

The Kaspersky logo is displayed in a bold, lowercase, sans-serif font. It is positioned within a white, rounded rectangular area that serves as a background for the text. The overall page has a green gradient background with a white, torn-paper-like shape in the center.

kaspersky

MDM básico en Kaspersky Next Expert View (cloud)

© 2026 AO Kaspersky Lab

Contenido

[Basic MDM in Kaspersky Next Expert View \(cloud\) help](#)

[What's new](#)

[Comparison of solution features by management tool](#)

[Working in Kaspersky Next Expert View \(cloud\)](#)

[About Basic MDM in Kaspersky Next Expert View \(cloud\)](#)

[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](#)

[Configuring Administration Server settings for connecting mobile devices](#)

[Scenario: Configuring a connection gateway to connect mobile devices to Kaspersky Next Expert View \(cloud\)](#)

[Adding a license key to the Administration Server repository](#)

[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](#)

[Viewing the list of installed iOS MDM Servers and configuring their settings](#)

[Receiving or renewing an APNs certificate](#)

[Installing an APNs certificate on iOS MDM Server](#)

[iOS MDM Server events](#)

[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](#)

[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](#)

[Managing mobile devices in Kaspersky Next Expert View \(cloud\)](#)

[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 \(cloud\)](#)

[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](#)

[Configuring certificate issuance rules](#)

[Issuing mobile device certificates](#)

[Renewing mobile device certificates](#)

[Deleting mobile device certificates](#)

[Viewing the list of mobile device certificates](#)

[Configuration and management](#)

[Control](#)

[Configuring restrictions](#)

[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](#)

[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](#)

[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](#)

[Participating in Kaspersky Security Network](#)

[Information exchange with Kaspersky Security Network](#)

[Enabling and disabling the use of Kaspersky Security Network](#)

[Samsung Knox](#)

[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 (cloud)

 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.
 Implementación Aprenda a desplegar la solución en su organización y a configurar sistemas de administración para dispositivos Android y dispositivos iOS.	 Configurar los ajustes del dispositivo Administre dispositivos móviles de forma remota: configure una conexión Wi-Fi, el correo electrónico, clips web y más.
 Comandos Administre los dispositivos móviles de forma remota con comandos móviles. Bloquear dispositivo, Eliminar datos corporativos, Localizar dispositivo, Tomar fotos, Activar alarma, y más.	 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.
 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.

Novedades

Versión 1.0

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

- La interfaz del complemento Kaspersky Mobile Devices Protection and Management ahora es compatible con nuevos idiomas:
 - Español (México)
 - Portugués (Brasil)
- 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	Kaspersky Security Center Web Console		Kaspersky Security Center Web Console		Kaspersky Security Center Cloud Console	
	MDM avanzado en Kaspersky Next Expert View (on-premise)	Kaspersky Secure Mobility Management (on-premise)	MDM básico en Kaspersky Next Expert View (on-premise)	Kaspersky Security para dispositivos móviles (local)	MDM básico en Kaspersky Next Expert View (cloud)	Kaspersky Security para dispositivos móviles (nube)
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	✓	✓	✓
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 reglas de concesión de permisos para aplicaciones instaladas	✓	—	—
Configurar contenedores corporativos	✓	✓ 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 mediante 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 (cloud)

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

Acerca del MDM básico en Kaspersky Next Expert View (cloud)

El MDM básico en Kaspersky Next Expert View (cloud) 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.

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:
 - **Localizar dispositivo.** Le permite obtener las coordenadas de la ubicación del dispositivo.
 - **Activar alarma.** Provoca que el dispositivo emita un sonido de alarma fuerte.
 - **Eliminar datos corporativos.** Borra 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 (cloud) 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 (cloud) 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 (cloud). 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.

El complemento Kaspersky Mobile Devices Protection and Management se puede instalar al configurar Kaspersky Next Expert View (cloud).

Requisitos de hardware y software

En esta sección, se enumeran los requisitos de hardware y software para los sistemas operativos de dispositivos móviles compatibles con MDM básico en Kaspersky Next Expert View (cloud).

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
- 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, 26.1, 26.2, 26.3, 26.4, 26.5
 - iPadOS:
 - iPadOS 15.x
 - iPadOS 16.x
 - iPadOS 17.x
 - iPadOS 26.2, 26.4
- Conexión a Internet

Requisitos de hardware y software para un perfil de administración

Para un perfil de administración, el dispositivo móvil debe cumplir 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
- Conexión a Internet

Compatibilidad con otros sistemas operativos

MDM básico en Kaspersky Next Expert View (cloud) admite 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.

Versión de Kaspersky Endpoint Security para Android	Versión del sistema operativo	Limitaciones
10.571.37	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 Security Center Web Console 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 **Servidor web**.

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 [Forzar sincronización](#) y la casilla [No desconectar del Servidor de administración](#) en la ventana de propiedades del dispositivo no son compatibles con dispositivos móviles. Utilice el comando [Sincronizar dispositivo](#) para forzar la sincronización de un dispositivo Android o un dispositivo MDM con iOS.
- En la lista de dispositivos móviles administrados, la capacidad total de almacenamiento que se muestra para los dispositivos iOS personales que funcionan en el modo "Kaspersky Protection para iOS" 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 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 **Bloquear apps del sistema** en la configuración de [Control de aplicaciones](#) 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.
- **Red personal (cualquiera)WEPWPAConectar automáticamente**En los dispositivos MDM con iOS que ejecutan iOS 18 y iOS 26, si se selecciona el tipo de protección de red Red personal (cualquiera) 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 Conectar automáticamente 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 conocimiento 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](#) ^[1].
- 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](#) ^[2].
- 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](#) ^[3]. 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 **Permitir sitios web indicados únicamente** 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 **Prohibir todos los sitios web**, 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 **Prohibir todos los sitios web**, 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 **Control web** 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 **Agregar a Favoritos del dispositivo** en la tarjeta **Control web** y especifique el nombre del marcador para cada sitio web de la lista.
- Si la opción **Verificar la URL completa al usar pestañas personalizadas** 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 "Kaspersky Protection para iOS", si cambia el idioma del dispositivo o reinicia el dispositivo, 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 **Bloquear apps del sistema**. 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 **Bloquear apps del sistema**. Esto se debe a las limitaciones del sistema operativo Android.
- Cuando se configura un contenedor corporativo en el dispositivo, recomendamos desmarcar la casilla **Bloquear apps del sistema**. El bloqueo de aplicaciones del sistema puede ocasionar problemas durante la creación del contenedor corporativo.
- Si la casilla **Bloquear apps del sistema** 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

- 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 **Mínimo de caracteres especiales** y se marca la casilla **Permitir contraseña simple**, 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 con Android 10 o una versión posterior, no se admite prohibir el 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 **Prohibir la sugerencias de Spotlight** 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 **Localizar dispositivo** falla.
- El comando **Localizar dispositivo** 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.
- El comando **Restablecer ajustes de fábrica** no está disponible para dispositivos personales y dispositivos con un contenedor corporativo con Android 14 o posterior.

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 en el modo de funcionamiento "Perfil de administración" que ejecutan iOS 18.2 - iOS 18.3.1, se puede prohibir el uso de Safari. Esto se debe a un problema reconocido por Apple.

- En ciertos dispositivos personales (por ejemplo, OnePlus, Honor) con Android 10 o posterior, 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 **Forzar sincronización** en la pestaña **General** de las propiedades del host de la puerta de enlace de conexión (**Administración de activos** → **Activos (dispositivos)**).
- Cuando configura un certificado de Servidor web personalizado, si las direcciones de los campos **Dirección del Servidor web** y **Dirección del certificado** 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 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 **Configuración de eventos**, 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 (cloud), así como a los especialistas que brindan soporte técnico a las organizaciones que lo usan.

Arquitectura de la solución

El MDM básico en Kaspersky Next Expert View (cloud) 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 e iOS en Kaspersky Next Expert View (cloud).

- 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 configurar los ajustes del Servidor de MDM para iOS.

Configurar el Servidor de administración para la conexión de dispositivos móviles

Antes de conectar dispositivos móviles a Kaspersky Next Expert View (cloud), 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 (cloud), 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 **Puertos adicionales**.
 - b. Habilite el botón de alternancia **Abrir puerto para dispositivos móviles**.

Si se selecciona esta opción, el puerto para dispositivos móviles se abrirá en el Servidor de administración.
 - c. En el campo **Puerto para la sincronización de dispositivos móviles**, 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 **Abrir puerto para dispositivos móviles** 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 **Certificados**.
- 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 **Guardar** 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 (nube)

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 autenticuen, 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 **Dispositivos administrados** 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 (cloud), 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 **Puerta de enlace de conexión** de las propiedades del punto de distribución. A continuación, habilite las opciones **Abrir puerto para dispositivos móviles (solo autenticación SSL del Servidor de administración)** y **Abrir puerto para dispositivos móviles (autenticación SSL bidireccional)** 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** → **Certificados**). 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 (**Operaciones** → **Repositorios** → **Paquetes de instalación**).

Agregar una clave de licencia al repositorio del Servidor de administración

Para conectar dispositivos móviles a Kaspersky Next Expert View (cloud) 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 extendida de MDM básico en Kaspersky Next Expert View (cloud), 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 (cloud), 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 **Claves de licencia**.
- b. En el bloque de configuración **Licencia actual**, haga clic en **Seleccionar** 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 **Guardar**.

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 (en la nube), seleccione **Operaciones** → **Licencias**.
2. Clic en el botón **Agregar**.
3. En la ventana que se abre, haga clic en el botón **Agregar archivo de clave**.
4. Haga clic en **Seleccionar archivo de clave** 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 **Guardar**.

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

Implementar un sistema de administración de dispositivos iOS

MDM básico en Kaspersky Next Expert View (cloud) 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:

- **Kaspersky Protection para iOS**

Protección contra amenazas web y detección de liberación en dispositivos iOS.

- **Perfil de administración**

Configuración básica y avanzada para administrar dispositivos iOS. Los dispositivos iOS en el modo de funcionamiento "Perfil de administración" solo se pueden agregar al grupo de administración "Dispositivos administrados".

Para conectar dispositivos iOS en el modo de funcionamiento "Perfil de administración", instale el [Servidor de MDM para iOS](#).

Un *dispositivo supervisado* es un dispositivo iOS o iPadOS cuya configuración es supervisada por Apple Configurator, un programa para la configuración grupal 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.

Acerca de los perfiles de administración del dispositivo

Un *perfil de administración del dispositivo* es un perfil que contiene la configuración para conectar dispositivos móviles iOS a Kaspersky Security Center. Después de la instalación del perfil de administración del dispositivo 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 Apple Push Notification (APNs).

Con un perfil de administración del dispositivo, 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 del dispositivo se realiza a través de Kaspersky Next Expert View (nube) mediante el [Asistente de conexión de dispositivos móviles](#). El usuario instala el perfil de administración del dispositivo 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 del dispositivo, debe [desplegar un sistema de administración de dispositivos iOS](#).

Implementar Kaspersky Protection para iOS

Los dispositivos iOS [en el modo de funcionamiento "Kaspersky Protection para iOS"](#) 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 (nube).
- 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 (nube) al especificar los [parámetros de las directivas](#) correspondientes.

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 **Enviar un mensaje a las direcciones de correo electrónico de los usuarios**, 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 **Dispositivos** de Kaspersky Next Expert View (nube).

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 **Mostrar códigos QR y vínculos después de completar el asistente**, 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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Haga clic en el botón **Licencia**.
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 **Reemplazar con la clave seleccionada si la clave en los dispositivos es diferente**.

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 **Guardar** 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 en el modo de funcionamiento "Perfil de administración" 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 [Recibir un certificado de APNs](#)
- 2 [Instalar el certificado de APNs en el Servidor de MDM para iOS](#)
- 3 [Conectar los dispositivos iOS a Kaspersky Security Center](#)

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

Kaspersky Next Expert View (cloud) le permite ver la lista de los 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 (cloud), seleccione **Administración de activos** → **Móviles** → **Servidores de MDM para iOS**.
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 **Instalar**.
 - b. 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 **Modificar configuración**.
Se abre la pestaña **Configuración de la aplicación** 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 **Configuración de la aplicación**.

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

1. Vaya a la pestaña **Configuración de la aplicación** de la ventana de configuración del Servidor de MDM para iOS siguiendo las instrucciones anteriores.
 - a. En la sección **Certificados**, puede administrar los certificados necesarios para el funcionamiento del Servidor de MDM para iOS.
 - **Certificado de Apple Push Notification service (APNs)**. 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](#).

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

- En el bloque de configuración **Sincronización**, puede habilitar o deshabilitar la sincronización de dispositivos administrados con el Servidor de MDM para iOS y especificar el **Período de sincronización (min)**.
- En el bloque de configuración **Perfil de administración de dispositivos**, puede configurar las propiedades del perfil de instalación. Puede especificar el **Nombre de perfil** (un campo obligatorio), la **Empresa** y la **Descripción del perfil**.

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 **Perfiles de configuración**, 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](#).

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 (cloud), seleccione **Administración de activos** → **Móviles** → **Servidores de MDM para iOS**. 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 **Configuración de la aplicación**.
3. Seleccione la pestaña **Certificados**.
4. En el bloque de configuración **Certificado de Apple Push Notification service (APNs)**, haga clic en **Emitir o renovar**.

Se abre el asistente del certificado de APNs. Haga clic en **Iniciar** y luego avance por el asistente con los botones **Atrás** y **Siguiente**.

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. Crear una solicitud de firma de certificado (CSR)

Para crear una CSR, siga estos pasos:

- a. Especifique la información requerida para generar un archivo de solicitud: **Nombre común (CN)**, **Nombre de la organización (O)**, **Unidad organizativa (OU)**, **Ciudad (L)**, **Región (S)**, **País (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. Firmar el archivo CSR

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 **Ir a 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. Recibir la clave pública del certificado APNs

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 **Ir al portal de Apple**.
- 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 **Ir al portal de Apple**.
- 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. Especifique la clave pública del certificado APNs

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

- a. Haga clic en **Seleccionar**.
- 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. Especifique la contraseña de la clave privada del certificado APNs

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

- a. En el campo **Nombre de certificado**, especifique un nombre personalizado para el certificado.
- b. En el campo **Contraseña de la clave privada**, 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 **Confirmar contraseña**, ingrese la contraseña nuevamente.

Paso 6. Finalizar el 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 **Descargar certificado APNs** 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 (nube), seleccione **Administración de activos** → **Móviles** → **Servidores de MDM para iOS**. 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 **Configuración de la aplicación**.
3. Seleccione la pestaña **Certificados**.
4. En el bloque de configuración **Certificado de Apple Push Notification service (APNs)**:
 - a. Haga clic en **Instalar**.
 - 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 **Instalando el certificado** que se abre, ingrese la contraseña de la clave privada especificada al [recibir el certificado de APNs](#) y luego haga clic en **Instalar**.

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

Eventos del Servidor de MDM para iOS

Kaspersky Next Expert View (cloud) 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 **Configuración de eventos** 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 (cloud), seleccione **Administración de activos** → **Móviles** → **Servidores de MDM para iOS**. 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 **Configuración de la aplicación**.
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 (cloud), 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 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_SUCCESSFUL	30 días
Datos del dispositivo móvil borrados	ERASEDEVICE_COMMAND_SUCCESSFUL	30 días
Actualización del sistema operativo programada	SCHEDULEOSUPDATE_COMMAND_SUCCESSFUL	30 días
Configuración de itinerancia aplicada	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	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_CHECKING_RULES_STARTED	30 días
Comprobación de Control de cumplimiento completada	COMPLIANCE_CONTROL_CHECKING_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 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
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

Nombre que se muestra para el tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
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 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

Implementar un sistema de administración de dispositivos Android

MDM básico en Kaspersky Next Expert View (cloud) le permite administrar dispositivos móviles que ejecutan 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

Kaspersky Endpoint Security para Android está instalado en los dispositivos móviles de los usuarios. La aplicación le permite configurar de forma remota los ajustes de los dispositivos, administrar dispositivos de forma centralizada mediante comandos y garantizar la protección de los dispositivos móviles contra amenazas web, virus y otros programas que representan amenazas.

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 (cloud), puede especificar la configuración de Firebase Cloud Messaging que permita 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 (cloud), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
2. Abra el menú de 3 puntos (⋮) y seleccione **Sincronización forzada de dispositivos Android**.
3. En el campo **Número de proyecto de Firebase**, ingrese el id. del remitente de FCM.
4. En el campo **Clave privada**, 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 (nube), 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:
 - **Localizar dispositivo.** Le permite obtener las coordenadas de la ubicación del dispositivo.
 - **Activar alarma.** Provoca que el dispositivo emita un sonido de alarma fuerte.
 - **Eliminar datos corporativos.** Borra 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 (nube) 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 mediante Kaspersky Security Center](#) usando el **sitio web de Kaspersky**

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.

- [Instalación manual](#)

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 **Continuar**.
3. Toque **Continuar** y otorgue a la aplicación los permisos requeridos.
4. En el campo **Servidor**, especifique el vínculo que recibió del administrador.
5. Toque **Continuar**.

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 **Continuar**.

3. Toque **Continuar** y otorgue a la aplicación los permisos requeridos.
4. En el campo **Servidor**, especifique la dirección del servidor de administración que le proporcionó el administrador.
5. Toque **Continuar**.
6. Toque **Habilitar** para habilitar la aplicación como administrador del dispositivo.
7. Toque **Permitir** 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)	Identificar el dispositivo mediante su IMEI (para Android 5 a 9; para Android 10 a 11 en el 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.

Permiso	Función de la aplicación
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
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

Permiso	Función de la aplicación
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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Haga clic en el botón **Licencia**.
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 **Reemplazar con la clave seleccionada si la clave en los dispositivos es diferente**.

5. Haga clic en el botón **Guardar** 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 (cloud), 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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
4. Seleccione **Android** y vaya a la sección **Configuración de KES para Android**.
5. En la tarjeta **Actualización de la app**, haga clic en **Configuración**.
Se abre la ventana **Actualización de la app**.
6. Habilite la configuración con el interruptor **Actualización de la app**.
7. Haga clic en **Seleccionar**.
Se abre la ventana **Seleccionar paquete de instalación**.

