kaspersky

Kaspersky Security para dispositivos móviles

Contenido

Ayuda de Kaspersky Security para dispositivos móviles

Kaspersky Security para dispositivos móviles está diseñado para proteger y administrar los dispositivos móviles corporativos, así como los dispositivos móviles personales que utilizan los empleados de la empresa con fines corporativos.

Los componentes y las funciones de Kaspersky Security para dispositivos móviles están disponibles en función de la consola de Kaspersky Security Center que utiliza como interfaz para proteger y administrar los dispositivos móviles.

Seleccione la sección que necesite en Ayuda, según su consola de Kaspersky Security Center:

- Consola de administración basada en Microsoft Management Console
- Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console

Diferentes secciones de Ayuda describen funcionalidades y operaciones disponibles para usuarios de las aplicaciones Kaspersky Endpoint Security para Android y Kaspersky Security para iOS.

Novedades

Kaspersky Security para iOS, versión técnica 1

La nueva aplicación de Kaspersky Security para iOS está diseñada para proteger y administrar los dispositivos iOS y iPadOS empresariales. La aplicación ofrece las siguientes funciones clave:

- Protección contra amenazas en línea.
- Detección de liberación.
- Administración de dispositivos empresariales con Kaspersky Security Center Web Console y Cloud Console.

Kaspersky Endpoint Security para Android, versión técnica 42

- Mejoras en la interfaz de usuario de la aplicación Kaspersky Endpoint Security para Android.
- La aplicación Kaspersky Endpoint Security para Android ahora requiere el permiso de "Dispositivos Bluetooth cercanos" en Android 12 o versiones posteriores para permitir que el administrador restrinja el uso de Bluetooth.
- Mejoras y correcciones de errores generales.

Kaspersky Endpoint Security para Android, versión técnica 41

- Mejoras en la interfaz de usuario de la aplicación Kaspersky Endpoint Security para Android.
- Mejoras de la interfaz de usuario en la configuración de directivas del complemento de Kaspersky Security for Mobile (Policies) para Kaspersky Security Center Web Console y Cloud Console.
- Mejoras y correcciones de errores generales.

Kaspersky Endpoint Security para Android, versión técnica 40

- Mejoras y correcciones de errores generales.

Kaspersky Endpoint Security para Android, versión técnica 39

- Ahora es compatible con Android 12L.
- Se actualizaron los siguientes contratos y declaraciones:
  - Contrato de licencia de usuario final
  - Declaración de Kaspersky Security Network
  - Declaración sobre el procesamiento de datos para propósitos de marketing

Tenga en cuenta que el administrador puede aceptar los nuevos términos de los contratos y las declaraciones en la Consola de administración. Esto permite omitir este paso para los usuarios de la aplicación Kaspersky Endpoint Security para Android en dispositivos.

- Mejoras y correcciones de errores generales.

Kaspersky Endpoint Security para Android, versión técnica 33

- Al administrar la aplicación Kaspersky Endpoint Security para Android mediante sistemas EMM de otras empresas, ahora puede aceptar varios contratos de licencia de usuario final con un solo comando.
- Ya no necesita una clave para habilitar Samsung KNOX.
- La estructura de las versiones de los componentes de Kaspersky Security for Mobile se modificó para incluir el número de versión.

Kaspersky Endpoint Security para Android, versión técnica 32

- La aplicación Kaspersky Endpoint Security para Android se modificó para admitir los requisitos actualizados de Android.

Kaspersky Endpoint Security para Android, versión técnica 31

- Si Kaspersky Security Center no está implementado en su organización o no es accesible para los dispositivos móviles, los usuarios pueden activar la aplicación Kaspersky Endpoint Security para Android en sus dispositivos manualmente.
- Kaspersky Security para dispositivos móviles ahora es compatible con la función Pestañas personalizadas de Google Chrome.

Kaspersky Endpoint Security para Android, versión técnica 30

- Kaspersky Security para dispositivos móviles ahora le permite proteger y administrar dispositivos móviles en Kaspersky Security Center Cloud Console.
- Kaspersky Security para dispositivos móviles ahora es compatible con iOS 15 y iPadOS 15.

