la base de datos del Servidor de administración principal. Los servidores de administración virtuales no son compatibles con la tarea de copia de seguridad y restauración de datos ni con la tarea de búsqueda y descarga de actualizaciones.
- El Servidor virtual no admite la creación de Servidores de administración secundarios (incluidos los Servidores virtuales).

Información sobre código de terceros

Puede descargar y leer información sobre el código de terceros en los siguientes archivos:

- legal_notices_Android.txt (para la aplicación Kaspersky Endpoint Security para Android)
- legal_notices_iOS.txt (para la aplicación Kaspersky Protection para iOS)
- legal_notices_KMDPM.txt (para el complemento Kaspersky Mobile Devices Protection and Management)
- legal_notices_iOS_MDM.txt (para el Servidor de MDM para iOS y el complemento de configuración del Servidor de MDM para iOS)

En dispositivos móviles, la información acerca del código de terceros está disponible en la sección **About the App** de las aplicaciones móviles.

Avisos de marcas comerciales

Las marcas registradas y las marcas de servicio son propiedad de sus respectivos titulares.

Adobe, Flash y PostScript son marcas comerciales registradas o marcas comerciales de Adobe en los Estados Unidos y/o en otros países.

AMD64 es una marca comercial o una marca comercial registrada de Advanced Micro Devices, Inc.

Amazon, Amazon EC2, Amazon Web Services, AWS y AWS Marketplace son marcas comerciales de Amazon.com, Inc. o sus filiales.

Apache es una marca comercial registrada o una marca comercial de Apache Software Foundation en los Estados Unidos o en otros países.

Apple, Apple Configurator, AirDrop, AirPlay, AirPort, AirPort Express, AirPrint, Aperture, App Store, Apple Music, Apple TV, Apple Watch, AppleScript, Bonjour, Face ID, FaceTime, FileVault, Find My, Find My Friends, Handoff, iBeacon, iBooks, iBooks Store, iCal, iCloud, iCloud Keychain, iMessage, iPad, iPadOS, iPhone, iPhoto, iTunes, iTunes Store, iTunes U, Keychain, macOS, OS X, Safari, Siri, Spotlight y Touch ID son marcas comerciales de Apple Inc.

La palabra, la marca y los logotipos de Bluetooth son propiedad de Bluetooth SIG, Inc.

Aironet, Cisco, IOS y Cisco AnyConnect son marcas comerciales registradas o marcas comerciales de Cisco Systems, Inc. o sus empresas afiliadas en los Estados Unidos y otros países.

Debian es una marca registrada de Software in the Public Interest, Inc.

Dell Technologies, Dell, SecurID y otras marcas comerciales son marcas comerciales de Dell Inc. o sus subsidiarias.

F5 es una marca comercial de F5 Networks, Inc. en EE. UU. y en otros países.

Google, Android, Chrome, Chromebook, Chromium, Crashlytics, Firebase, Gmail, Google Analytics, Google Assistant, Google Chrome, Google Mail, Google Maps, Google Mobile, Google Play, Google Safe Browsing, Google SafeSearch, Google Translate, Nexus, SPDY y YouTube son marcas comerciales de Google LLC.

HTC es una marca comercial o una marca comercial registrada en los EE. UU. y/o en otros países de HTC Corporation y sus filiales.

HUAWEI y EMUI son marcas comerciales de Huawei Technologies Co., Ltd.

Juniper Networks, Juniper y JUNOS son marcas comerciales o marcas comerciales registradas de Juniper Networks, Inc. en los Estados Unidos y otros países.

Linux es una marca comercial registrada de Linus Torvalds en EE. UU. y en otros países.

Mail.ru es una marca comercial de Mail.ru LLC.

Microsoft, Active Directory, ActiveSync, Bing, Forefront, Microsoft Edge, Outlook, SQL Server, Tahoma, Windows, Windows Mobile, Windows Phone y Windows Server son marcas comerciales del grupo de empresas Microsoft.

MOTOROLA y el logo de Stylized M son marcas comerciales o marcas comerciales registradas de Motorola Trademark Holdings, LLC.

Mozilla y Firefox son marcas comerciales de Mozilla Foundation en los EE. UU. y otros países.

OPPO es una marca comercial o una marca comercial registrada de Guangdong OPPO Mobile Telecommunications Co., Ltd.

Oracle y JavaScript son marcas comerciales registradas de Oracle o sus empresas afiliadas.

Red Hat y Red Hat Enterprise Linux son marcas comerciales o marcas registradas de Red Hat, Inc. o sus filiales en Estados Unidos y otros países.

La marca comercial de BlackBerry es propiedad de Research In Motion Limited y se encuentra registrada en los Estados Unidos y puede estar pendiente o registrada en otros países.

Samsung es una marca comercial de SAMSUNG en los Estados Unidos y en otros países.

SonicWALL, Aventail y SonicWALL Mobile Connect son marcas comerciales de SonicWall, Inc.

Symantec es una marca comercial o marca comercial registrada de Symantec Corporation o de sus empresas afiliadas en los Estados Unidos y otros países.

La marca comercial Symbian es propiedad de Symbian Foundation Ltd.