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 **Seleccionar**.

10. Haga clic en **Aceptar**.

11. Haga clic en el botón **Guardar** 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 **Configurar el acceso a la configuración de la app** de la sección **Configuración de KES para Android** en la configuración de la directiva.

2. [Eliminación de la aplicación por parte del administrador](#) (solo Android 13 o versiones anteriores)

El administrador elimina la aplicación de forma remota mediante Kaspersky Next Expert View (cloud). 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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Configuración de KES para Android**.
4. En la tarjeta **Configurar el acceso a la configuración de la app**, haga clic en **Configuración**.
Se abre la ventana **Configurar el acceso a la configuración de la app**.
5. Seleccione la casilla **Permitir eliminar la app del dispositivo**.
6. Haga clic en **Aceptar**.
7. Haga clic en el botón **Guardar** 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 **Configuración** → **Configuración de la aplicación** → **Adicional** → **Eliminar aplicación**.
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

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 **Configuración** → **Configuración de la aplicación** → **Adicional** → **Eliminar aplicación**.

Si el botón **Eliminar aplicación** no se muestra, esto significa que el administrador activó la [protección contra la eliminación de Kaspersky Endpoint Security para Android](#).

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

Puede eliminar de forma remota la aplicación Kaspersky Endpoint Security para Android de dispositivos con Android 13 o versiones anteriores enviando el comando **Restablecer ajustes de fábrica**.

Al ejecutar el comando **Restablecer ajustes de fábrica**, 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 (nube), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
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 **Enviar comando**.
4. En la ventana **Enviar comando** que se abre, en el campo **Comando**, seleccione el comando **Restablecer ajustes de fábrica**.
5. Haga clic en **Enviar**.

Puede ver y cancelar comandos en el **Historial de comandos**.

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 **Eliminar**.
El dispositivo se elimina de la lista de dispositivos administrados en Kaspersky Next Expert View (nube).

Si el dispositivo no se elimina de Kaspersky Next Expert View (nube), puede haber problemas con la instalación de aplicaciones de Kaspersky en este dispositivo.

Administración de dispositivos móviles en Kaspersky Next Expert View (cloud)

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 (cloud), seleccione **Administración de activos > Jerarquía de grupos**.
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 **Nombre del nuevo grupo de administración** 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 (cloud), seleccione **Administración de activos > Jerarquía de grupos**.
2. Haga clic en **Importar**.

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 (cloud).

Crear una directiva

Kaspersky Next Expert View (nube) le permite crear directivas para configurar los ajustes de seguridad de un grupo de dispositivos móviles Android y iOS. 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 (nube), seleccione **Administración de activos → Directivas**.
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 **Dispositivos móviles**.

3. Haga clic en **Agregar** para iniciar el Asistente de directivas móviles.
4. En la ventana **Seleccionar aplicación**, 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 **Iniciar** y luego avance por el asistente con los botones **Atrás** y **Siguiente**.

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 forma predeterminada, se preselecciona la licencia que admite la funcionalidad MDM básico en Kaspersky Next Expert View (cloud). Puede seleccionar una licencia diferente manualmente.

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** (protección de dispositivos Android y configuración para el contenedor corporativo)
- **iOS**
 - Kaspersky Protection para iOS (protección contra amenazas web y detección de liberación en dispositivos iOS)
 - Perfil de administración (configuración básica y avanzada para administrar dispositivos iOS)
Para obtener información detallada, consulte la sección [Acerca de los modos de funcionamiento del dispositivo iOS](#).

Para conectar dispositivos iOS en el modo de funcionamiento "Perfil de administración", debe tener instalado [un servidor de MDM para iOS](#).

Para el modo de funcionamiento "Kaspersky Protection para iOS", puede crear un grupo de administración independiente sin servidor de MDM para iOS y distribuir una directiva.

Para el modo de funcionamiento "Perfil de administración", puede crear grupos de administración con diferentes servidores de MDM para iOS y distribuir diferentes directivas, respectivamente.

En la pestaña **General** de la ventana *Nueva directiva*:

1. En el campo **Nombre**, 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 **Estado de la directiva**, seleccione el estado de la directiva:
 - **Activa**. 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.
 - **Inactiva**. 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 **Herencia de configuración**, seleccione las opciones de herencia:

- **Heredar configuración de la directiva primaria**

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.

- **Forzar la herencia de configuración en las directivas secundarias**

Si habilita esta opción en una directiva principal, se habilita la opción **Heredar configuración de la directiva primaria** 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 **Heredar configuración de la directiva primaria** está habilitada y la opción **Forzar la herencia de configuración en las directivas secundarias** está deshabilitada.

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.

Modificar una directiva

Kaspersky Next Expert View (nube) 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 (nube), seleccione **Administración de activos** → **Directivas**. 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 (nube), seleccione **Administración de activos** → **Móviles** → **Dispositivos**. Seleccione el dispositivo móvil al que se aplica la directiva que desee modificar y, luego, seleccione la directiva en la pestaña **Directivas y perfiles de directivas activos**.

2. En la ventana de propiedades de la directiva, vaya a la pestaña **Configuración de la aplicación** 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](#).

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.

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 (cloud) 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 (cloud), seleccione **Administración de activos** → **Directivas**.
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 **Agregar grupo secundario**.
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 (cloud) 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 (cloud), seleccione **Administración de activos** → **Directivas**.
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 **Agregar grupo secundario**.

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 (cloud) 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 (cloud), seleccione **Administración de activos** → **Directivas**.
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 (cloud) 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 (cloud), seleccione **Administración de activos** → **Directivas**.
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 **Distribución**.

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 **Configurar directiva**.

Administrar revisiones de directivas

Kaspersky Next Expert View (cloud) 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 (cloud), seleccione **Administración de activos** → **Directivas**.
2. En la lista de directivas que se abre, haga clic en la directiva cuya revisión desea ver y luego vaya a la sección **Historial de revisiones**.
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 (cloud). 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 **Guardar en archivo**.

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 (cloud) para diferentes funciones de la solución MDM básico en Kaspersky Next Expert View (cloud) según las tareas del trabajo de los usuarios.

En la interfaz de Kaspersky Next Expert View (cloud), puede configurar los derechos de acceso en las pestañas **Seguridad** y **Roles de usuario** de la ventana de propiedades del Servidor de administración. La pestaña **Roles de usuario** 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 (cloud) puede cambiar la configuración de las directivas en la ventana de propiedades.
- **Bloquear modificación.** El usuario de Kaspersky Next Expert View (cloud) 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.

Configurar el control de acceso basado en roles

Kaspersky Next Expert View (cloud) proporciona herramientas para el acceso basado en roles a las funciones de MDM básico en Kaspersky Next Expert View (cloud).

Puede configurar los derechos de acceso a las funciones de la aplicación para MDM básico en Kaspersky Next Expert View (cloud) 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 de MDM básico en Kaspersky Next Expert View (cloud) se enumeran en la siguiente tabla.

Roles de usuario predefinidos para MDM básico en Kaspersky Next Expert View (cloud)

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](#).

Área funcional	Derecho
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (cloud) > 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 (cloud) > Controles de seguridad	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (cloud) > Contenedor corporativo	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (cloud) > Configuración del dispositivo	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (cloud) > Configuración de las aplicaciones de administración de dispositivos de Kaspersky	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (cloud) > Protección	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (cloud) > Restricciones	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (cloud) > Configuración de Samsung Knox	

Derechos de acceso a la Administración de dispositivos móviles

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 (cloud)
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

Configuración de perfiles de directivas

A veces, puede ser necesario crear y modificar de manera centralizada varias instancias de una sola directiva para un grupo de administración. Las versiones de la directiva podrían diferir en uno o dos valores de configuración únicamente.

Para evitar la creación de varias instancias de una sola directiva, Kaspersky Next Expert View (nube) permite crear perfiles de directivas. Los perfiles de directivas permiten que los dispositivos de un mismo grupo de administración operen con diferentes configuraciones de directiva.

Un perfil de directiva es un subconjunto nominado de los valores de configuración definidos en una directiva. Este subconjunto se distribuye en dispositivos de destino junto con la directiva y se complementa bajo una condición específica denominada Condición de activación del perfil. Un perfil contiene solamente los valores de configuración que difieren de los de la directiva "básica" que se encuentra activa en el dispositivo administrado. Cuando el perfil se activa, se modifican los valores de configuración que la directiva "básica" había impuesto inicialmente en el dispositivo. La configuración toma los valores especificados en el perfil.

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:

- **Reglas para un propietario del dispositivo específico**

Activación del perfil en el dispositivo según su propietario.

- Propietario del dispositivo
- El propietario del dispositivo está incluido en un grupo de seguridad interno

- **Reglas para la asignación de roles**

Activación del perfil en el dispositivo según el rol del propietario.

- Activar el perfil de directiva según el rol específico del propietario del dispositivo

- **Reglas para el uso de la etiqueta**

Activación del perfil en el dispositivo en función de las etiquetas asignadas al dispositivo.

- Lista de etiquetas
- Aplicar a los dispositivos que no tengan las etiquetas especificadas

- **Reglas para el uso de Active Directory**

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.

- Membrecía del propietario del dispositivo en un grupo de seguridad de Active Directory
- Membrecía del dispositivo en un grupo de seguridad de Active Directory
- Asignación de dispositivos en la unidad organizativa de Active Directory

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 (cloud) 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.

Para eliminar una directiva:

1. En la ventana principal de Kaspersky Next Expert View (cloud), seleccione **Administración de activos** → **Directivas**.
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 (cloud)

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 (cloud), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
2. En la lista de dispositivos móviles que se abre, haga clic en **Agregar**.
El Asistente para conectar un nuevo dispositivo móvil empieza a ejecutarse. Haga clic en **Iniciar** y luego avance por el asistente con los botones **Atrás** y **Siguiente**.

Bienvenido

En la pantalla de bienvenida, puede leer un resumen de los pasos del asistente de conexión de dispositivos móviles.

Paso 1. Directiva

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](#).

- **Usar una directiva existente**

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 **Ir a la directiva** para ver las propiedades de la directiva que seleccionó.

- **Crear una nueva directiva**

Para esta opción, haga clic en el botón **Crear directiva** 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. Sistemas operativos

En este paso, seleccione los sistemas operativos de los dispositivos que se conectarán. La configuración de la directiva determina los sistemas operativos disponibles: Android o iOS.

- **Android**

- **iOS**

Para conectar dispositivos iOS en el modo de funcionamiento "Perfil de administración", debe tener instalado [un servidor de MDM para iOS](#).

La *aplicación Kaspersky Protection para iOS* se instalará en los dispositivos iOS personales en el modo de funcionamiento "Kaspersky Protection para iOS".

Se instalará un [perfil de administración](#) en los dispositivos en el modo de funcionamiento "Perfil de administración".

En los dispositivos que ejecutan iOS 12.1 o posterior, debe confirmar manualmente la instalación de un perfil de administración de dispositivos en un dispositivo móvil. También debe conceder el permiso para la administración remota del dispositivo.

Paso 3. Aceptar acuerdos

En este paso, seleccione quién debe aceptar el Contrato de licencia de usuario final (EULA) y la Política de privacidad.

- **Administrador**

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.

- **Usuarios**

Los usuarios aceptan los acuerdos en los 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. Contrato de licencia de usuario final y Política de privacidad

En este paso, si se selecciona **Administrador** 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. Usuarios

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 **Agregar usuario**.

a. Especifique las credenciales de usuario en el bloque de configuración **Credenciales**.

- **Nombre de usuario**

- **Contraseña**

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 **Información opcional**.

- **Nombre de usuario completo**
- **Descripción**
- **Dirección de correo electrónico**
- **Número de teléfono**

c. Haga clic en **Aceptar** 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 **Editar usuario**.

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. Enviar detalles de conexión

En este paso, seleccione cómo enviar los códigos QR y los vínculos para instalar las aplicaciones de administración móvil o los perfiles de administración de dispositivos. Puede seleccionar una de las siguientes opciones:

- **Enviar un mensaje a las direcciones de correo electrónico de los usuarios**

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 de dispositivos, 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 **Enviar una copia del mensaje a una dirección de correo electrónico alternativa** y luego especifique la dirección de correo electrónico requerida.

- **Mostrar códigos QR y enlaces después de completar el asistente**

Elija esta opción para analizar el código QR con la cámara del dispositivo móvil o haga clic en el vínculo del asistente.

Paso 7. Confirmar

En este paso, verifique los detalles de conexión del dispositivo móvil especificados en los pasos anteriores y luego haga clic en **Finalizar** 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.

Finalizar

En la pantalla Finalizar:

- Si elige la opción **Enviar un mensaje a las direcciones de correo electrónico de los usuarios**, los usuarios especificados recibirán los correos electrónicos con códigos QR y vínculos para conectar dispositivos móviles al Servidor de administración.
- Si elige la opción **Mostrar códigos QR y enlaces después de completar el asistente**, los detalles de la conexión estarán disponibles en la pantalla Finalizar. Puede ver los detalles que se muestran o hacer clic en **Descargar lista** para recibir un archivo con información resumida.

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 (cloud).

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 **Descubrimiento y despliegue > Dispositivos no asignados** de Kaspersky Next Expert View (cloud). 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 (cloud), seleccione **Descubrimiento y despliegue > Dispositivos no asignados**.
2. Seleccione el dispositivo que desee mover a un grupo de administración y, a continuación, haga clic en **Mover a un grupo**.
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 **Agregar grupo secundario**.
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 del dispositivo.

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.

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 [Sincronizar dispositivo](#) para forzar la sincronización de un dispositivo Android o un dispositivo MDM con iOS.

El botón [Forzar sincronización](#) y la casilla [No desconectar del Servidor de administración](#) 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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Configuración de KES para Android**.
4. En la tarjeta **Sincronización programada**, haga clic en **Configuración**.
Se abrirá la ventana **Sincronización programada**.
5. Habilite la sincronización con el interruptor **Sincronización programada**.
6. En la lista desplegable **Período de sincronización**, 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 **No sincronizar en itinerancia**.

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 **Guardar** 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 de dispositivos iOS que operan en el modo "Kaspersky Protection para iOS":

1. En la ventana principal de Kaspersky Next Expert View (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Configuración de KP para iOS**.
4. En la tarjeta **Sincronización programada**, haga clic en **Configuración**.
Se abrirá la ventana **Sincronización programada**.
5. Habilite la sincronización con el interruptor **Sincronización programada**.
6. En la lista desplegable **Período de sincronización**, 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 **Guardar** 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](#).

Administrar los certificados de dispositivos móviles

Kaspersky Next Expert View (cloud) 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.

Configuración de las reglas de emisión de certificados

Kaspersky Next Expert View (nube) 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 (nube), seleccione **Administración de activos** → **Móviles** → **Certificados**.
2. En la lista de certificados que se abre, haga clic en **Reglas de emisión**.
 - En la sección **Certificados para dispositivos móviles**, puede hacer lo siguiente:
 - a. En el bloque de configuración **Validez**, en el campo **Período de validez del certificado (días)**, 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 **Renovación**, en el campo **Renovar el certificado antes de que caduque en (días)**, 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 **Renovar el certificado automáticamente** 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 **Protección con contraseña**, seleccione la casilla **Solicitar contraseña durante la instalación del certificado** 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 **Longitud de la contraseña**.

La protección con contraseña solo está disponible para certificados de celular.

- 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 (cloud), seleccione **Administración de activos** → **Móviles** → **Certificados**.
2. En la lista de certificados que se abre, haga clic en **Agregar**.
Se inicia el Asistente de emisión de certificados. Haga clic en **Iniciar** y luego avance por el asistente con los botones **Atrás** y **Siguiente**.

Bienvenido

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 [Reglas de emisión](#).

Paso 1. Tipo de certificado

En este paso, elija el certificado que se emitirá.

- **Certificado de correo** (para configurar el correo electrónico corporativo en los dispositivos).
- **Certificado de VPN** (para configurar el acceso a redes privadas y recursos web corporativos en los dispositivos).
- **Certificado para dispositivos móviles** (para identificar dispositivos móviles en el Servidor de administración).

Paso 2. Sistema operativo

En este paso, seleccione el sistema operativo de los dispositivos para los que se emitirá el certificado.

- **Android**
- **iOS**

Paso 3. Método de conexión

Este paso solo se muestra si seleccionó **Certificado de correo** o **Certificado de VPN** 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.

- **Conectar mediante autenticación de certificado para dispositivos móviles**
Seleccione esta opción si desea que el certificado móvil se utilice para identificar al usuario cuando se conecta al Servidor de administración.
- **Conectar sin autenticación de certificado para dispositivos móviles**

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. Usuarios

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 **Agregar usuario**.

a. Especifique las credenciales de usuario en el bloque de configuración **Credenciales**.

- **Nombre de usuario**

- **Contraseña**

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 **Información opcional**.

- **Nombre de usuario completo**
- **Descripción**
- **Dirección de correo electrónico**
- **Número de teléfono**

c. Haga clic en **Aceptar** 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 **Editar usuario**.

Los campos que puede modificar dependen del subtipo de usuario: *interno* o *dominio*.

Paso 5. Alias y origen del certificado

En este paso, elija el alias del certificado y la fuente para importar el certificado.

- **Alias del certificado**

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 **Certificado de correo** o **Certificado de VPN** como el tipo de certificado.

- **Cargar archivo**

Para esta opción, especifique el **Formato del certificado**:

- Para el formato PKCS # 12, en el campo **Archivo de certificado**, haga clic en **Seleccionar** y, a continuación, especifique un archivo P12 o PFX.
- Para el formato X.509, en el campo **Archivo de la clave privada**, haga clic en **Seleccionar** y, a continuación, especifique un archivo PRK o PEM.

En el campo **Archivo de certificado**, haga clic en **Seleccionar** y, a continuación, especifique un archivo CER, CRT o CERT.

Después de especificar los archivos, también puede ingresar la **Contraseña del certificado**.