Kaspersky Endpoint Security para Android, versión técnica 29

- Ahora, Kaspersky Endpoint Security para Android funciona en Android 12.

Kaspersky Endpoint Security para Android, versión técnica 27

- Kaspersky Security para dispositivos móviles ahora le permite proteger y administrar dispositivos móviles en Kaspersky Security Center Web Console.

Kaspersky Endpoint Security para Android, versión técnica 26

- Kaspersky Endpoint Security ahora admite licencias y suscripciones con renovación automática.

Kaspersky Endpoint Security para Android, versión técnica 22

- Kaspersky Endpoint Security ahora es compatible con Kaspersky Private Security Network, una solución que permite el acceso a las bases de datos de reputación de Kaspersky Security Network sin enviar datos fuera de la red corporativa.
- Kaspersky Endpoint Security para Android ya no admite la instalación en dispositivos con versiones de Android 4.2 - 4.4.4.

Kaspersky Endpoint Security para Android, versión técnica 20

- No se les solicita a los usuarios que acepten las declaraciones legales si el administrador opta por aceptar las declaraciones globalmente.
- Se ha optimizado el rendimiento de la aplicación.

Kaspersky Endpoint Security para Android, versión técnica 19

- El administrador ahora puede aceptar las declaraciones de Kaspersky Security Network y otras declaraciones en nombre de los usuarios finales a través de Kaspersky Security Center.
- Se han corregido varios errores y se ha mejorado la estabilidad operativa.

Kaspersky Endpoint Security para Android, versión técnica 18

- Ahora Kaspersky Security for Mobile es compatible con Huawei Mobile Services.
- Ahora, Kaspersky Endpoint Security para Android puede instalarse desde Huawei AppGallery.

Kaspersky Endpoint Security para Android, versión técnica 17

- Kaspersky Endpoint Security ahora apunta al nivel 29 y superiores de la API, lo que provoca algunos cambios en el comportamiento de las aplicaciones en los dispositivos que ejecutan Android 10 o superior.
- Nueva configuración de la seguridad de la contraseña para que el usuario pueda establecer contraseñas de la complejidad requerida.
- La configuración del uso de la huella dactilar como método de desbloqueo de pantalla está ahora disponible sólo para el perfil de trabajo de Android.
- Se han corregido varios errores y se ha mejorado la estabilidad operativa.

Kaspersky Endpoint Security para Android, versión técnica 16

- Ahora, Kaspersky Endpoint Security para Android funciona en Android 11.
- Android 11 introdujo nuevos requisitos para los permisos de geolocalización y cámara. Puede leer más acerca de las nuevas reglas sobre los permisos de acceso a la cámara y la ubicación en esta sección.
- Ahora, puede especificar las direcciones de correo electrónico corporativo de los usuarios en una consola EMM de terceros. Estos correos electrónicos se visualizarán en el Kaspersky Security Center, siempre y cuando el nuevo KscCorporateEmail esté configurado.

Kaspersky Endpoint Security para Android, versión técnica 14

- Cada vez que un usuario permite o revoca los privilegios de administrador de dispositivos de la aplicación, se envía un evento a la Consola de gestión.
- Ahora, el parámetro "KscGroup" puede configurarse en consolas EMM de terceros. Cuando un dispositivo se conecta a Kaspersky Security Center, se lo añade automáticamente a una subcarpeta de la carpeta Dispositivos no asignados con el mismo nombre que el grupo configurado en la consola EMM.

Kaspersky Endpoint Security para Android, versión técnica 13

- Nuevo diseño de la interfaz de usuario para Kaspersky Endpoint Security para Android.
- Ahora todas las secciones de ayuda son en línea.
- Las direcciones IP de los dispositivos administrados ahora se envían a Kaspersky Security Center y pueden visualizarse en las secciones de información de los dispositivos.