Paso 6. Método de autenticación

Este paso solo se muestra si seleccionó **Certificado para dispositivos móviles** como tipo de certificado o si seleccionó **Certificado de correo** o **Certificado de VPN** 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.

- **Credenciales de usuario internas o de dominio.** 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
- **Contraseña.** 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 **Uso del certificado en el dispositivo**, haga clic en la casilla **Permitir el uso de un certificado en varias ocasiones dentro del mismo dispositivo (solo para dispositivos con Kaspersky Endpoint Security para Android instalado)** si desea permitir el uso de un certificado 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. Enviar detalles del certificado

En este paso, elija cómo enviar los detalles de instalación del certificado. Puede seleccionar una de las siguientes opciones:

- **Enviar un mensaje a las direcciones de correo electrónico de los usuarios**

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 **Enviar una copia del mensaje a una dirección de correo electrónico alternativa** y luego especifique la dirección de correo electrónico requerida.

- **Mostrar los detalles después de completar el asistente**

Elija esta opción para mostrar los detalles de la instalación del certificado en el paso final del asistente de emisión de certificados.

Paso 8. Confirmar

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.

Finalizar

En la pantalla Finalizar:

- Si elige la opción **Enviar un mensaje a las direcciones de correo electrónico de los usuarios**, los usuarios especificados recibirán los correos electrónicos con los detalles de instalación del certificado.
- Si elige la opción **Mostrar los detalles después de completar el asistente**, los detalles de la instalación del certificado se muestran en la pantalla Finalizar. Puede ver los detalles que se muestran o hacer clic en **Descargar lista** 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 (nube). Si sigue los pasos que se indican a continuación, puede renovar un certificado para dispositivos móviles.

Para renovar un certificado para dispositivos móviles, haga lo siguiente:

1. En la ventana principal de Kaspersky Next Expert View (nube), seleccione **Administración de activos** → **Móviles** → **Certificados**.
2. En la lista de certificados que se abre, seleccione el certificado que desea renovar y luego haga clic en **Renovar**.

El estado del certificado cambia a **Certificado renovado**.

Eliminar certificados de dispositivos móviles

Puede eliminar los certificados para dispositivos móviles mediante Kaspersky Next Expert View (nube).

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 (nube) y ya no se renueva, sino que 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 (nube), 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 (nube) y luego volver a conectarlo mediante el [Asistente de conexión de dispositivos móviles](#).

Para eliminar un certificado de Kaspersky Next Expert View (nube):

1. En la ventana principal de Kaspersky Next Expert View (nube), seleccione **Administración de activos** → **Móviles** → **Certificados**.
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.

Ver la lista de certificados de dispositivos móviles

Kaspersky Next Expert View (cloud) 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 (cloud), seleccione **Administración de activos** → **Móviles** → **Certificados**.
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 (cloud), seleccione **Administración de activos** → **Móviles** → **Certificados**.
2. En la lista de certificados que se abre, seleccione el certificado cuyas propiedades quiera ver.

3. En la ventana **Detalles del certificado**, vea las propiedades del certificado:

- Nombre de usuario
- Estado
- Tipo
- Protocolo
- Origen
- Fecha de caducidad
- Fecha de emisión
- Última actualización de estado
- Alias
- Renovación automática habilitada
- Huella digital

Para ver los certificados instalados en un dispositivo MDM con iOS, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (cloud), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
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 **Certificados**.
Se muestra la lista de certificados instalados en el dispositivo y sus propiedades.

- Nombre de certificado
- Certificado de usuario
- Huella digital del certificado

Configuración y administración

Esta sección está destinada a los especialistas que administran el MDM básico en Kaspersky Next Expert View (cloud), así como a los especialistas que brindan soporte técnico a las organizaciones que lo utilizan.

Control

Esta sección contiene información sobre cómo monitorear dispositivos móviles de forma remota en Kaspersky Next Expert View (nube).

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 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 **Restricciones** 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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Restricciones**.
4. En la tarjeta **Restricciones de funciones del dispositivo**, haga clic en **Configuración**.
Se abre la ventana **Restricciones de funciones del dispositivo**.
5. Habilite la configuración con el interruptor **Restricciones de funciones del dispositivo**.
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 **Configuración del dispositivo**:
 - **Prohibir la marcación por voz en un dispositivo bloqueado**

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.
 - **Limitar seguimiento de anuncios**

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 marcada, 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.

■ Prohibir 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.

■ Prohibir la edición del nombre del dispositivo

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.

■ Prohibir la modificación de restricciones

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.

■ Prohibir la sugerencias de Spotlight

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 **Protección contra pérdida de datos:**

- **Prohibir las capturas y grabaciones de pantalla**

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.

- **Prohibir que las apps no administradas usen documentos de las apps administradas**

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.

- **Prohibir que las apps administradas usen documentos de las apps no administradas**

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:

- **Prohibir que las apps no administradas usen documentos de las apps administradas**
- **Prohibir que las apps administradas usen documentos de las apps no administradas**

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 **Prohibir que las apps no administradas usen documentos de las apps administradas** y **Prohibir que las apps administradas usen documentos de las apps no administradas** tienen efectos diferentes en términos de la capacidad del usuario para usar el portapapeles.

Prohibir que las apps no administradas usen documentos de las apps administradas	Prohibir que las apps administradas usen documentos de las apps no administradas	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.

■ **Deshabilitar el cifrado de copias de seguridad**

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.

■ **Prohibir el restablecimiento de la configuración de fábrica**

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.

■ **Prohibir la modificación de la configuración de la cuenta**

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 no está marcada, el usuario del dispositivo móvil puede añadir nuevas cuentas y editar la configuración de las cuentas existentes.

Si la casilla está marcada, no se permite al usuario del dispositivo móvil añadir nuevas cuentas ni editar la configuración de las cuentas existentes.

Esta casilla está desactivada por defecto.

■ En la sección **Seguridad y privacidad**:

■ **Prohibir el envío de datos personales y de diagnóstico a 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.

■ **Prohibir el cambio de contraseña**

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.

■ **Prohibir la modificación de la configuración de Touch ID y Face ID**

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.

■ **Prohibir el desbloqueo del dispositivo usando Touch ID y 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 está desactivada, el usuario puede utilizar una huella dactilar o reconocimiento facial en lugar de introducir 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.

■ **Solicitar contraseña para cada compra en 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.

■ **Solicitar contraseña ante la primera conexión con 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 está marcada, 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 introducirla 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.

■ **Prohibir la instalación de perfiles de configuración**

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.

■ **Prohibir hosts sin Configurator**

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.

■ **Prohibir la modificación de la configuración para enviar datos de diagnóstico**

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:**

■ **Prohibir copia de seguridad en 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.

■ Prohibir el almacenamiento de documentos y datos en 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.

■ Prohibir llavero de iCloud

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.

■ Prohibir que apps administradas almacenen datos en 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.

■ Prohibir la copia de seguridad de libros empresariales

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.

■ Prohibir la sincronización de notas y fragmentos destacados en libros empresariales

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.

- **Prohibir el intercambio de fotografías de iCloud**

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.

- **Prohibir la biblioteca multimedia de iCloud**

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 **Certificados**:

- **Prohibir que los usuarios acepten certificados TLS no confiables**

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.

- **Prohibir actualizaciones automáticas de certificados de confianza**

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**:

- **Prohibir el uso de la cámara**

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 está marcada, se desactiva 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.

■ **Prohibir FaceTime**

■ **Prohibir 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.

■ **Prohibir 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.

■ **Prohibir la instalación de apps de Apple Configurator y 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.

■ **Prohibir la instalación de apps desde App Store**

Habilidad de instalar independientemente aplicaciones en un dispositivo móvil desde App Store. La casilla está disponible si la casilla **Prohibir la instalación de apps de Apple Configurator y 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.

■ **Prohibir la descarga automática de aplicaciones**

Uso de descargas automáticas de aplicaciones en el dispositivo móvil del usuario. La casilla está disponible si la casilla **Prohibir la instalación de apps de Apple Configurator y 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.

- **Prohibir las compras desde la app**

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.

- **Prohibir confiar en nuevos desarrolladores empresariales**

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.

- **Prohibir la eliminación de 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 **AirDrop**:

- **Prohibir 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.

- **Tratar a AirDrop como una aplicación administrada**

Uso de AirDrop como aplicación administrada para transferir datos desde el dispositivo móvil a otros dispositivos Apple. Esta restricción requiere que seleccione la casilla **Prohibir que las apps no administradas usen documentos de las apps administradas**. 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**:

- **Prohibir 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.

- **Prohibir la radio en 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**:

- **Deshabilitar la detección de muñeca del Apple Watch**

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.

- **Prohibir la sincronización con el 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**:

- **Prohibir 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.

- **Prohibir cuando el dispositivo está bloqueado**

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.

- **Prohibir el uso del filtro de malas palabras**

En desuso en iOS 26.4 y versiones posteriores.

Esta opción desactiva 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.

- **Prohibir que Siri realice búsquedas en Internet**

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 **Buscar mi**:

- **Prohibir la ubicación de dispositivos con Buscar mi**

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.

- **Prohibir la ubicación de amigos con Buscar mi**

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**:

- **Prohibir la visualización de pantalla mediante 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 **Red**:

- En la sección **Datos móviles**:

- **Prohibir la sincronización automática en roaming**

Prohibir la sincronización automática de los datos del usuario cuando el dispositivo MDM de iOS está en itinerancia.

Si la casilla no está marcada, el usuario puede activar 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.

- **Prohibir la modificación de la configuración de datos móviles**

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 **Configuración adicional**:

- En la sección **Pantalla**:

- **Prohibir el cambio de fondo de pantalla**

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 **Texto**:

- **Prohibir el corrector ortográfico**

Obsoleto 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.

- **Prohibir la corrección automática**

Obsoleto 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.

- **Prohibir la búsqueda en el diccionario**

Obsoleto 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 **Teclado**:

- **Prohibir el texto predictivo**

Obsoleto 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.

- **Prohibir los atajos de teclado**

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 **Notificaciones**:

- **Prohibir las notificaciones en pantalla de Wallet cuando la pantalla está bloqueada**

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.

- **Ocultar el Centro de control cuando la pantalla está bloqueada**

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.

- **Ocultar el Centro de notificaciones cuando la pantalla está bloqueada**

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.

- **Ocultar Hoy cuando la pantalla está bloqueada**

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.

■ Prohibir la modificación de la configuración de notificaciones

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.

7. Haga clic en **Aceptar**.

8. Haga clic en el botón **Guardar** 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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.

3. Seleccione **iOS** y vaya a la sección **Restricciones**.

4. En la tarjeta **Restricciones de aplicaciones**, haga clic en **Configuración**.

Se abre la ventana **Restricciones de aplicaciones**.

5. Habilite la configuración con el interruptor **Restricciones de aplicaciones**.

6. Configure las restricciones de aplicaciones del dispositivo MDM con iOS.

Lista de restricciones de aplicaciones

Restricciones en la sección **Safari**:

- **Permitir el uso de 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.

- **Permitir el Relleno automático**

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.

- **Advertir al usuario cuando visite un sitio web peligroso**

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.

- **Permitir 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.

- **Bloquear ventanas emergentes**

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.

- **Configuración de cookies**

Seleccione las condiciones para aceptar cookies:

- **Permitir cookies y seguimiento de sitios web.** El navegador Safari acepta cookies y permite rastrear la actividad del usuario.
- **Permitir cookies y bloquear seguimiento de sitios web.** El navegador Safari acepta cookies y bloquea el seguimiento de la actividad del usuario.
- **Bloquear cookies y seguimiento de sitios web.** El navegador Safari bloquea las cookies y el seguimiento de la actividad del usuario.

El valor predeterminado es **Permitir cookies y seguimiento de sitios web**.

Restricciones en la sección **Game Center**:

- **Permitir uso de 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.

- **Permitir agregar amigos en 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.

- **Permitir juegos multijugador en 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 **Configuración adicional**:

- **Permitir el uso de 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.

- **Permitir el uso de Noticias**

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.

- **Permitir el uso de 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 **Guardar** 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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Restricciones**.
4. En la tarjeta **Restricciones de contenido**, haga clic en **Configuración**.
Se abre la ventana **Restricciones de contenido**.
5. Habilite la configuración con el interruptor de **Restricciones de contenido**.
6. Configure las restricciones de contenido del dispositivo MDM con iOS.

Lista de restricciones de contenido

Región

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 **Clasificación por edades**:

- **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 **Permitir todo** el usuario puede ver cualquier película en el dispositivo móvil.

La opción **Permitir todo** está seleccionada de manera predeterminada.

- **Programas de TV**

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 **Permitir todo** el usuario puede ver cualquier programación de TV en el dispositivo móvil.

La opción **Permitir todo** 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 **Permitir todo** el usuario puede utilizar cualquier aplicación de terceros en el dispositivo móvil.

La opción **Permitir todo** está seleccionada de manera predeterminada.

Las restricciones de la aplicación pueden aplicarse incluso si la opción **Permitir todo** está seleccionada. Esto se debe a un problema reconocido por Apple.

- **Permitir la descarga de contenido erótico en 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.

- **Permitir contenido explícito**

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 **Guardar** 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, "Apuestas, loterías, sorteos" o "Comunicación por Internet"). Control web está activado 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.

Si Kaspersky Endpoint Security para Android no está habilitado como una función de Accesibilidad y hay un proxy habilitado en la tarjeta **Configuración de Google Chrome**, 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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Controles de seguridad**.
4. En la tarjeta **Control web**, haga clic en **Configuración**.
Se abre la ventana **Control web**.

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 **Modo de funcionamiento**, en la lista desplegable, seleccione **Prohibir sitios web de las categorías seleccionadas**.
 - b. En la sección **Categorías**, 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 **Modo de funcionamiento**, seleccione **Permitir sitios web indicados únicamente** o **Permitir todos los sitios web excepto los indicados**.
 - b. Clic en el botón **Agregar**.
 - 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](#) ².

d. Haga clic en **Agregar**.

- Si desea que la app bloquee el acceso del usuario a todos los sitios web, en la sección **Modo de funcionamiento**, en la lista desplegable, seleccione **Prohibir todos los sitios web**.
6. Si desea que la aplicación verifique la URL completa al abrir un sitio web en Pestañas personalizadas, seleccione la casilla **Verificar la URL completa al usar pestañas personalizadas**.

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 **Control web** y haga clic en **Deshabilitar**.

8. Haga clic en **Aceptar**.

9. Haga clic en el botón **Guardar** 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:

- **Agregar**: haga clic para agregar un sitio web a la lista ingresando una URL o una expresión regular.
- **Cargar**: 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.
- **Modificar**: haga clic para cambiar la dirección de un sitio web.
- **Eliminar**: 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 en el modo de funcionamiento "Perfil de administración".

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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Controles de seguridad**.
4. En la tarjeta **Control web**, haga clic en **Configuración**.
Se abre la ventana **Control web**.
5. Habilite la configuración con el interruptor de **Control web**.
6. En la lista desplegable **Modo de funcionamiento**, realice una de las siguientes acciones:
 - Si desea crear una lista de sitios web permitidos, seleccione **Permitir sitios web indicados únicamente**.
 - Si desea crear una lista de sitios web prohibidos, seleccione **Permitir todos los sitios web excepto los indicados**.
7. Haga lo siguiente:
 - a. Clic en el botón **Agregar**.
 - 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 **Agregar a Favoritos del dispositivo** debajo de la dirección del sitio web.
 - c. Haga clic en **Agregar**.

8. Haga clic en **Aceptar**.

9. Haga clic en el botón **Guardar** 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 for 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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Controles de seguridad**.
4. En la tarjeta **Control de cumplimiento**, haga clic en **Configuración**.
Se abre la ventana **Control de cumplimiento**.
5. Habilite la configuración con el interruptor **Control de cumplimiento**.

6. En la sección **Cuando se detecte un incumplimiento**:

- Seleccione la casilla **Notificar al usuario** 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 **Notificar al administrador a través de la sección "Eventos"** para informar al administrador que el dispositivo no cumple con la directiva.

7. Clic en el botón **Agregar**.

Se inicia el Asistente para agregar reglas. 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 **Siguiente** y **Atrás**.

Paso 1. Criterio de incumplimiento

Haga clic en **Agregar criterio** para especificar el criterio de incumplimiento que activa la regla.

Los siguientes criterios están disponibles:

- **La protección en tiempo real está deshabilitada**

Kaspersky Endpoint Security for Android no está instalado o no se está ejecutando en el dispositivo.

- **Las bases de datos antimalware del dispositivo están desactualizadas**

Las bases de datos antimalware se actualizaron por última vez hace 3 días o más.

- **Se instalaron apps prohibidas**

La lista de aplicaciones del dispositivo contiene aplicaciones que están configuradas como prohibidas en la configuración **Control de aplicaciones** de la directiva.

- **Se instalaron apps de categorías prohibidas**

La lista de aplicaciones del dispositivo contiene aplicaciones de las categorías que están establecidas como prohibidas en la configuración de **Control de aplicaciones** de la directiva.

- **No se instalaron todas las apps necesarias**

La lista de aplicaciones del dispositivo no contiene una aplicación que esté establecida como requerida en la configuración de **Control de aplicaciones** de la directiva.

- **La versión del sistema operativo está desactualizada**

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 **Versión mínima** y **Versión máxima**. Si la versión máxima permitida se establece en **Cualquiera**, también se permitirán las versiones futuras de Android compatibles con Kaspersky Endpoint Security for Android.

- **El dispositivo lleva mucho tiempo sin sincronizarse**

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 **Período sin sincronización**.

- **Se detectó acceso root en el dispositivo**

El dispositivo está hackeado (se ha obtenido acceso al root en el dispositivo).

- **La contraseña de desbloqueo no cumple la configuración de seguridad especificada en la directiva**

La contraseña de desbloqueo del dispositivo no es compatible con la configuración definida en la tarjeta **Configuración de desbloqueo de pantalla**.

Paso 2. Respuestas por incumplimiento de los requisitos de seguridad

Añadir las respuestas que se realizarán en el dispositivo si se detecta el criterio de incumplimiento especificado.

Seleccione una de las siguientes opciones:

- **Agregar respuesta instantánea.** La respuesta se aplica instantáneamente después de que se detecta el criterio de incumplimiento.
- **Agregar respuesta diferida.** La respuesta se aplica después de un período de retraso que puede especificar en el campo **Periodo de diferimiento**.

Las siguientes respuestas están disponibles:

- **Bloquear todas las apps excepto las apps del sistema**

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.

- **Bloquear dispositivo**

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 **Desbloquear dispositivo**.

- **Eliminar datos corporativos**

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 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.

- **Restablecer ajustes de fábrica**

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 que ejecutan Android 14 o posterior, esta respuesta no es aplicable.

Haga clic en **Agregar regla** para finalizar el Asistente para agregar reglas. 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.

Haga clic en el botón **Guardar** 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 **Se instalaron apps prohibidas**, **Se instalaron apps de categorías prohibidas** o **No se instalaron todas las apps necesarias**.

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.

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 (en la nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Controles de seguridad**.
4. En la tarjeta **Control de aplicaciones**, haga clic en **Configuración**.
Se abre la ventana **Control de aplicaciones**.
5. Habilite la configuración con el interruptor **Control de aplicaciones**.

6. Ajuste la configuración en las siguientes pestañas:

- Si desea configurar las reglas generales de administración de aplicaciones, **vaya a la pestaña Uso de la app.**

1. En la lista desplegable **Modo de funcionamiento**, 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 **Usar todas las apps excepto las prohibidas**. 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 **Usar solo apps permitidas**. 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 **No bloquear las apps prohibidas, solamente agregar un registro al registro de eventos**.

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 **Bloquear apps del sistema**. Esta casilla se muestra en el modo **Usar solo apps permitidas**.

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. Haga clic en **Agregar** para agregar aplicaciones y categorías para las que desea establecer reglas.

Se abre la ventana **Agregar app o categoría**.

5. En el campo **Objeto**, seleccione **Aplicación** o **Categoría de la app** y haga lo siguiente:

- Si seleccionó **Aplicación**, seleccione un paquete de instalación o especifique el nombre del paquete y el nombre de la aplicación en los campos correspondientes.
- Si seleccionó **Categoría de la app**, seleccione una categoría e ingrese una descripción en los campos correspondientes.
- Clic en el botón **Agregar**.

La aplicación o categoría se agrega a la lista.

6. Si desea recibir informes sobre las aplicaciones instaladas, en la sección **Informe sobre apps instaladas**, seleccione la casilla **Enviar datos sobre las apps instaladas**.

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 Administración de la app**.

1. En la tabla **Acciones para apps**, haga clic en **Agregar**.

2. En la ventana que se abre, haga lo siguiente:

a. En la sección **Acción**, realice una de las siguientes acciones:

- **Instalar**. Se solicita al usuario que instale la aplicación.
- **Eliminar**. La aplicación se eliminará del dispositivo del usuario.
- **Recomendar instalación**. 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.

- **Nombre del paquete**
- **Nombre de la app**
- **Vínculo**

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.

- **Versión**

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 **Vínculo** y **Versión** no se muestran si selecciona **Eliminar** en el campo **Acción**.

c. Clic en el botón **Agregar**.

La acción configurada se agrega a la lista.

7. Haga clic en **Aceptar**.

8. Haga clic en el botón **Guardar** 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 (nube) le permite evaluar rápidamente el nivel de protección actual de los dispositivos móviles administrados en la sección **Administración de activos** → **Móviles** → **Dispositivos**.

Un dispositivo puede tener uno de los siguientes niveles de protección: **Normal**, **Advertencia** o **Crítico**.

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 *Normal*.

Niveles de protección y sus significados

Nivel de protección	Significado
 Normal	No se requiere intervención de un administrador.
 Advertencia	Se registraron eventos relacionados con amenazas posibles o reales para la seguridad de los dispositivos administrados.
 Crítico	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 *Normal* 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.

Condición	Motivo del nivel de protección	Valor predeterminado
Protección en tiempo real no se está ejecutando	Uno de los siguientes motivos: - No se otorgó el permiso Acceso para administrar todos los archivos. - Kaspersky Security Network está desactivado.	<i>Crítico</i>
Protección web y Control web no se están ejecutando	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.	<i>Advertencia</i>
Control de aplicaciones no se está ejecutando	No se concedió el permiso Accesibilidad .	<i>Advertencia</i>
El bloqueo de dispositivo no está disponible	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.	<i>Advertencia</i>
La ubicación de dispositivo no está disponible	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).	<i>Advertencia</i>
Las versiones de la Declaración de Kaspersky Security Network no coinciden	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.	<i>Advertencia</i>
Las versiones de la Declaración de marketing no coinciden	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.	<i>Normal</i>

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 **Eventos**. 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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Controles de seguridad**.
4. En la tarjeta **Control de aplicaciones**, haga clic en **Configuración**.
Se abre la ventana **Control de aplicaciones**.
5. En la sección **Informe sobre apps instaladas**, seleccione la casilla **Enviar datos sobre las apps instaladas**.
6. Si desea recibir datos sobre las aplicaciones del sistema, seleccione la casilla **Enviar datos sobre apps integradas**.
7. Si desea recibir datos sobre aplicaciones de servicio, que no tienen una interfaz y el usuario no puede abrirlas, seleccione la casilla **Enviar datos sobre apps de servicio**.

8. Haga clic en **Aceptar**.

9. Haga clic en el botón **Guardar** 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 remotamente la protección de dispositivos móviles en Kaspersky Next Expert View (nube).

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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Protección**.
4. En la tarjeta **Protección en tiempo real**, haga clic en **Configuración**.

Se abre la ventana **Protección en tiempo real**.

5. Habilite la configuración con el interruptor **Protección en tiempo real**.

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 **Análisis de app**, seleccione el modo de análisis de la aplicación:

- **No analizar apps**
- **Analizar solo las apps y los archivos nuevos en la carpeta Descargas**
- **Analizar todas las apps y supervisar las acciones con archivos**

7. En la lista desplegable **Acción al detectar una amenaza**, seleccione una de las siguientes opciones:

- **Eliminar**

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.

- **Omitir**

Si se han omitido objetos detectados, Kaspersky Endpoint Security for 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.

- **Eliminar el archivo y guardar una copia de seguridad en cuarentena**

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 **Protección adicional de 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 **Detecta adware, marcadores automáticos y apps legítimas que los intrusos pueden utilizar para poner en riesgo el dispositivo y los datos del usuario**.

10. Haga clic en **Aceptar**.

11. Haga clic en el botón **Guardar** 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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.

3. Seleccione **Android** y vaya a la sección **Protección**.

4. En la tarjeta **Analizar**, haga clic en **Configuración**.

Se abre la ventana **Analizar**.

5. Habilite la configuración con el interruptor **Analizar**.

6. En la lista **Acción al detectar una amenaza**, seleccione una de las siguientes opciones:

- **Eliminar**

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.

- **Omitir**

Si se han omitido objetos detectados, Kaspersky Endpoint Security for 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.

- **Eliminar el archivo y guardar una copia de seguridad en cuarentena**

- **Preguntar al usuario**

Kaspersky Endpoint Security para Android muestra una notificación para que el usuario elija la acción que debe hacerse con el objeto detectado: **Omitir** o **Eliminar**.

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 **Eliminar**. 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 **Preguntar al usuario**, 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 **Eliminar el archivo y guardar una copia de seguridad en cuarentena**, 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 **Análisis programado**, puede configurar los 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 **Día** y **Hora**.

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 **Guardar** 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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Protección**.
4. En la tarjeta **Actualización de bases de datos**, haga clic en **Configuración**.
Se abre la ventana **Actualización de bases de datos**.
5. Habilite la configuración con el interruptor **Actualización de bases de datos**.
6. En el campo **Actualización de bases de datos programada**, puede configurar las opciones para actualizaciones automáticas de la base de datos antimalware en el dispositivo del usuario.
7. Si seleccionó una actualización de 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 **Día** y **Hora**.

Si el dispositivo está en modo de ahorro de batería, la aplicación puede realizar esta tarea más tarde de lo especificado.

8. 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 **Permitir la actualización de la base de datos durante la itinerancia** de la sección **Actualización de la base de datos durante la itinerancia**.

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.

9. Haga clic en **Aceptar**.
10. Haga clic en el botón **Guardar** 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.
- 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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Protección**.
4. En la tarjeta **Protección web**, habilite la configuración con el interruptor **Protección web**.

5. Haga clic en **Habilitar**.

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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Protección**.
4. En la tarjeta **Protección web**, seleccione la casilla **Bloquee notificaciones que contengan URL maliciosas y de phishing**.
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
Bloquear dispositivo	El dispositivo móvil está bloqueado. Para obtener acceso a los datos, debe desbloquear el dispositivo mediante el comando Desbloquear dispositivo o un código de acceso único.
Desbloquear dispositivo	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.
Restablecer ajustes de fábrica	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.
Eliminar datos corporativos	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. • 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.

Comando	Resultado
Localizar dispositivo	Se obtienen las coordenadas de la ubicación del dispositivo móvil. Para ver la ubicación del dispositivo en Yandex.Maps, vaya a la sección Administración de activos → Móviles → Dispositivos. Luego, elija un dispositivo y seleccione Historial de comandos → Localizar dispositivo → Coordenadas del dispositivo → Ver en el mapa. Después de hacer clic en Ver en el mapa, 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.
Activar alarma	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.

Comandos para dispositivos MDM con iOS

Comandos para proteger datos de un dispositivo MDM con iOS perdido o robado

Comando	Resultado
Bloquear dispositivo	El dispositivo móvil está bloqueado. Para acceder a los datos, debe desbloquear el dispositivo.
Restablecer la contraseña de desbloqueo	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.
Restablecer ajustes de fábrica	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.
Eliminar datos corporativos	Todos los perfiles de configuración instalados, los perfiles de aprovisionamiento, el perfil de administración de dispositivos y las aplicaciones para las que se seleccionó la casilla Eliminar cuando se elimine el perfil de administración se eliminan del 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 (cloud), 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 **Antirrobo** 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 (cloud), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
2. Haga clic en el dispositivo móvil para el cual desea recibir un código de acceso único.
3. Seleccione **Aplicaciones** → **Kaspersky Mobile Devices Protection and Management**.
Se abre la ventana de propiedades de Kaspersky Mobile Devices Protection and Management.
4. Seleccione la pestaña **Configuración de la aplicación**.
Se muestra un código de acceso único para el dispositivo seleccionado en el campo **Código de un solo uso** de la sección **Código de acceso de un solo uso del dispositivo**.
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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Protección**.
4. En la tarjeta **Antirrobo**, haga clic en **Configuración**.
Se abre la ventana **Antirrobo**.
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 **Texto que se muestra en el dispositivo bloqueado**, ingrese el texto del mensaje que se mostrará en la pantalla de bloqueo.
7. Haga clic en **Aceptar**.
8. Haga clic en el botón **Guardar** 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 **La contraseña de desbloqueo no cumple con los requisitos de seguridad**.

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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Controles de seguridad**.
4. En la tarjeta **Configuración de desbloqueo de pantalla**, haga clic en **Configuración**.
Se abre la ventana **Configuración de desbloqueo de pantalla**.
5. Habilite la configuración con el interruptor **Configuración de desbloqueo de pantalla**, 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:

- **Longitud mínima de la contraseña**

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.

- **Permitir el desbloqueo con huella dactilar**

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 **Permitir métodos de desbloqueo biométricos** 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 **Período de inactividad antes de que se bloquee el contenedor corporativo (segundos)** después de establecer una huella digital como el método de desbloqueo de pantalla.

7. Haga clic en **Aceptar**.

8. Haga clic en el botón **Guardar** 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 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 en el modo de funcionamiento "Perfil de administración".

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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Controles de seguridad**.
4. En la tarjeta **Configuración de desbloqueo de pantalla**, haga clic en **Configuración**.
Se abre la ventana **Configuración de desbloqueo de pantalla**.
5. Habilite la configuración con el interruptor **Configuración de desbloqueo de pantalla**.

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 **Permitir contraseña simple**. Incluso si esta casilla no está marcada, el usuario puede establecer una contraseña con menos de 6 caracteres.
 - Para requerir el uso de letras y números en la contraseña, active la casilla **Solicitar valor alfanumérico**.
 - En la lista **Longitud mínima de la contraseña**, seleccione la longitud mínima de la contraseña en caracteres.
 - En la lista **Mínimo de caracteres especiales**, seleccione la cantidad mínima de caracteres especiales en la contraseña (como "\$", "&", "!").
En algunos dispositivos con MDM de iOS, si se especifica el valor **Mínimo de caracteres especiales** y se marca la casilla **Permitir contraseña simple**, 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 **Duración máxima de la contraseña (días)**, 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 **Bloqueo automático**, 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 **Reutilización de contraseñas anteriores**, 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 **Plazo máximo para desbloqueo sin contraseña**, seleccione la cantidad de tiempo durante la cual el usuario puede desbloquear el dispositivo MDM con iOS sin ingresar la contraseña.
- En **Cantidad máxima de intentos de contraseña fallidos**, 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 **Guardar** 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 (en la nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Configuración de Samsung Knox**.
4. En la tarjeta **VPN**, haga clic en **Configuración**.
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 **Red**:
 - En el campo **Nombre de la red**, escriba el nombre del túnel VPN.
 - En la lista desplegable **Protocolo**, seleccione el tipo de conexión VPN:
 - **IPSec Xauth PSK**. Un protocolo de túnel entre puertos 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 puertos 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 **Configuración del protocolo**:
 - En la lista **Dominio(s) de búsqueda DNS**, 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 **Servidor(es) DNS**, 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 **Enrutamiento**, 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 **Enrutamiento**, 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 **Clave compartida IPSec**, escriba la contraseña de la clave de seguridad preestablecida IPSec.
 - En el campo **ID de IPSec**, 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 **Clave de L2TP**.
- Para la red **PPTP**, seleccione la casilla **Utilizar conexión SSL** 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 **Guardar** 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 en el modo de funcionamiento "Perfil de administración".

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.

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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Configuración del dispositivo**.
4. En la tarjeta **VPN**, haga clic en **Configuración**.
Se abre la ventana **VPN**.
5. Habilite la configuración con el interruptor **VPN**.
6. Haga clic en **Agregar**.
Se abre la ventana **Agregar configuración de VPN**.
7. En la pestaña **General**, en la sección **Red**, configure los siguientes ajustes:
 - a. En el campo **Nombre de la red**, escriba el nombre del túnel VPN.
 - b. En la lista desplegable **Protocolo**, 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.
 - **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.
- **SSL personalizado.** La conexión admite autenticación del usuario de un dispositivo MDM con iOS mediante contraseñas y autenticación de dos factores.

c. En el campo **Dirección del servidor**, 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 **Autenticación**:

- **Tipo de autenticación**

Autenticación de dos factores del usuario de un dispositivo MDM con iOS mediante un token RSA SecurID o autenticación basada en contraseña.

- **Nombre de la cuenta**

Nombre de la cuenta para obtener autorización en el servidor de VPN.

- **Contraseña**

La contraseña de la cuenta para autenticación en la red virtual privada.

- **Método de autenticación**

Método para autenticar a los usuarios de dispositivos MDM con iOS en la red privada virtual.

- **Secreto compartido**

Contraseña para la clave de seguridad preestablecida IPsec para los protocolos L2TP y IPsec (Cisco).

- **Certificado de autenticación**

Certificado utilizado para la autenticación de usuarios.

- Ajustes de la sección **Otro**:

- **Enviar todo el tráfico a través de 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 **Autenticación**:

- **Método de autenticación**

- Método para autenticar a los usuarios de dispositivos MDM con iOS en la red privada virtual.

- **Nombre de la cuenta**

- Nombre de la cuenta para obtener autorización en el servidor de VPN.

- **Contraseña**

- La contraseña de la cuenta para autenticación en la red virtual privada.

- **Secreto compartido**

- Contraseña para la clave de seguridad preestablecida IPSec para los protocolos L2TP y IPSec (Cisco).

- **Nombre del grupo**

- 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 **Utilizar la autenticación híbrida** está marcada, el nombre del grupo debe terminar en "[hybrid]" (por ejemplo: "mycompany [hybrid]").

- **Utilizar la autenticación híbrida**

- 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.

- **Certificado de autenticación**

- Certificado utilizado para la autenticación de usuarios.

- Ajustes de la sección **Dominios**:

- **Habilitar VPN al conectarse a dominios específicos**

- Los dominios para los que se habilitará la conexión VPN.

- Ajustes de la sección **Otro**:

- **Solicitar 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.

- **Cisco AnyConnect**

- Ajustes de la sección **Red**:

- **Tiempo de inactividad antes de la desconexión (min)**

- El tiempo de espera antes de desconectar una conexión a pedido.

- Ajustes de la sección **Autenticación**:

- **Método de autenticación**

- Método para autenticar a los usuarios de dispositivos MDM con iOS en la red privada virtual.

- **Nombre de la cuenta**

- Nombre de la cuenta para obtener autorización en el servidor de VPN.

- **Contraseña**

- La contraseña de la cuenta para autenticación en la red virtual privada.

- **Grupo**

- Alias del grupo de túnel para los clientes de Cisco AnyConnect que se conectan a una VPN.

- **Certificado de autenticación**

- Certificado utilizado para la autenticación de usuarios.

- Ajustes de la sección **Dominios**:

- **Habilitar VPN al conectarse a dominios específicos**

- Los dominios para los que se habilitará la conexión VPN.

- Ajustes de la sección **Otro**:

- **Enviar todo el tráfico a través de VPN**

- Enruta todo el tráfico a través de la VPN.

- **Excluir tráfico local**

- Excluye el tráfico local del tráfico enrutado a través de la conexión VPN.

- Esta casilla está disponible si se selecciona la casilla **Enviar todo el tráfico a través de VPN**.

- **Juniper SSL**

- Ajustes de la sección **Red**:

- **Tiempo de inactividad antes de la desconexión (min)**

- El tiempo de espera antes de desconectar una conexión a pedido.