Kaspersky Endpoint Security para Android, versión técnica 12

- Se añadió la capacidad de aceptar remotamente el Contrato de licencia de usuario final (EULA) en Kaspersky Security Center 12.1. Si el administrador acepta los términos del Contrato de licencia y la Política de privacidad en la Consola de administración, la aplicación omite estos pasos durante el proceso de instalación.
- Se agregó la capacidad de editar el nombre del dispositivo en Kaspersky Security Center para usuarios que utilizan VMware AirWatch. Agregamos una nueva opción al archivo de configuración, que se utiliza para configurar la aplicación. Puede agregar más información al nombre del dispositivo (por ejemplo, su número de serie). Esto hace que sea más fácil encontrar y ordenar dispositivos en Kaspersky Security Center.

Kaspersky Endpoint Security para Android, versión técnica 11

Se han corregido varios errores y se ha mejorado la estabilidad operativa.

Kaspersky Endpoint Security para Android, versión técnica 10

- Ahora Kaspersky Security para dispositivos móviles es compatible con Kaspersky Security Center 12.
- La compatibilidad con Kaspersky Safe Browser se ha suspendido en Kaspersky Security Center 12. Puede utilizar las funciones de Kaspersky Safe Browser cuando use Kaspersky Security Center 11 o versiones anteriores.
- Se han corregido varios errores y se ha mejorado la estabilidad operativa.

Kaspersky Endpoint Security para Android Service Pack 4 Maintenance Release 3

- Compatibilidad comprobada de Kaspersky Endpoint Security para Android en Microsoft Intune (una solución de Gestión de Movilidad Empresarial, (EMM)). Kaspersky participa en la Comunidad AppConfig para garantizar que la aplicación opere con las soluciones EMM de otras empresas.

- Se agregó la capacidad de desactivar las notificaciones y los mensajes emergentes cuando la aplicación se ejecute en segundo plano. Tenga en cuenta que no es seguro realizar estas acciones en segundo plano. Si desactiva 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. Los usuarios de dispositivos móviles pueden conocer el estado de protección del dispositivo solo cuando abren la aplicación.

- Se añadió la capacidad de aceptar el Contrato de licencia de usuario final (EULA) y la Política de privacidad en VMware AirWatch. Si el administrador aceptó el Contrato de licencia y la Política de privacidad en la consola AirWatch, Kaspersky Endpoint Security para Android omitirá el paso de aceptación en el Asistente de configuración inicial.

- Se agregó la Declaración sobre el procesamiento de datos para usar Protección web (Declaración de Protección web). Debe aceptar la declaración para usar la Protección web. Kaspersky Endpoint Security para Android utiliza Kaspersky Security Network (KSN) para analizar sitios web. La Declaración de Protección web contiene los términos y las condiciones del intercambio de datos con KSN. Puede aceptar la Declaración de Protección web en la directiva o solicitar la aceptación del usuario del dispositivo.

- Se han corregido varios errores y se ha mejorado la estabilidad operativa.

Comparación de las funciones de la aplicación según las herramientas de administración

Puede administrar dispositivos móviles en Kaspersky Security Center mediante las siguientes herramientas de administración:

- Consola de administración basada en Microsoft Management Console (en lo sucesivo, "basada en MMC") de Kaspersky Security Center
- Kaspersky Security Center Web Console
- Kaspersky Security Center Cloud Console

La siguiente tabla compara las funciones que están disponibles en estas herramientas.