- Ajustes de la sección **Autenticación**:

- **Método de autenticación**

- Método para autenticar a los usuarios de dispositivos MDM con iOS en la red privada virtual.

- **Nombre de la cuenta**

- Nombre de la cuenta para obtener autorización en el servidor de VPN.

- **Contraseña**

- La contraseña de la cuenta para autenticación en la red virtual privada.

- **Alcance**

- Nombre de la red que incluye los servidores VPN y los dispositivos MDM con iOS para la conexión VPN establecida utilizando Juniper SSL.

- **Rol**

- 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.

- **Certificado de autenticación**

- Certificado utilizado para la autenticación de usuarios.

- Ajustes de la sección **Dominios**:

- **Habilitar VPN al conectarse a dominios específicos**

- Los dominios para los que se habilitará la conexión VPN.

- Ajustes de la sección **Otro**:

- **Enviar todo el tráfico a través de VPN**

- Enruta todo el tráfico a través de la VPN.

- **Excluir tráfico local**

- Excluye el tráfico local del tráfico enrutado a través de la conexión VPN.

- Esta casilla está disponible si se selecciona la casilla **Enviar todo el tráfico a través de VPN**.

- **F5 SSL**

- Ajustes de la sección **Red**:

- **Tiempo de inactividad antes de la desconexión (min)**

- El tiempo de espera antes de desconectar una conexión a pedido.

- Ajustes de la sección **Autenticación**:

- **Método de autenticación**

- Método para autenticar a los usuarios de dispositivos MDM con iOS en la red privada virtual.

- **Nombre de la cuenta**

Nombre de la cuenta para obtener autorización en el servidor de VPN.

- **Contraseña**

La contraseña de la cuenta para autenticación en la red virtual privada.

- **Certificado de autenticación**

Certificado utilizado para la autenticación de usuarios.

- Ajustes de la sección **Dominios**:

- **Habilitar VPN al conectarse a dominios específicos**

Los dominios para los que se habilitará la conexión VPN.

- Ajustes de la sección **Otro**:

- **Enviar todo el tráfico a través de VPN**

Enruta todo el tráfico a través de la VPN.

- **Excluir tráfico local**

Excluye el tráfico local del tráfico enrutado a través de la conexión VPN.

Esta casilla está disponible si se selecciona la casilla **Enviar todo el tráfico a través de VPN**.

- **SonicWALL Mobile Connect**

- Ajustes de la sección **Red**:

- **Tiempo de inactividad antes de la desconexión (min)**

El tiempo de espera antes de desconectar una conexión a pedido.

- Ajustes de la sección **Autenticación**:

- **Método de autenticación**

Método para autenticar a los usuarios de dispositivos MDM con iOS en la red privada virtual.

- **Nombre de la cuenta**

Nombre de la cuenta para obtener autorización en el servidor de VPN.

- **Contraseña**

La contraseña de la cuenta para autenticación en la red virtual privada.

- **Dominio o grupo**

Nombre del dominio del servidor SSL VPN (ejemplo: vpn.compañía.com) o el nombre de un grupo de usuarios de SonicWALL Mobile Connect.

- **Certificado de autenticación**

Certificado utilizado para la autenticación de usuarios.

- Ajustes de la sección **Dominios**:
 - **Habilitar VPN al conectarse a dominios específicos**
Los dominios para los que se habilitará la conexión VPN.
- Ajustes de la sección **Otro**:
 - **Enviar todo el tráfico a través de VPN**
Enruta todo el tráfico a través de la VPN.
 - **Excluir tráfico local**
Excluye el tráfico local del tráfico enrutado a través de la conexión VPN.
Esta casilla está disponible si se selecciona la casilla **Enviar todo el tráfico a través de VPN**.
- **Aruba VIA**
 - Ajustes de la sección **Red**:
 - **Tiempo de inactividad antes de la desconexión (min)**
El tiempo de espera antes de desconectar una conexión a pedido.
 - Ajustes de la sección **Autenticación**:
 - **Método de autenticación**
Método para autenticar a los usuarios de dispositivos MDM con iOS en la red privada virtual.
 - **Nombre de la cuenta**
Nombre de la cuenta para obtener autorización en el servidor de VPN.
 - **Contraseña**
La contraseña de la cuenta para autenticación en la red virtual privada.
 - **Certificado de autenticación**
Certificado utilizado para la autenticación de usuarios.
 - Ajustes de la sección **Dominios**:
 - **Habilitar VPN al conectarse a dominios específicos**
Los dominios para los que se habilitará la conexión VPN.
 - Ajustes de la sección **Otro**:
 - **Enviar todo el tráfico a través de VPN**
Enruta todo el tráfico a través de la VPN.
 - **Excluir tráfico local**
Excluye el tráfico local del tráfico enrutado a través de la conexión VPN.

Esta casilla está disponible si se selecciona la casilla **Enviar todo el tráfico a través de VPN**.

- **SSL personalizado**

- Ajustes de la sección **Red**:

- **Tiempo de inactividad antes de la desconexión (min)**

- El tiempo de espera antes de desconectar una conexión a pedido.

- Ajustes de la sección **Datos de la configuración**:

- **Clave**

- Contiene una clave con configuraciones adicionales para la conexión personalizada SSL.

- **Valor**

- Contiene un valor con configuraciones adicionales para la conexión personalizada SSL.

- Ajustes de la sección **Autenticación**:

- **Método de autenticación**

- Método para autenticar a los usuarios de dispositivos MDM con iOS en la red privada virtual.

- **Nombre de la cuenta**

- Nombre de la cuenta para obtener autorización en el servidor de VPN.

- **Contraseña**

- La contraseña de la cuenta para autenticación en la red virtual privada.

- **Certificado de autenticación**

- Certificado utilizado para la autenticación de usuarios.

- **ID de paquete**

- 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 **Dominios**:

- **Habilitar VPN al conectarse a dominios específicos**

- Los dominios para los que se habilitará la conexión VPN.

9. Si es necesario, en la pestaña **Avanzado**, en la sección **Servidor proxy**, configure los ajustes de la conexión VPN a través de un servidor proxy:

a. Seleccione la casilla **Usar un servidor proxy**.

b. Configure una conexión a un servidor proxy:

a. Si desea configurar la conexión automáticamente:

- Seleccione **Automático**.
- En el campo **URL de archivo PAC**, 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 **Permitir conexión directa si no se puede acceder al archivo PAC**.

b. Si desea configurar la conexión manualmente:

- Seleccione **Manual**.
- En el campo **Dirección de servidor proxy y Puerto**, escriba la dirección IP o nombre DNS del servidor proxy y el número de puerto.
- En el campo **Nombre de usuario**, seleccione una macro que se utilizará como nombre de usuario para la conexión al servidor proxy.

c. En el campo **Contraseña**, especifique la contraseña para la conexión al servidor proxy.

10. Clic en el botón **Agregar**.

La nueva VPN se muestra en la lista.

Puede modificar o eliminar redes VPN en la lista con los botones **Modificar** y **Eliminar** que se encuentran en la parte superior de la lista.

11. Haga clic en el botón **Guardar** 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.

Firewall solo se puede configurar en dispositivos Samsung con Android 15 o versiones anteriores.

Para configurar el firewall en el dispositivo móvil de un usuario, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Configuración de Samsung Knox**.
4. En la tarjeta **Firewall**, haga clic en **Configuración**.
Se abre la ventana **Firewall**.
5. Habilite la configuración con el interruptor **Firewall**.
6. En la lista desplegable **Acceso a Internet**, 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 **Permitir para todas las apps**. Este modo está seleccionado de forma predeterminada.
 - Si desea bloquear toda la actividad de la red, excepto varias aplicaciones especificadas, seleccione **Permitir para todas las apps de la lista**.
7. Si seleccionó **Permitir para todas las apps de la lista** 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 con acceso a Internet**, haga clic en **Agregar**.
Se abre la ventana **Agregar aplicación**.
 - b. En el campo **Nombre de la app**, escriba el nombre de una aplicación móvil.
 - c. En el campo **Nombre del paquete**, 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 **Modificar** y **Eliminar** que se encuentran en la parte superior de la lista.

8. Haga clic en **Aceptar**.
9. Haga clic en el botón **Guardar** 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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Configuración de KES para Android**.
4. En la tarjeta **Configurar el acceso a la configuración de la app**, haga clic en **Configuración**.
Se abre la ventana **Configurar el acceso a la configuración de la app**.
5. Habilite la configuración con el interruptor **Configurar el acceso a la configuración de la app**.

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 **Permitir eliminar la app del dispositivo**.
7. Haga clic en **Aceptar**.
8. Haga clic en el botón **Guardar** 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 (nube) le permite detectar dispositivos Android comprometidos (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 (nube), en la sección **Supervisión** → **Panel**. 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 **Se detectó acceso root en el dispositivo**.

Configuración de un proxy HTTP global en dispositivos iOS con MDM

Esta configuración se aplica a los dispositivos en el modo operativo "Perfil de administración".

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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Configuración del dispositivo**.
4. En la tarjeta **Proxy HTTP global**, haga clic en **Configuración**.
Se abre la ventana **Proxy HTTP global**.
5. Habilite la configuración con el interruptor **Proxy HTTP global**.

6. Seleccione el tipo de configuración de proxy HTTP global:

- Para especificar la configuración de conexión al servidor proxy manualmente:
 - a. En la sección **Tipo de configuración**, seleccione **Manual**.
 - b. En los campos **Dirección de servidor proxy** y **Puerto**, escriba el nombre del host o la dirección IP del servidor proxy y el número de puerto del servidor proxy.
 - c. En el campo **Nombre de usuario**, ingrese el nombre de la cuenta de usuario para obtener autorización en el servidor proxy.
 - d. En el campo **Contraseña**, 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 **Permitir acceso a redes cautivas sin conectarse al servidor proxy**.
- Para configurar las opciones de conexión al servidor proxy mediante un archivo PAC (autoconfiguración de proxy) predefinido:
 - a. En la sección **Tipo de configuración**, seleccione **Automático**.
 - b. En el campo **URL de archivo PAC**, 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 **Permitir conexión directa si no se puede acceder al archivo PAC**.
 - d. Para permitir al usuario acceder a redes cautivas, seleccione la casilla **Permitir acceso a redes cautivas sin conectarse al servidor proxy**.

7. Haga clic en **Aceptar**.

8. Haga clic en el botón **Guardar** 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 en el modo de funcionamiento "Perfil de administración".

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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Configuración del dispositivo**.
4. En la tarjeta **Administración de certificados**, haga clic en **Configuración**.
Se abre la ventana **Administración de certificados**.
5. Habilite la configuración con el interruptor **Administración de certificados**.
6. Haga clic en **Cargar** 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 **Guardar** 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 en el modo de funcionamiento "Perfil de administración".

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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Configuración del dispositivo**.
4. En la tarjeta **SCEP**, haga clic en **Configuración**.
Se abre la ventana **SCEP**.
5. Habilite la configuración con el interruptor **SCEP**.
6. Clic en el botón **Agregar**.
Se abre la ventana **Agregar perfil de SCEP**.
7. En la sección **Servidor SCEP**, especifique la siguiente configuración del servidor SCEP:
 - En el campo **Nombre de la configuración**, 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 **URL del servidor**, 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 **Número máximo de intentos de sondeo**, 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 **Intervalo de sondeos (s)**, 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 **Frase de desafío estático**, 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 **Método para cargar la huella digital del certificado**, 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 **Manualmente**, en el campo **Huella digital del certificado** que aparece, ingrese una huella digital del certificado única para verificar la autenticidad de la respuesta del Centro de certificación.
- Si seleccionó la opción **Desde el archivo**, 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 **Asunto**, especifique la siguiente configuración:

- En el campo **Nombre del asunto**, 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 **Agregar nombre alternativo del asunto** para agregar un campo a fin de especificar el nombre alternativo del titular:
 - En la lista desplegable **Tipo de nombre alternativo del asunto** 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.
 - **Nombre de DNS.** Identificación mediante el nombre de dominio.
 - **Nombre de NT principal.** 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.
 - **Dirección de correo electrónico.** Identificación mediante la dirección de correo electrónico. La dirección de correo electrónico debe ser especificada de acuerdo al RFC 822.
 - **Identificador de recursos uniforme (URI).** Identificación mediante la dirección IP o la dirección en formato FQDN.
- En el campo **Nombre alternativo del asunto**, 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 **Clave**, ajuste la configuración de la clave de cifrado:

- En la lista desplegable **Longitud de la clave (bits)**, 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 **Usar como firma digital**.

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 **Utilizar para cifrado**.

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 **Permitir que todas las apps accedan a la clave privada**.
- Si no desea que la clave privada se exporte desde el llavero, seleccione la casilla **Prohibir exportar la clave privada del llavero**.

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 **Modificar** y **Eliminar** que se encuentran en la parte superior de la lista.

11. Haga clic en **Aceptar**.

12. Haga clic en el botón **Guardar** 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 (cloud).

Administrar dispositivos Android

Kaspersky Next Expert View (nube) 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 contróleos de forma remota.
- Desconecte los dispositivos Android de la administración.

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 Security Center Web Console, seleccione **Administración de activos** → **Móviles** → **Apps y archivos**.
2. Haga clic en **Android**.
3. Haga clic en **Apps** y luego en **Agregar**.
Se abre la ventana **Agregar aplicación**.
4. Especifique el nombre de la aplicación en el campo **Nombre de la app**. Este nombre se usará para identificar la aplicación en la configuración de la directiva.
5. Haga clic en **Seleccionar** y seleccione un archivo APK en su equipo.
6. Haga clic en el botón **Guardar** 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 y archivos** hasta que se cargue la aplicación.

En la sección **Apps y archivos**, 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 (nube), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
Se abre la lista de dispositivos administrados.

2. Para filtrar dispositivos Android, haga clic en el encabezado de la columna **Sistema operativo** 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 5–9 y para los dispositivos con un contenedor corporativo con Android 10–11.

Si se instala una versión anterior de Kaspersky Endpoint Security para Android (10.52.1.3 o anterior) en los dispositivos, el valor del **Modo de funcionamiento** 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 (nube).

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 (nube), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.

Se abre la lista de dispositivos administrados.

2. Para filtrar dispositivos Android, haga clic en el encabezado de la columna **Sistema operativo** y seleccione **Android**.

Se muestra la lista de dispositivos Android.

3. Seleccione el dispositivo móvil que desea desconectar.

4. Haga clic en **Eliminar**.

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 (nube).

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 de dispositivos no está firmado con un certificado, al instalar el perfil de administración de dispositivos, 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 (cloud), seleccione **Administración de activos** → **Móviles** → **Servidores de MDM para iOS**.

Se abre la lista de Servidores de MDM para iOS.

2. Haga clic en **Certificado de firma**.

Se abre la ventana **Certificado de firma**.

3. En el campo **Formato del certificado**, 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 **Guardar**.

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 (cloud), seleccione **Administración de activos** → **Móviles** → **Servidores de MDM para iOS**. 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 **Configuración de la aplicación**.
3. Seleccione la pestaña **Perfiles de configuración**.
4. Para agregar un nuevo perfil de configuración, haga clic en **Agregar**.
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 **Enviar comando** o en la pestaña **Perfiles de configuración** en la ventana de propiedades del dispositivo.

En la ventana **Enviar comando**, puede instalar perfiles de configuración en varios dispositivos.

Para instalar un perfil de configuración en la ventana Enviar comando, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (cloud), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
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 **Enviar comando**.
4. En la ventana **Enviar comando** que se abre, en el campo **Comando**, seleccione el comando **Instalar perfil de configuración**.

5. En la sección **Perfiles de configuración**, seleccione los [perfiles de configuración que desea instalar](#) en los dispositivos.

6. Haga clic en **Enviar**.

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 (nube), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
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 **Perfiles de configuración**.
4. En la parte superior de la lista de perfiles de configuración, haga clic en **Instalar**.
5. En la ventana que se abre, seleccione los perfiles de configuración que desea instalar en el dispositivo y haga clic en **Instalar**.

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 **Actualizar lista**.

Eliminar un perfil de configuración de un dispositivo

Puede eliminar un perfil de configuración de un dispositivo MDM con iOS en la ventana **Enviar comando** o en la pestaña **Perfiles de configuración** en la ventana de propiedades del dispositivo.

En la ventana **Enviar comando**, puede eliminar los perfiles de configuración de varios dispositivos.

*Para eliminar un perfil de configuración en la ventana **Enviar comando**, siga estos pasos:*

1. En la ventana principal de Kaspersky Next Expert View (cloud), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
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 **Enviar comando**.
4. En la ventana **Enviar comando** que se abre, en el campo **Comando**, seleccione el comando **Eliminar perfil de configuración**.

5. En la sección **Perfiles de configuración**, seleccione los perfiles de configuración que desea eliminar de los dispositivos.

6. Haga clic en **Enviar**.

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 (nube), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
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 **Perfiles de configuración**.
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 **Actualizar lista**.

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 (cloud), seleccione **Administración de activos** → **Móviles** → **Apps y archivos**.
2. Haga clic en **iOS** y luego en **Agregar**.
Se abre la ventana **Agregar aplicación**.
3. Especifique el nombre de la aplicación en el campo **Nombre de la app**. Este nombre se usará para identificar la aplicación en la configuración de la directiva.

4. En el campo **Método de instalación**, seleccione uno de los siguientes métodos para agregar la aplicación:

- **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 **Paquete de instalación**, haga clic en **Seleccionar** y cargue un archivo IPA desde su equipo.
- Si seleccionó **Vínculo al archivo de manifiesto**, 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, ajuste la configuración siguiente:

- Seleccione la casilla **Eliminar cuando se elimine el perfil de administración** si desea que la aplicación se elimine del dispositivo móvil del usuario junto con el perfil de administración del dispositivo. Esta casilla está marcada por defecto.
- Seleccione la casilla **Bloquear la copia de seguridad de los datos de la app en iCloud** si desea bloquear la copia de seguridad de los datos de la aplicación en iCloud.