Disponibilidad de las funciones según las herramientas de administración

	Consola basada en MMC	Web Console	Cloud Console
General			
Administración de dispositivos Android	Disponible	Disponible	Disponible
Administración de dispositivos iOS	Disponible (mediante un certificado de APN)	Disponible (mediante la aplicación Kaspersky Security para iOS)	Disponible (mediante la aplicación Kaspersky Security para iOS)
Administración de dispositivos móviles			
Agregado de dispositivos mediante un enlace de Google Play	Disponible	Disponible	Disponible
Agregado de dispositivos mediante un enlace de App Store	No disponible	Disponible	Disponible
Agregado de dispositivos iOS mediante un perfil de MDM para iOS	Disponible	No disponible	No disponible
Agregado de dispositivos mediante la creación de un paquete de instalación	Disponible	No disponible	No disponible
Envío de comandos a dispositivos móviles	Disponible	Disponible (excepto el comando Foto de identificación)	Disponible (excepto el comando Foto de identificación)
Eliminación de dispositivos móviles de Kaspersky Security Center	Disponible	Disponible (Eliminación de la lista de dispositivos únicamente. La aplicación debe eliminarse del dispositivo de forma manual.)	Disponible (Eliminación de la lista de dispositivos únicamente. La aplicación debe eliminarse del dispositivo de forma manual.)

Administración de certificados			
Emisión de certificados de correo	Disponible	No disponible	No disponible
Emisión de certificados de VPN	Disponible	No disponible	No disponible
Emisión de certificados móviles	Disponible	Disponible	Disponible
Emisión de certificados móviles mediante herramientas del Servidor de administración	Disponible	Disponible	Disponible
Especificación de archivos de certificado	Disponible	No disponible	No disponible
Integración con la infraestructura de clave pública	Disponible	No disponible	No disponible
Administración de directivas			
Acceso basado en roles para configurar las directivas de grupo	Disponible	No disponible	No disponible
Configuración de la sincronización de dispositivos móviles con Kaspersky Security Center	Disponible	Disponible	Disponible
Configuración del análisis de virus en dispositivos móviles	Disponible	Disponible	Disponible
Configuración de la protección de dispositivos móviles	Disponible	Disponible	Disponible
Configuración de las actualizaciones de las bases de datos antivirus	Disponible	Disponible	Disponible
Configuración de la protección de datos de dispositivos robados o perdidos	Disponible	Disponible	Disponible
Configuración de acceso de usuarios a sitios web	Disponible	Disponible	Disponible
Configuración del Control de apps	Disponible	Disponible	Disponible
Configuración del control de cumplimiento	Disponible	Disponible	Disponible
Configuración de los perfiles de trabajo de Android	Disponible	No disponible	No disponible

Configuración de conexión a una red Wi-Fi	Disponible	No disponible	No disponible
Samsung KNOX	Disponible	No disponible	No disponible
Otras funciones			
Aceptación global del EULA en Kaspersky Security Center	Disponible	No disponible	No disponible
Configuración de Kaspersky Private Security Network	Disponible	No disponible	No disponible

Kit de distribución

El kit de distribución de Kaspersky Security para dispositivos móviles puede incluir varios componentes según la versión de aplicación seleccionada.

Administración de dispositivos móviles en Kaspersky Security Center Web Console

- `on_prem_ksm_devices_xx.x.x.x.zip`

  Carpeta comprimida que contiene los archivos necesarios para instalar el complemento de Kaspersky Security for Mobile (Devices):

  - `plugin.zip`

    Carpeta comprimida que contiene el complemento de Kaspersky Security for Mobile (Devices).

  - `signature.txt`

    Archivo que contiene la firma del complemento de Kaspersky Security for Mobile (Devices).

- `on_prem_ksm_policies_xx.x.x.x.zip`

  Carpeta comprimida que contiene los archivos necesarios para instalar el complemento de Kaspersky Security for Mobile (Policies):

  - `plugin.zip`

    Carpeta comprimida que contiene el complemento de Kaspersky Security for Mobile (Policies).

  - `signature.txt`

    Archivo que contiene la firma del complemento de Kaspersky Security for Mobile (Policies).

Administración de dispositivos móviles en Kaspersky Security Center Cloud Console

Para administrar dispositivos móviles en Kaspersky Security Center Cloud Console, no es necesario descargar un paquete de distribución. Solo necesita crear una cuenta en Kaspersky Security Center Cloud Console. Para obtener más información sobre cómo crear una cuenta, consulte la *Ayuda de Kaspersky Security Center Cloud Console*.

Administración de dispositivos móviles en la Consola de administración basada en MMC

- `Klcfginst_en.exe`

  Instalador del complemento de administración de Kaspersky Endpoint Security para Android con el fin de gestionar la aplicación mediante el sistema de administración remota de Kaspersky Security Center.

- `Klmdminst.exe`

  Instalador del complemento de administración de Kaspersky Device Management para iOS con el fin de gestionar la aplicación mediante el sistema de administración remota de Kaspersky Security Center.

Archivo de la aplicación Kaspersky Endpoint Security para Android

`KES10_xx_xx_xxx.apk`: archivo de paquete de Android de la aplicación Kaspersky Endpoint Security para Android.

Archivos auxiliares

- `sc_package_xx.exe`

  Carpeta comprimida de extracción automática que contiene los archivos necesarios para instalar la aplicación Kaspersky Endpoint Security para Android mediante la creación de paquetes de instalación:

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

    Archivos necesarios para crear paquetes de instalación.

  - `installer.ini`

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

  - `KES10_xx_xx_xxx.apk`

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

  - `kmlisten.exe`

    Herramienta para enviar paquetes de instalación a través del equipo del administrador.

  - `kmlisten.ini`

    Archivo de configuración que contiene los ajustes de la utilidad `kmlisten.exe`.

  - `kmlisten.kpd`

    Archivo de descripción de la aplicación.

- `SigningUtility.zip`

  Carpeta comprimida que contiene la utilidad para firmar el paquete de distribución de la aplicación Kaspersky Endpoint Security para Android y los contenedores para dispositivos iOS.

Documentación

- Ayuda de Kaspersky Security para dispositivos móviles.

Trabajar en Kaspersky Security Center Web Console y Kaspersky Security Center Cloud Console

En esta sección de Ayuda, se describe la protección y administración de dispositivos móviles mediante Kaspersky Security Center Web Console (en adelante, también denominada Web Console) o Kaspersky Security Center Cloud Console (en adelante, también denominada Cloud Console).

Acerca de la administración de dispositivos móviles en Kaspersky Security Center Web Console y Cloud Console

Puede administrar los dispositivos móviles en Kaspersky Security Center Web Console y Cloud Console con los siguientes componentes:

- **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.

- **Aplicación Kaspersky Security para iOS**

  La aplicación Kaspersky Security para iOS garantiza la protección de dispositivos móviles frente a phishing y malware.

- **Complemento de Kaspersky Security for Mobile (Devices)**

  El complemento de Kaspersky Security for Mobile (Devices) proporciona la interfaz a fin de administrar los dispositivos móviles y las aplicaciones móviles allí instaladas a través de Kaspersky Security Center Web Console y Cloud Console.

- **Complemento de Kaspersky Security for Mobile (Policies)**

  El complemento de Kaspersky Security for Mobile (Policies) le permite definir las opciones de configuración para los dispositivos conectados a Kaspersky Security Center mediante el uso de directivas de grupo.

Los complementos están integrados en *el sistema de administración remota de Kaspersky Security Center*. Puede utilizar Kaspersky Security Center Web Console o Cloud Console para administrar dispositivos móviles, equipos cliente y sistemas virtuales. Los dispositivos móviles pasan a estar administrados tras conectarlos al Servidor de Administración. Puede supervisar los dispositivos administrados de forma remota.

Funciones clave de administración de dispositivos móviles en Kaspersky Security Center Web Console y Cloud Console

Kaspersky Security para dispositivos móviles presta las siguientes funciones:

- Distribución de mensajes de correo electrónico para conectar dispositivos móviles Android a Kaspersky Security Center mediante enlaces de descarga de la aplicación Kaspersky Endpoint Security para Android desde Google Play.

- Distribución de mensajes de correo electrónico para conectar dispositivos móviles iOS a Kaspersky Security Center mediante enlaces de descarga de la aplicación Kaspersky Security para iOS desde App Store.