7. Haga clic en el botón **Guardar** 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 y archivos** 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 **Eliminar**.

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 (cloud), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
2. En la lista de dispositivos que se abre, seleccione los dispositivos en los que desea instalar aplicaciones.
3. Haga clic en **Enviar comando**.
4. En la ventana **Enviar comando** que se abre, en el campo **Comando**, seleccione el comando **Instalar aplicación**.
5. En el campo **Apps**, seleccione [las aplicaciones que desea instalar en los dispositivos](#).
6. Haga clic en **Enviar**.

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 **Enviar comando** o en la pestaña **Apps** en la ventana de propiedades del dispositivo.

En la ventana **Enviar comando**, puede actualizar aplicaciones en varios dispositivos.

*Para actualizar una aplicación en un dispositivo MDM con iOS en la ventana **Enviar comando**, siga estos pasos:*

1. En la ventana principal de Kaspersky Next Expert View (cloud), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
2. En la lista de dispositivos que se abre, seleccione los dispositivos en los que desea actualizar aplicaciones.
3. Haga clic en **Enviar comando**.
4. En la ventana **Enviar comando** que se abre, en el campo **Comando**, seleccione el comando **Actualizar aplicación**.
5. En la sección **Apps**, seleccione las aplicaciones que desea actualizar en los dispositivos.
6. Haga clic en **Enviar**.

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 (nube), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
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 **Actualizar**.
5. En la ventana que se abre, seleccione las aplicaciones que desea actualizar en el dispositivo y haga clic en **Actualizar**.

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 **Actualizar lista**.

Eliminar una app de un dispositivo

Puede eliminar una aplicación de un dispositivo MDM con iOS en la ventana **Enviar comando** o en la pestaña **Apps** en la ventana de propiedades del dispositivo.

En la ventana **Enviar comando**, puede eliminar aplicaciones de varios dispositivos.

*Para eliminar una aplicación de un dispositivo MDM con iOS en la ventana **Enviar comando**, siga estos pasos:*

1. En la ventana principal de Kaspersky Next Expert View (cloud), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
2. En la lista de dispositivos que se abre, seleccione los dispositivos de los que desea eliminar las aplicaciones.
3. Haga clic en **Enviar comando**.
4. En la ventana **Enviar comando** que se abre, en el campo **Comando**, seleccione el comando **Eliminar aplicación**.
5. En la sección **Apps**, seleccione las aplicaciones que desea eliminar de los dispositivos.
6. Haga clic en **Enviar**.

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 (nube), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
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 **Eliminar**.

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 **Actualizar lista**.

Configuración de roaming en un dispositivo móvil MDM con iOS

Para configurar roaming:

1. En la ventana principal de Kaspersky Next Expert View (nube), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
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 **Enviar comando**.
4. En la ventana **Enviar comando** que se abre, en el campo **Comando**, seleccione el comando **Cambiar la configuración de la itinerancia**.
5. En la sección **Acción**, realice una de las siguientes acciones:
 - Si desea habilitar el roaming de datos, seleccione **Habilitar la itinerancia de datos**.
 - Si desea deshabilitar el roaming de datos, seleccione **Deshabilitar la itinerancia de datos**.
6. Haga clic en **Enviar**.

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 (cloud), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
Se abre la lista de dispositivos administrados.
2. Para filtrar los dispositivos MDM con iOS, haga clic en el encabezado de la columna **Modo de funcionamiento** 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 **Certificados** 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 **Perfiles de configuración** 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 del dispositivo, 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 (cloud), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
Se abre la lista de dispositivos administrados.
2. Para filtrar los dispositivos MDM con iOS, haga clic en el encabezado de la columna **Modo de funcionamiento** 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 **Eliminar**.

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 del dispositivo y las aplicaciones para las que se habilitó la opción **Eliminar cuando se elimine el perfil de administración** 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 remotamente la configuración de dispositivos móviles en Kaspersky Next Expert View (cloud).

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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Configuración del dispositivo**.
4. En la tarjeta **Wi-Fi**, haga clic en **Configuración**.
Se abre la ventana **Wi-Fi**.
5. Habilite la configuración con el interruptor **Wi-Fi**.
6. Clic en el botón **Agregar**.
Se abre la ventana **Agregar red Wi-Fi**.
7. En el campo **Identificador de conjunto de servicios (SSID)**, escriba el nombre de la red Wi-Fi que incluye el punto de acceso (SSID).
8. Seleccione la casilla **Red oculta** 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.
9. En la sección **Protección**, seleccione el tipo de seguridad de la red Wi-Fi (red abierta o red segura protegida con los protocolos WEP o WPA2 PSK).

El protocolo WEP solo es compatible con Android 9 o versiones anteriores.

10. En el campo **Contraseña**, establezca una contraseña de acceso a la red si seleccionó una red segura en el paso 8.
11. En la pestaña **Adicional**, seleccione la casilla **Usar un servidor proxy** si desea usar un servidor proxy para conectarse a la red Wi-Fi.
12. Si seleccionó **Usar un servidor proxy**, en los campos **Dirección de servidor proxy** y **Puerto**, 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.

13. En el campo **No usar el servidor proxy para las direcciones especificadas**, 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.

14. 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 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 **Modificar** y **Eliminar** que se encuentran en la parte superior de la lista.

15. Haga clic en **Aceptar**.

16. Haga clic en el botón **Guardar** 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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Configuración del dispositivo**.
4. En la tarjeta **Wi-Fi**, haga clic en **Configuración**.
Se abre la ventana **Wi-Fi**.
5. Habilite la configuración con el interruptor **Wi-Fi**.
6. Haga clic en **Agregar**.
Se abre la ventana **Agregar red Wi-Fi**.
7. En el campo **Identificador de conjunto de servicios (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 **Conectar automáticamente**.

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 **Deshabilitar la detección de redes cautivas**.
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 **Red oculta**.
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. En la sección **Protección**, 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.

- **Red abierta.** 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.
- **Red personal (cualquiera).** 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 (red corporativa).** Se protege la red utilizando el protocolo WEP y con una clave dinámica.
- **WPA (red corporativa).** La red está protegida mediante el protocolo de cifrado WPA o WPA2 con el uso del protocolo 802.1X.
- **WPA2 (red corporativa).** La red está protegida mediante el protocolo de cifrado WPA2 o WPA3 y con una clave única para todos los usuarios (802.1X).
- **WPA3 (red corporativa).** La red está protegida mediante el protocolo de cifrado WPA3 y con una clave única para todos los usuarios (802.1X).
- **Red corporativa (cualquiera).** 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 **Protocolo EAP** puede seleccionar los tipos de protocolos EAP (Protocolo de autenticación extensible) para la identificación de usuarios en la red Wi-Fi.

En la sección **Certificados de confianza**, también puede crear una lista de certificados de confianza para la autenticación del usuario de dispositivos MDM con iOS en servidores de confianza.

12. En la sección **Autenticación**, 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 **Nombre de usuario**, escriba el nombre de la cuenta para la autenticación del usuario al conectarse a la red Wi-Fi.
 - b. En el campo **ID de usuario**, 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 **Contraseña**, 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 **Solicitar contraseña en cada conexión**.
- e. En la lista desplegable **Certificado de autenticación**, seleccione un certificado para la autenticación del usuario en la red Wi-Fi.
- f. En la lista desplegable **Versión de TLS mínima**, seleccione la versión mínima de TLS permitida.
- g. En la lista desplegable **Versión de TLS máxima**, seleccione la versión máxima de TLS permitida.
13. Si es necesario, en la pestaña **Adicional**, configure los ajustes para conectarse a la red Wi-Fi a través de un servidor proxy:
- a. Seleccione la casilla **Usar un servidor proxy**.
- b. Configure una conexión a un servidor proxy:
- a. Si desea configurar la conexión automáticamente:
- Seleccione **Automático**.
 - En el campo **URL de archivo PAC**, 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 **Permitir conexión directa si no se puede acceder al archivo PAC**.
- b. Si desea configurar la conexión manualmente:
- Seleccione **Manual**.
 - En el campo **Dirección de servidor proxy y Puerto**, escriba la dirección IP o nombre DNS del servidor proxy y el número de puerto.
 - En el campo **Nombre de usuario**, seleccione una macro que se utilizará como nombre de usuario para la conexión al servidor proxy.
 - En el campo **Contraseña**, especifique la contraseña para la conexión al servidor proxy.
14. Haga clic en **Agregar**.
- La nueva red Wi-Fi se muestra en la lista.
15. Haga clic en **Aceptar**.
16. Haga clic en el botón **Guardar** 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 en el modo de funcionamiento "Perfil de administración".

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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Configuración del dispositivo**.
4. En la tarjeta **Correo electrónico**, haga clic en **Configuración**.
Se abre la ventana **Correo electrónico**.
5. Habilite la configuración con el interruptor **Correo electrónico**.
6. Clic en el botón **Agregar**.
Se abre la ventana **Agregar cuenta de correo electrónico**.
7. Especifique la configuración de la cuenta de correo electrónico:
 - En la pestaña **General**, defina los siguientes ajustes:
 - a. En el campo **Nombre de usuario**, escriba el nombre del usuario del dispositivo MDM con iOS.
 - b. En el campo **Dirección de correo electrónico**, especifique la dirección de correo electrónico del usuario del dispositivo MDM con iOS.
 - c. En el campo **Descripción de la cuenta**, escriba una descripción de la cuenta de correo electrónico del usuario.

d. En el campo **Protocolo de correo electrónico**, seleccione uno de los siguientes protocolos:

- **POP**
- **IMAP**

e. Si seleccionó **IMAP**, especifique el prefijo de ruta IMAP en el campo **Prefijo de ruta IMAP**.

El prefijo de la ruta IMAP debe introducirse en letras mayúsculas (por ejemplo, GMAIL para Google Mail).

f. En las secciones **Configuración del servidor de correo entrante** y **Configuración del servidor de correo saliente**, configure los ajustes de conexión del servidor:

- En el campo **Dirección del servidor**, especifique los nombres de los hosts o las direcciones IP de los servidores de correo entrante y saliente.
- En los campos **Puerto del servidor**, 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 **Más configuraciones** y haga lo siguiente:

- En el campo **Nombre de usuario**, especifique el nombre de la cuenta del usuario para la autorización en los servidores de correo entrante y saliente.
 - En el campo **Tipo de autenticación**, seleccione el tipo de autenticación de la cuenta de correo electrónico del usuario en los servidores de correo entrante y saliente.
 - En el campo **Contraseña**, 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 **Utilizar conexión SSL**.
- En la pestaña **Avanzado**, configure los ajustes adicionales de la cuenta de correo electrónico:

a. En la sección **Restricciones**, seleccione o desmarque las siguientes casillas, si es necesario:

- **Permitir la sincronización de direcciones recientes**

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 **Permitir el movimiento de mensajes entre cuentas (incluidas las de trabajo y las personales)** y seleccione la casilla [Prohibir que las apps no administradas usen documentos de las apps administradas](#) y [Prohibir que las apps administradas usen documentos de las apps no administradas](#).

- **Permitir el movimiento de mensajes entre cuentas (incluidas las de trabajo y las personales)**

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.

- **Permitir 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.

- **Permitir usar solo la aplicación de correo**

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 **Firma** y **Cifrado**, 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 autenticación, 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.

- **Firmar mensajes**

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.

- **Certificado de firma para mensajes salientes**

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 **Administración de certificados** de la directiva o en la sección **Certificados** de Kaspersky Next Expert View (en la nube).

Esta lista desplegable está disponible solo si la casilla **Firmar mensajes** está marcada.

- **Cifrado de mensajes de manera predeterminada**

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.

- **Certificado de cifrado**

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 **Administración de certificados** de la directiva o en la sección **Certificados** de Kaspersky Next Expert View (nube).

Esta lista desplegable está disponible solo si la casilla **Cifrado de mensajes de manera predeterminada** está marcada.

- **Mostrar botón para cifrar los mensajes seleccionados**

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 **Cifrado de mensajes de manera predeterminada** determina si el correo saliente se cifra.

8. Haga clic en **Guardar**.

La nueva cuenta de correo electrónico aparece en la lista.

Puede modificar o eliminar cuentas de correo electrónico en la lista con los botones **Modificar** y **Eliminar** que se encuentran en la parte superior de la lista.

9. Haga clic en **Aceptar**.

10. Haga clic en el botón **Guardar** 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 en el modo de funcionamiento "Perfil de administración".

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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.

3. Seleccione **iOS** y vaya a la sección **Configuración del dispositivo**.

4. En la tarjeta **Exchange ActiveSync**, haga clic en **Configuración**.

Se abre la ventana **Exchange ActiveSync**.

5. Habilite la configuración con el interruptor **Exchange ActiveSync**.

6. Clic en el botón **Agregar**.

Se abre la ventana **Agregar cuenta de Exchange ActiveSync**.

7. Especifique la configuración de Exchange ActiveSync:

- En la pestaña **General**, especifique los datos del usuario:
 - En el campo **Nombre de la cuenta**, escriba el nombre de la cuenta para la autorización en el servidor Microsoft Exchange.
 - En el campo **Dirección de servidor de Exchange ActiveSync**, escriba el nombre DNS o la dirección IP del servidor Microsoft Exchange.

- Ajustes de la sección **Credenciales de usuario**:

- En el campo **Dominio de usuario**, escriba el nombre de dominio del usuario del dispositivo MDM con iOS.
- En el campo **Nombre de usuario**, escriba el nombre del usuario del dispositivo MDM con iOS.
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 **Dirección de correo electrónico**, especifique la dirección de correo electrónico del usuario del dispositivo MDM con iOS.

- Ajustes de la sección **Autenticación**:

- En el campo **Contraseña**, escriba la contraseña de la cuenta Exchange ActiveSync para la autorización en el servidor Microsoft Exchange.
- En la lista desplegable **Certificado de autenticación**, 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 **Administración de certificados** de la directiva o en la sección **Certificados** de Kaspersky Next Expert View (nube).

- En la pestaña **Adicional**, configure las opciones adicionales de la cuenta de Exchange ActiveSync:

- En la sección **Sincronización de correo electrónico**, en la lista desplegable **Período de sincronización**, 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 semana**.
- En la sección **Restricciones**, seleccione o desmarque las siguientes casillas, si es necesario:

- **Permitir el movimiento de mensajes entre cuentas (incluidas las de trabajo y las personales)**

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 **Permitir el movimiento de mensajes entre cuentas (incluidas las de trabajo y las personales)** y seleccione la casilla [Prohibir que las apps no administradas usen documentos de las apps administradas](#) y [Prohibir que las apps administradas usen documentos de las apps no administradas](#).

- **Permitir la sincronización de direcciones recientes**

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.

- **Permitir usar solo la aplicación de correo**

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.

- **Utilizar conexión SSL**

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 **Firma y cifrado**, 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 autenticación, 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.

- **Firmar mensajes**

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.

- **Certificado de firma para mensajes salientes**

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 **Administración de certificados** de la directiva o en la sección **Certificados** de Kaspersky Next Expert View (nube).

Esta lista desplegable está disponible solo si la casilla **Firmar mensajes** está marcada.

- **Cifrado de mensajes de manera predeterminada**

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.

- **Certificado de cifrado**

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 **Administración de certificados** de la directiva o en la sección **Certificados** de Kaspersky Next Expert View (nube).

Esta lista desplegable está disponible solo si la casilla **Cifrado de mensajes de manera predeterminada** está marcada.

- **Mostrar botón para cifrar los mensajes seleccionados**

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 **Cifrado de mensajes de manera predeterminada** determina si el correo saliente se cifra.

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 **Modificar** y **Eliminar** que se encuentran en la parte superior de la lista.

9. Haga clic en **Aceptar**.

10. Haga clic en el botón **Guardar** 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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Configuración de Samsung Knox**.

4. En la tarjeta **Exchange ActiveSync**, haga clic en **Configuración**.
Se abre la ventana **Exchange ActiveSync**.
5. Habilite la configuración con el interruptor **Exchange ActiveSync**.
6. En el campo **Dirección del servidor**, escriba la dirección IP o el nombre DNS del servidor que aloja al servidor de correo.
7. En el campo **Nombre de dominio**, escriba el nombre de dominio del usuario del dispositivo móvil en la red corporativa.
8. En la lista desplegable **Intervalo de sincronización**, 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 **Utilizar conexión SSL**. 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 **Verificar certificado del servidor**. 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 **Guardar** 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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Configuración de KES para Android**.
4. En la tarjeta **Configuración de gravedad para el nivel de protección del dispositivo**, haga clic en **Configuración**.
Se abre la ventana **Configuración de gravedad para el nivel de protección del dispositivo**.
5. Habilite la configuración mediante el interruptor **Configuración de gravedad para el nivel de protección del dispositivo**.

6. Seleccione el nivel de protección **Normal**, **Advertencia** o **Crítico** para cada una de las siguientes condiciones:

- **Protección en tiempo real no se está ejecutando**

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 **Control de cumplimiento** de la directiva.

- **Protección web y Control web no se están ejecutando**

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 **Control de cumplimiento** de la directiva.

- **Control de aplicaciones no se está ejecutando**

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 **Control de cumplimiento** de la directiva.

- **El bloqueo de dispositivo no está disponible**

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 un 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.
- **La ubicación de dispositivo no está disponible**

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 **Localizar dispositivo**.

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.
 - **Las versiones de la Declaración de Kaspersky Security Network no coinciden**
- 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.
- **Las versiones de la Declaración de marketing no coinciden**
- 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 **Guardar** 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 **Informar sobre las aplicaciones móviles instaladas** 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 **Enviar datos sobre las apps instaladas** debe estar seleccionada en la configuración **Control de aplicaciones** 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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Controles de seguridad**.
4. En la tarjeta **Control de aplicaciones**, haga clic en **Configuración**.
Se abre la ventana **Control de aplicaciones**.
5. En la sección **Informe sobre apps instaladas**, seleccione la casilla **Enviar datos sobre las apps instaladas**.
6. Si desea recibir datos sobre las aplicaciones del sistema, seleccione la casilla **Enviar datos sobre apps integradas**.
7. Si desea recibir datos sobre aplicaciones de servicio, que no tienen una interfaz y el usuario no puede abrirlas, seleccione la casilla **Enviar datos sobre apps de servicio**.
8. Haga clic en **Aceptar**.
9. Haga clic en el botón **Guardar** para guardar los cambios que realizó.
10. Haga clic en el nombre de la directiva y seleccione **Configuración de eventos**.
11. Vaya a la sección **Información**.
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 **Guardar en la base de datos del Servidor de administración por (días)** 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](#).

14. Haga clic en **Aceptar**.

15. Haga clic en el botón **Guardar** 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 (nube), seleccione **Supervisión** → **Informes**.
2. Haga clic en la plantilla de informe **Informar sobre las aplicaciones móviles instaladas** para abrir sus propiedades.
3. En la ventana que se abre, haga clic en **Editar**.
4. Modifique las propiedades de la plantilla de informe:
 - En la pestaña **General**, especifique los siguientes parámetros:

- Nombre de la plantilla de informe
- **Cantidad máxima de entradas para mostrar**

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 **Campos** → **Campos Detalles** 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.

- **Grupo**

El conjunto de dispositivos cliente para los que se crea el informe.

- **Incluir datos de los Servidores de administración secundarios y virtuales**

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.

- **Hasta el nivel de anidamiento**

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.

- **Intervalo de espera de datos (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 **Almacenar en caché los datos de los Servidores de administración secundarios** está habilitada, mostrará información tomada de la caché.

El valor predeterminado es 5 (minutos).

- **Almacenar en caché los datos de los Servidores de administración secundarios**

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.

- **Transferir información detallada desde los Servidores de administración secundarios**

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 **Campos**, 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 **Guardar** 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 (nube), seleccione **Supervisión** → **Informes**.
2. Haga clic en un informe con el tipo **Informar sobre las aplicaciones móviles instaladas**.

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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Configuración de KES para Android**.
4. En la tarjeta **Configurar las notificaciones**, haga clic en **Configuración**.
Se abre la ventana **Configurar las notificaciones**.
5. Habilite la configuración con el interruptor **Configurar las notificaciones**.

6. Si desea ocultar todas las notificaciones y los mensajes emergentes, en la sección **Notificaciones de Kaspersky Endpoint Security**, seleccione la casilla **Deshabilitar notificaciones cuando Kaspersky Endpoint Security está en segundo plano**.

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 **Notificaciones dentro de la app Kaspersky Endpoint Security**, 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 **El dispositivo lleva mucho tiempo sin sincronizarse con el Servidor de Administración**. Si desea tener más control sobre la frecuencia de sincronización, [al configurar las reglas para verificar el cumplimiento de la directiva](#), seleccione el criterio **El dispositivo lleva mucho tiempo sin sincronizarse** 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 **Guardar** 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.

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 en el modo de funcionamiento "Perfil de administración".

Para configurar la conexión de un dispositivo iOS con MDM a dispositivos AirPlay:

1. En la ventana principal de Kaspersky Next Expert View (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.

3. Seleccione **iOS** y vaya a la sección **Configuración del dispositivo**.
4. En la tarjeta **AirPlay**, haga clic en **Configuración**.
Se abre la ventana **AirPlay**.
5. Habilite la configuración con el interruptor **AirPlay**.
6. En la sección **Contraseñas**, haga clic en **Agregar contraseña**.
7. En el campo **Dispositivo**, escriba el nombre del dispositivo AirPlay en la red inalámbrica.
8. En la columna **Contraseña**, 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 **Dispositivos permitidos**. Para hacerlo, haga clic en **Agregar dispositivo** 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 **Guardar** 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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Configuración del dispositivo**.

4. En la tarjeta **AirPrint**, haga clic en **Configuración**.

Se abre la ventana **AirPrint**.

5. Habilite la configuración con el interruptor **AirPrint**.

6. Haga clic en **Agregar**.

Se abre la ventana **Agregar impresora**.

7. En el campo **Dirección IP o FQDN**, ingrese la dirección IP o el nombre de dominio completo (FQDN) de la impresora AirPrint.

8. En el campo **Puerto**, ingrese el puerto de escucha del destino de AirPrint.

9. En el campo **Ruta de recurso**, 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. Haga clic en **Agregar**.

La impresora AirPrint recién agregada aparece en la lista.

11. Haga clic en **Aceptar**.

12. Haga clic en el botón **Guardar** 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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Configuración de Samsung Knox**.
4. En la tarjeta **Configuración de APN**, haga clic en **Configuración**.
Se abre la ventana **Configuración de APN**.
5. Habilite la configuración con el interruptor **Configuración de APN**.

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 **Tipo de APN**, 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 y MMS**. Conexión a Internet e intercambio de mensajes multimedia. Este es el valor predeterminado.
 - En el campo **Nombre de APN**, 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 y MMS** como el tipo de punto de acceso, especifique las siguientes opciones adicionales del servidor de MMS en la sección **Servidor MMS**:
 - En el campo **Nombre del servidor MMS**, 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 **Dirección de servidor proxy de MMS**, especifique el nombre de la red o la dirección IP del servidor proxy.
 - En el campo **Puerto del servidor proxy de MMS**, especifique el número de puerto del servidor de la empresa de telefonía móvil que se utiliza para intercambiar MMS.

8. En la sección **Autenticación**, especifique la siguiente configuración de autenticación:

- En la lista desplegable **Tipo de autenticación**, 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:
 - **Ninguna**. 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.
 - **Simultáneamente**. Uso combinado de los protocolos CHAP y PAP.
- En el campo **Nombre de usuario**, escriba el nombre usuario para la autorización en la red móvil.
- En el campo **Contraseña**, escriba la contraseña para la autorización del usuario en la red móvil.

9. En la sección **Red**, especifique la siguiente configuración de la red:

- En el campo **Nombre de la red**, escriba el nombre de la red.
- En el campo **Dirección del servidor**, 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 **Servidor proxy**, especifique la siguiente configuración del servidor proxy:

- Seleccione la casilla **Usar un servidor proxy** para habilitar el uso de un servidor proxy. Esta casilla está desactivada por defecto.
- En el campo **Dirección de servidor proxy**, 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 **Usar un servidor proxy** está marcada.
- En el campo **Puerto**, 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 **Usar un servidor proxy** está marcada.

11. Haga clic en **Aceptar**.

12. Haga clic en el botón **Guardar** 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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Configuración del dispositivo**.
4. En la tarjeta **Configuración de APN**, haga clic en **Configuración**.
Se abre la ventana **Configuración de APN**.
5. Habilite la configuración con el interruptor **Configuración de APN**.

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 **Tipo de APN**, seleccione el tipo de punto de acceso para la transferencia de datos en una red móvil GPRS/3G/4G:
 - **APN integrado**. 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.
 - **APN y APN integrado**. 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 **Agregar APN**.
8. Especifique la siguiente configuración:
 - a. En el campo **Nombre de APN**, especifique el nombre del punto de acceso.
 - b. En la lista desplegable **Tipo de autenticación**, 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 **Nombre de usuario**, escriba el nombre usuario para la autorización en la red móvil.
 - d. En el campo **Contraseña**, escriba la contraseña para la autorización del usuario en la red móvil.
 - e. En el campo **Dirección de servidor proxy**, ingrese el nombre del host o la dirección IP del servidor proxy.
 - f. En el campo **Puerto**, ingrese el número del puerto del servidor proxy.
 - g. En la lista desplegable **Protocolo permitido**, seleccione el protocolo de Internet.

- h. En la lista desplegable **Protocolo permitido para el roaming**, seleccione el protocolo de Internet que se utilizará durante el roaming internacional.
- i. En la lista desplegable **Protocolo permitido para el roaming nacional**, 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 **Usar la tecnología 4G4XLAT**.
- k. Haga clic en **Aceptar**.

9. Si seleccionó **APN integrado**, configure los siguientes ajustes:

- a. En el campo **Nombre de APN integrado**, especifique el nombre del punto de acceso.
- b. En la lista desplegable **Tipo de autenticación**, 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 **Nombre de usuario**, escriba el nombre usuario para la autorización en la red móvil.
- d. En el campo **Contraseña**, escriba la contraseña para la autorización del usuario en la red móvil.
- e. En la lista desplegable **Protocolo permitido**, seleccione el protocolo de Internet.

10. Haga clic en **Aceptar**.

11. Haga clic en el botón **Guardar** 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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Contenedor corporativo**.
4. En la tarjeta **Contenedor corporativo en dispositivos**, haga clic en **Configuración**.
Se abre la ventana **Contenedor corporativo en dispositivos**.
5. Habilite la configuración mediante el interruptor **Contenedor corporativo en dispositivos**.
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 **Acceso y uso compartido de datos**:

- **Prohibir el uso del portapapeles entre las apps personales y el contenedor corporativo**

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.

- **Prohibir la activación de la depuración USB**

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.

- En la pestaña **Apps**, puede configurar los siguientes ajustes:

- Ajustes de la sección **General**:

- **Habilitar el Control de aplicaciones solo en el contenedor corporativo**

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 **Control de aplicaciones**.

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.

- **Habilitar la Protección web y el Control web solo en el contenedor corporativo**

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 **Control web**.

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.

- **Prohibir la instalación de apps desde fuentes desconocidas en el contenedor corporativo**

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 **Control de aplicaciones** no se pueden instalar.

Esta casilla está desactivada por defecto.

- **Prohibir la eliminación de apps del contenedor corporativo**

Seleccione o desmarque esta casilla para especificar si el usuario tiene prohibido eliminar aplicaciones del contenedor corporativo.

Esta casilla está desactivada por defecto.

- En la pestaña **Certificados**, puede configurar los siguientes ajustes:

- **Duplicar la instalación de certificados de VPN en el espacio personal del usuario**

Seleccione o desmarque la casilla para especificar si el certificado de VPN agregado en la sección **Móviles** → **Certificados** de Kaspersky Next Expert View (cloud) 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.

7. Haga clic en **Aceptar**.

8. Haga clic en el botón **Guardar** 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 **Contenedor corporativo en dispositivos** 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 (nube), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
2. Haga clic en el dispositivo móvil para el cual desea recibir un código de acceso único.
3. Seleccione **Aplicaciones** → **Kaspersky Mobile Devices Protection and Management**.
Se abre la ventana de propiedades de Kaspersky Mobile Devices Protection and Management.
4. Seleccione la pestaña **Configuración de la aplicación**.
Se muestra un código de acceso único para el dispositivo seleccionado en el campo **Código de un solo uso** de la sección **Código de acceso de un solo uso del contenedor corporativo**.
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 en el modo de funcionamiento "Perfil de administración".

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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Configuración del dispositivo**.

4. En la tarjeta **LDAP**, haga clic en **Configuración**.

Se abre la ventana **LDAP**.

5. Habilite la configuración con el interruptor **LDAP**.

6. Clic en el botón **Agregar**.

Se abre la ventana **Agregar cuenta LDAP**.

7. En la pestaña **General**, especifique las siguientes opciones de LDAP:

- En la sección **Servidor**, especifique la configuración del servidor:
 - En el campo **Descripción**, escriba una descripción de la cuenta LDAP del usuario.
 - En el campo **Dirección del servidor**, escriba el nombre de dominio del servidor LDAP.
- En la sección **Autenticación**, especifique las credenciales del usuario:
 - En el campo **Nombre de la cuenta**, escriba el nombre de la cuenta para la autorización en el servidor LDAP.
 - En el campo **Contraseña**, 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 **Utilizar conexión SSL**.

8. En la pestaña **Buscar**, 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 **Agregar configuración** para agregar un bloque de la configuración de búsqueda.
- b. En la columna **Nombre**, escriba el nombre de una búsqueda.
- c. En la lista desplegable **Alcance de la búsqueda**, seleccione el nivel de anidamiento de la carpeta para la búsqueda de datos corporativos en el servidor LDAP:
 - **Carpeta raíz del servidor LDAP**. Búsqueda en la carpeta base del servidor LDAP.
 - **Subcarpetas del primer nivel**. Búsqueda en las carpetas del primer nivel de anidamiento contando desde la carpeta base.
 - **Todas las subcarpetas**. Búsqueda en las carpetas en todos los niveles de anidamiento contando desde la carpeta base.
- d. En la columna **Buscar 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 **Modificar** y **Eliminar** que se encuentran en la parte superior de la lista.

10. Haga clic en **Aceptar**.

11. Haga clic en el botón **Guardar** 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 en el modo de funcionamiento «Perfil de administración».

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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Configuración del dispositivo**.
4. En la tarjeta **Contactos**, haga clic en **Configuración**.
Se abre la ventana **Contactos**.
5. Habilite la configuración con el interruptor **Contactos**.
6. Clic en el botón **Agregar**.
Se abre la ventana **Agregar cuenta CardDAV**.
7. En la sección **Servidor**, en el campo **Descripción**, ingrese una descripción de la cuenta CardDAV del usuario.
8. En los campos **Dirección del servidor** y **Puerto del servidor**, escriba el nombre de host o la dirección IP del servidor CardDAV y el número de puerto del servidor CardDAV.
9. En el campo **URL de contacto**, 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 **Autenticación**, en el campo **Nombre de la cuenta**, escriba el nombre de la cuenta para la autorización en el servidor CardDAV.
11. En el campo **Contraseña**, 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 **Utilizar conexión SSL**.
13. Haga clic en **Agregar**.
La nueva cuenta CardDAV aparece en la lista.

Puede modificar o eliminar cuentas CardDAV en la lista con los botones **Modificar** y **Eliminar** que se encuentran en la parte superior de la lista.

14. Haga clic en **Aceptar**.
15. Haga clic en el botón **Guardar** 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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Configuración del dispositivo**.
4. En la tarjeta **Calendario**, haga clic en **Configuración**.
Se abre la ventana **Calendario**.
5. Habilite la configuración con el interruptor **Calendario**.
6. Clic en el botón **Agregar**.
Se abre la ventana **Agregar cuenta CalDAV**.

7. En la sección **Servidor**, en el campo **Descripción**, ingrese una descripción de la cuenta CalDAV del usuario.
8. En los campos **Dirección del servidor** y **Puerto del servidor**, escriba el nombre de host o la dirección IP del servidor CalDAV y el número de puerto del servidor CalDAV.
9. En el campo **URL del calendario**, 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 **Autenticación**, en el campo **Nombre de la cuenta**, escriba el nombre de la cuenta para la autorización en el servidor CalDAV.
11. En el campo **Contraseña**, 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 **Utilizar conexión SSL**.
13. 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 **Modificar** y **Eliminar** que se encuentran en la parte superior de la lista.

14. Haga clic en **Aceptar**.
15. Haga clic en el botón **Guardar** 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 en el modo operativo "Perfil de administración".

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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Configuración del dispositivo**.
4. En la tarjeta **Calendarios suscritos**, haga clic en **Configuración**.
Se abre la ventana **Calendarios suscritos**.
5. Habilite la configuración con el interruptor **Calendarios suscritos**.
6. Clic en el botón **Agregar**.
Se abre la ventana **Agregar suscripción al calendario**.
7. En el campo **Descripción**, escriba una descripción para la suscripción al calendario.
8. En el campo **Dirección del servidor**, 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 **Nombre de usuario**, 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 **Contraseña**, 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 **Utilizar conexión SSL**.
12. 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 **Modificar** y **Eliminar** que se encuentran en la parte superior de la lista.

13. Haga clic en **Aceptar**.
14. Haga clic en el botón **Guardar** 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 en el modo de funcionamiento "Perfil de administración".

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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Configuración del dispositivo**.
4. En la tarjeta **SSO**, haga clic en **Configuración**.
Se abre la ventana **SSO**.
5. Habilite la configuración con el interruptor **SSO**.
6. Especifique la siguiente configuración:
 - En el campo **Nombre de la cuenta**, especifique el nombre de la cuenta de inicio de sesión único del usuario para la autorización del servidor Kerberos.
 - En la sección **Autenticación**, especifique la siguiente configuración de autenticación:

- **Nombre de usuario de Kerberos**

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.

No use el símbolo arroba (@) en este campo. De lo contrario, el perfil SSO no se aplicará al dispositivo.

- **Alcance de 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`.

- **Certificado de autenticación**

Certificado utilizado para la autenticación de usuarios.

- En la sección **Prefijos de URL**, especifique las direcciones de los sitios web en los que Kaspersky Mobile Devices Protection and Management permite el uso de SSO:

- **Limitar cuenta a las URLs de la lista**

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 **Agregar 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.

- **Agregar URL**

Al hacer clic en el botón, se agrega el campo **Prefijo de URL** 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 **Limitar cuenta a las URLs de la lista** 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 **IDs de paquetes**, especifique los ID de las aplicaciones en las que Kaspersky Mobile Devices Protection and Management permite el uso de SSO:

- **Limitar cuenta a las apps de la lista**

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 **Agregar aplicación** 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.

- **Agregar aplicación**

Al hacer clic en el botón, se agrega el campo **ID de paquete** 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 **Limitar cuenta a las apps de la lista** 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 **Guardar** 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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Configuración del dispositivo**.
4. En la tarjeta **Clips web**, haga clic en **Configuración**.
Se abre la ventana **Clips web**.
5. Habilite la configuración con el interruptor **Clips web**.
6. Haga clic en **Agregar**.
Se abre la ventana **Agregar clip web**.
7. En el campo **Nombre de clip web**, escriba el nombre del Clip web a mostrar en la pantalla de inicio del dispositivo MDM con iOS.
8. En el campo **URL de sitio web**, 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 **Control web** de la directiva, los usuarios no podrán acceder a este sitio web a través del Clip web.

9. Haga clic en **Seleccionar** 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 **Opciones**, especifique la siguiente configuración adicional:

- a. Si desea permitir que el usuario elimine el Clip web del dispositivo MDM con iOS, seleccione la casilla **Permitir la eliminación del clip web**.
- b. Si desea que el ícono de Clip web se muestre sin efectos visuales especiales (efecto de redondeo de bordes y brillo del ícono), active la casilla **Ícono precompuesto**.
- 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 **Clip web de pantalla completa**.

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 **Guardar** 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 en el modo de funcionamiento "Perfil de administración".

Para añadir una fuente en el dispositivo iOS con MDM de un usuario:

1. En la ventana principal de Kaspersky Next Expert View (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **iOS** y vaya a la sección **Configuración del dispositivo**.
4. En la tarjeta **Fuentes personalizadas**, haga clic en **Configuración**.
Se abre la ventana **Fuentes personalizadas**.
5. Habilite la configuración con el interruptor **Fuentes personalizadas**.
6. Clic en el botón **Agregar**.
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 **Abrir**.
La nueva fuente aparece en la lista.

Puede eliminar las fuentes de la lista con el botón **Eliminar** en la parte superior de la lista.

9. Haga clic en **Aceptar**.
10. Haga clic en el botón **Guardar** 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 [Historial de comandos](#).

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
Bloquear dispositivo	El dispositivo móvil está bloqueado. Para obtener acceso a los datos, debe desbloquear el dispositivo mediante el comando Desbloquear dispositivo o un código de acceso único.
Desbloquear dispositivo	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.
Restablecer ajustes de fábrica	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.
Eliminar datos corporativos	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. • 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.
Sincronizar dispositivo	Los datos del dispositivo móvil se sincronizan con el Servidor de administración. El estado <i>Ejecutado</i> puede mostrarse cuando el comando se envió correctamente pero el dispositivo aún no recibió.

Comando	Resultado
Localizar dispositivo	Se obtienen las coordenadas de la ubicación del dispositivo móvil. Para ver la ubicación del dispositivo en Yandex.Maps, vaya a la sección Administración de activos → Móviles → Dispositivos. Luego, elija un dispositivo y seleccione Historial de comandos → Localizar dispositivo → Coordenadas del dispositivo → Ver en el mapa. Después de hacer clic en Ver en el mapa, 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.
Activar alarma	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.

Comandos para dispositivos MDM con iOS

Comando	Resultado
Bloquear dispositivo	El dispositivo móvil está bloqueado. Para acceder a los datos, debe desbloquear el dispositivo.
Restablecer la contraseña de desbloqueo	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.
Restablecer ajustes de fábrica	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.
Eliminar datos corporativos	Todos los perfiles de configuración instalados, el perfil de administración de dispositivos y las aplicaciones para las que se seleccionó la casilla Eliminar cuando se elimine el perfil de administración se eliminan del dispositivo.
Sincronizar dispositivo	Los datos del dispositivo móvil se sincronizan con el Servidor de administración.
Instalar perfil de configuración	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.
Eliminar perfil de configuración	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.
Instalar aplicación	Se instala la aplicación especificada en el dispositivo móvil.
Actualizar aplicación	Se actualiza la aplicación especificada en el dispositivo móvil.
Eliminar aplicación	Se elimina la aplicación especificada del dispositivo móvil.
Cambiar la configuración de la itinerancia	Se habilita o deshabilita el roaming de datos y de voz.

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 (cloud), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.
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 **Enviar comando**.
4. En la ventana **Enviar comando** que se abre, en el campo **Comando**, seleccione un comando.
5. Configure el comando que desea enviar.
6. Haga clic en **Enviar**.

Puede ver y cancelar comandos en el **Historial de comandos**.

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 (nube), seleccione **Administración de activos** → **Móviles** → **Dispositivos**.

2. En la lista de dispositivos móviles, seleccione aquel para el que desee ver el historial de comandos.

3. Haga clic en **Historial de comandos**.

Se abre la ventana **Historial de comandos**. Las secciones de la ventana **Historial de comandos** 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.

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 "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 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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Configuración de KES para Android**.
4. En la tarjeta **Kaspersky Security Network**, haga clic en **Configuración**.
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. Haga clic en **Aceptar**.

7. En la tarjeta **Envío de datos adicionales**, haga clic en **Configuración**.

8. En la sección **Envío de datos a Kaspersky Security Network**, seleccione la casilla **Permitir el envío de estadísticas a 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.

9. En la sección **Envío de datos con fines de marketing**, seleccione la casilla **Permitir el procesamiento de datos para ayudar a mejorar la calidad, el aspecto y el rendimiento de la aplicación** 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.

10. Seleccione quién debe aceptar las Declaraciones:

- Si selecciona **El administrador aceptó las declaraciones**, se le pedirá que acepte las declaraciones en la ventana que se abre.
- Si selecciona **Los usuarios aceptaron las declaraciones**, se le pedirá al usuario del dispositivo que las acepte.

11. Haga clic en **Aceptar**.

12. Haga clic en el botón **Guardar** 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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.

3. Seleccione **iOS** y vaya a la sección **Configuración de KP para iOS**.

4. Habilite el interruptor de la tarjeta **Kaspersky Security Network** para el componente Protección web.

5. En la tarjeta **Envío de datos adicionales**, haga clic en **Configuración**.

6. En la sección **Envío de datos a Kaspersky Security Network**, seleccione la casilla **Permitir el envío de estadísticas a 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 **El administrador aceptó las declaraciones**, se le pedirá que acepte las declaraciones en la ventana que se abre.
- Si selecciona **Los usuarios aceptaron las declaraciones**, se le pedirá al usuario del dispositivo que las acepte.

8. Haga clic en **Aceptar**.

9. Haga clic en el botón **Guardar** para guardar los cambios que realizó.

La configuración del dispositivo móvil se modifica después de la siguiente sincronización del dispositivo con 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](#).

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 (nube), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.

3. Seleccione **Android** y vaya a la sección **Configuración de Samsung Knox**.

4. En la tarjeta **VPN**, haga clic en **Configuración**.

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 **Red**:
 - En el campo **Nombre de la red**, escriba el nombre del túnel VPN.
 - En la lista desplegable **Protocolo**, 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 **Configuración del protocolo**:
 - En la lista **Dominio(s) de búsqueda DNS**, 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 **Servidor(es) DNS**, 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 **Enrutamiento**, 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 **Enrutamiento**, 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 **Clave compartida IPSec**, escriba la contraseña de la clave de seguridad preestablecida IPSec.
 - En el campo **ID de IPSec**, 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 **Clave de L2TP**.
- Para la red **PPTP**, seleccione la casilla **Utilizar conexión SSL** 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 **Guardar** 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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Configuración de Samsung Knox**.
4. En la tarjeta **Exchange ActiveSync**, haga clic en **Configuración**.
Se abre la ventana **Exchange ActiveSync**.
5. Habilite la configuración con el interruptor **Exchange ActiveSync**.
6. En el campo **Dirección del servidor**, escriba la dirección IP o el nombre DNS del servidor que aloja al servidor de correo.
7. En el campo **Nombre de dominio**, escriba el nombre de dominio del usuario del dispositivo móvil en la red corporativa.
8. En la lista desplegable **Intervalo de sincronización**, 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 **Utilizar conexión SSL**. 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 **Verificar certificado del servidor**. 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 **Guardar** 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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Configuración de Samsung Knox**.
4. En la tarjeta **Configuración de APN**, haga clic en **Configuración**.
Se abre la ventana **Configuración de APN**.
5. Habilite la configuración con el interruptor **Configuración de APN**.

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 **Tipo de APN**, 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 y MMS**. Conexión a Internet e intercambio de mensajes multimedia. Este es el valor predeterminado.
 - En el campo **Nombre de APN**, 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 y MMS** como el tipo de punto de acceso, especifique las siguientes opciones adicionales del servidor de MMS en la sección **Servidor MMS**:
- En el campo **Nombre del servidor MMS**, 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 **Dirección de servidor proxy de MMS**, especifique el nombre de la red o la dirección IP del servidor proxy.
 - En el campo **Puerto del servidor proxy de MMS**, especifique el número de puerto del servidor de la empresa de telefonía móvil que se utiliza para intercambiar MMS.
8. En la sección **Autenticación**, especifique la siguiente configuración de autenticación:
- En la lista desplegable **Tipo de autenticación**, 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:
 - **Ninguna**. 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.
 - **Simultáneamente**. Uso combinado de los protocolos CHAP y PAP.
 - En el campo **Nombre de usuario**, escriba el nombre usuario para la autorización en la red móvil.
 - En el campo **Contraseña**, escriba la contraseña para la autorización del usuario en la red móvil.
9. En la sección **Red**, especifique la siguiente configuración de la red:
- En el campo **Nombre de la red**, escriba el nombre de la red.
 - En el campo **Dirección del servidor**, 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 **Servidor proxy**, especifique la siguiente configuración del servidor proxy:
- Seleccione la casilla **Usar un servidor proxy** para habilitar el uso de un servidor proxy. Esta casilla está desactivada por defecto.
 - En el campo **Dirección de servidor proxy**, 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 **Usar un servidor proxy** está marcada.
 - En el campo **Puerto**, 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 **Usar un servidor proxy** está marcada.

11. Haga clic en **Aceptar**.

12. Haga clic en el botón **Guardar** 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.

Firewall solo se puede configurar para dispositivos Samsung con Android 15 o versiones anteriores.

Para configurar el firewall en el dispositivo móvil de un usuario, siga estos pasos:

1. En la ventana principal de Kaspersky Next Expert View (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Seleccione **Android** y vaya a la sección **Configuración de Samsung Knox**.
4. En la tarjeta **Firewall**, haga clic en **Configuración**.
Se abre la ventana **Firewall**.
5. Habilite la configuración con el interruptor **Firewall**.
6. En la lista desplegable **Acceso a Internet**, 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 **Permitir para todas las apps**. Este modo está seleccionado de forma predeterminada.
 - Si desea bloquear toda la actividad de la red, excepto varias aplicaciones especificadas, seleccione **Permitir para todas las apps de la lista**.
7. Si seleccionó **Permitir para todas las apps de la lista** 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 con acceso a Internet**, haga clic en **Agregar**.
Se abre la ventana **Agregar aplicación**.
 - b. En el campo **Nombre de la app**, escriba el nombre de una aplicación móvil.
 - c. En el campo **Nombre del paquete**, 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 **Modificar** y **Eliminar** que se encuentran en la parte superior de la lista.

8. Haga clic en **Aceptar**.

9. Haga clic en el botón **Guardar** 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 **Configuración** → **Configuración de la aplicación** → **Antimalware** → **Iniciar análisis**.

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 **Configuración** → **Configuración de la aplicación** → **Antimalware** → **Configuración de análisis**.
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 (**Configuración** → **Informes**). 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](#) ^[2].

Para configurar la programación del análisis completo del dispositivo:

1. En la ventana principal de Kaspersky Endpoint Security, toque **Configuración** → **Configuración de la aplicación** → **Antimalware** → **Configuración de análisis**.
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 **Configuración** → **Configuración de la aplicación** → **Antimalware** → **Modo de protección en tiempo real**.
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 **Configuración** → **Configuración de la aplicación** → **Antimalware**.
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 **Configuración** → **Configuración de la aplicación** → **Antimalware** → **Configuración de análisis**.
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 (**Configuración** → **Informes**). 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 **Configuración** → **Configuración de la aplicación** → **Antimalware** → **Iniciar actualización de las bases de datos**.

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 **Configuración** → **Configuración de la aplicación** → **Antimalware** → **Configuración de actualización de las bases de datos**.
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 for Android como un Servicio 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. 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 **Configuración** → **Configuración de la aplicación** → **Protección web**.

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 **Configuración** → **Configuración de la aplicación** → **Protección web**.

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 **Configuración** → **Configuración de la aplicación** → **Adicional** → **Obtener certificado**.
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 **Configuración** → **Configuración de la aplicación** → **Sincronización**.
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 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 **Notificaciones**.
3. En la notificación sobre el certificado, toque **Instalar**.
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.

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, [active la aplicación](#). Si su dispositivo no está conectado a Kaspersky Security Center, puede [ingresar el código de activación manualmente](#).

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 **Contrato de licencia de usuario final** y **Política de Privacidad de Productos y Servicios**.
O bien, puede aceptar la **Declaración de Kaspersky Security Network** para permitir el envío de estadísticas a Kaspersky Security Network. Esto mejora el rendimiento de la aplicación y garantiza su funcionamiento ininterrumpido.
3. Pulse **Siguiente**. 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 **Activar la app**.
2. En la ventana de activación, ingrese el código de activación que le dio el administrador y toque **Activar**.
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 **Acerca de la app** que se abre, toque **Diagnósticos**.
3. En la ventana **Diagnósticos** que se abre, habilite el diagnóstico mediante el interruptor **Diagnósticos**.
4. Acepte la Declaración de soporte. La Declaración de soporte describe [qué datos se guardan en el archivo con información de diagnóstico](#).
5. Toque **Sin inconvenientes**.

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 (cloud).

Acerca del Contrato de licencia de usuario final

El *Contrato de licencia de usuario final* (EULA) es un acuerdo vinculante entre usted y AO Kaspersky Lab en el que se estipulan los Términos y condiciones para utilizar MDM básico en Kaspersky Next Expert View (cloud).

Le recomendamos que lea detenidamente los Términos y condiciones del EULA antes de utilizar MDM básico en Kaspersky Next Expert View (cloud).

Puede consultar los Términos y condiciones del EULA de las siguientes maneras:

- Durante la instalación de componentes de MDM básico en Kaspersky Next Expert View (cloud).
- 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 **Acerca de la app** → **Contratos y Declaraciones** 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** → **Contratos de licencia de usuario final** en las propiedades del Servidor de administración de Kaspersky Security Center Web Console.
- En el paso 4 del proceso de [conexión de dispositivos móviles a Kaspersky Security Center Web Console](#), si se seleccionó **Administrador** en el paso 3. Se le pedirá al administrador que acepte el EULA.
- Durante la instalación de la aplicación, si se seleccionó **Usuarios** en el paso 3 del proceso de [conexión de dispositivos móviles a Kaspersky Security Center Web Console](#). 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 de MDM básico en Kaspersky Next Expert View (cloud), indica que 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 de MDM básico en Kaspersky Next Expert View (cloud) y abstenerse de utilizarlos.

Acerca de la licencia

Una *licencia* AO es un derecho con límite de tiempo para usar MDM básico en Kaspersky Next Expert View (cloud), que se otorga 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.

Se proporcionan los siguientes tipos de licencia:

- *Prueba*

Una licencia gratuita destinada a probar MDM básico en Kaspersky Next Expert View (cloud).

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.

Con una licencia que no proporciona la funcionalidad extendida de MDM básico en Kaspersky Next Expert View (cloud), solo están disponibles los ajustes básicos de protección del dispositivo en el complemento Kaspersky Mobile Devices Protection and Management.

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 (cloud), seleccione **Administración de activos** → **Directivas**. 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 **Configuración de la aplicación**.
3. Haga clic en **Licencia**.

Se abre la ventana **Licencia** que contiene información sobre la licencia.

Acerca de la suscripción

La suscripción para MDM básico en Kaspersky Next Expert View (cloud) 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 MDM básico en Kaspersky Next Expert View (cloud) 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 MDM básico en Kaspersky Next Expert View (cloud) siga funcionando después de que venza 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 MDM básico en Kaspersky Next Expert View (cloud) 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 de MDM básico en Kaspersky Next Expert View (cloud).

Acerca de la clave de licencia

Una *clave de licencia* es una secuencia de bits que puede aplicar para activar y luego usar la solución integrada MDM básico en Kaspersky Next Expert View (cloud) 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 (cloud) o de solicitar la versión de prueba de MDM básico en Kaspersky Next Expert View (cloud).

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 (cloud) o solicitó la versión de prueba de MDM básico en Kaspersky Next Expert View (cloud).

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

MDM básico en Kaspersky Next Expert View (cloud) 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 apps.** 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 (contenido 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 subprocesso
- marca que indica si el marco fue el motivo del error de Software
- marca que indica que el subprocesso 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 subprocesso, 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 (cloud) 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 **Acerca de la app** → **Contratos y Declaraciones** 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 (cloud) ni en ninguna de las fuentes de información sobre este, póngase en contacto con el 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 (cloud).

Kaspersky ofrece soporte para el MDM básico en Kaspersky Next Expert View (cloud) durante su vida útil ([página de vida útil del soporte técnico del producto](#)). Antes de comunicarse con el Servicio de soporte técnico, lea las [reglas del soporte técnico](#).

Puede comunicarse con el Servicio de soporte técnico de una de las siguientes maneras:

- [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 del Servicio de soporte técnico](#) .

Fuentes de información acerca de la aplicación

Página web de MDM básico en Kaspersky Next Expert View (cloud) en el sitio web de Kaspersky

En la [página de MDM básico en Kaspersky Next Expert View \(cloud\)](#), podrá encontrar información general sobre la aplicación, sus funciones y sus parámetros de funcionamiento.

La página web de MDM básico en Kaspersky Next Expert View (cloud) proporciona un vínculo a eStore. Donde podrá comprar la aplicación o hacer la renovación.

Página web de MDM básico en Kaspersky Next Expert View (cloud) 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 de MDM básico en Kaspersky Next Expert View \(cloud\) en la Base de conocimientos](#), podrá encontrar artículos con información útil, recomendaciones y respuestas a las preguntas más frecuentes sobre la adquisición, la instalación y el uso de la aplicación.

Los artículos de la Base de conocimientos pueden responder preguntas relacionadas no solo con MDM básico en Kaspersky Next Expert View (cloud), 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 contextual de los complementos de administración para MDM básico en Kaspersky Next Expert View (cloud) proporciona información sobre las ventanas de Kaspersky Security Center: una descripción de la configuración de MDM básico en Kaspersky Next Expert View (cloud) y enlaces a las descripciones de las tareas que usan esta configuración.

La ayuda completa de las aplicaciones Kaspersky Endpoint Security para Android y Kaspersky Protection para iOS proporciona información de la configuración y el uso de 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 y tareas de grupo para dispositivos de un 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 (nube). 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 del servidor de administración aprobado por Kaspersky que se envía 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 134.

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. El Servidor web 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

Archivo en formato PLIST que contiene un vínculo al archivo de 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 dedicado que proporciona la interfaz para administrar dispositivos móviles a través de Kaspersky Next Expert View (nube).

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 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 **Acerca de la 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, SecuriID 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.