- Conexión remota de dispositivos móviles a Kaspersky Security Center y otros sistemas de EMM externos (por ejemplo, VMWare AirWatch, MobileIron, IBM Maas360, SOTI MobiControl).
- Configuración remota de la aplicación móvil, así como configuración remota de servicios, aplicaciones y funciones de dispositivos móviles.
- Configuración remota de los dispositivos móviles de acuerdo con los requerimientos de seguridad corporativa.
- Prevención de la fuga de información corporativa almacenada en los dispositivos móviles en caso de pérdida o robo (Antirrobo). Compatible solo con dispositivos Android.
- Control de cumplimiento con los requisitos corporativos de seguridad (Control de cumplimiento). Compatible solo con dispositivos Android.
- Control de la protección frente a amenazas en línea y control del uso de Internet en dispositivos móviles (Protección web).
- Configuración de las notificaciones que se muestran al usuario en las aplicaciones Kaspersky Endpoint Security para Android y Kaspersky Security para iOS.
- Las notificaciones de administrador sobre el estado y los eventos de las aplicaciones Kaspersky Endpoint Security para Android y Kaspersky Security para iOS pueden comunicarse en Kaspersky Security Center o por correo electrónico.
- Control de cambios para la configuración de la directiva (historial de revisiones).

Kaspersky Security para dispositivos móviles incluye los siguientes componentes de protección y administración:

- Antivirus (para dispositivos con Android)
- Antirrobo (para dispositivos con Android)
- Protección web (en dispositivos con Android y iOS)
- Control de apps (en dispositivos Android)
- Control de cumplimiento (en dispositivos con Android)
- Detección de privilegios de root en dispositivos Android y detección de liberación en dispositivos iOS

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 los siguientes componentes:

- **Antivirus**. Este componente detecta y neutraliza amenazas en el dispositivo mediante las bases de datos antivirus de la aplicación y el servicio en la nube de Kaspersky Security Network. Antivirus 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 para un archivo o carpeta previamente seleccionados.
- **Actualizar**. Le permite descargar nuevas bases de datos antivirus para la aplicación.

- **Antirrobo**. El componente protege 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**. Le permite obtener las coordenadas de la ubicación del dispositivo.
  - **Alarma**. Provoca que el dispositivo emita un sonido de alarma fuerte.
  - **Eliminar**. Borre los datos corporativos para proteger la información confidencial de la empresa.
- **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. Protección web también permite filtrar sitios web por 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, páginas web con las categorías "Juegos de azar, loterías, sorteos" o "Comunicación por Internet").
- **Control de apps.** Este componente le 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 apps permite eliminar aplicaciones bloqueadas que infrinjan 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 Security Center Web Console y Cloud Console al definir la configuración de las directivas de grupo.

Acerca de la aplicación Kaspersky Security para iOS

La aplicación Kaspersky Security para iOS garantiza la protección de dispositivos móviles frente a phishing y malware.

La aplicación Kaspersky Security 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 Security Center Web Console al definir los parámetros de las directivas de grupo.
- **Detección de liberación**. Cuando Kaspersky Security para iOS detecta una liberación, muestra un mensaje crítico y le brinda una notificación sobre el problema.

Acerca del complemento de Kaspersky Security for Mobile (Devices)

El complemento de Kaspersky Security for Mobile (Devices) proporciona la interfaz a fin de administrar los dispositivos móviles y las aplicaciones móviles allí instaladas a través de Kaspersky Security Center Web Console y Cloud Console. El complemento de Kaspersky Security for Mobile (Devices) le permite realizar lo siguiente:

- Conectar los dispositivos móviles a Kaspersky Security Center.
- Administrar los certificados de dispositivos móviles.
- Configurar Firebase Cloud Messaging (solo para dispositivos Android).
- Enviar comandos a dispositivos móviles (solo para dispositivos Android).

El complemento de Kaspersky Security for Mobile (Devices) se puede instalar al configurar Kaspersky Security Center Web Console. Si utiliza Kaspersky Security Center Cloud Console, no necesita instalar este complemento. Para obtener más información sobre los escenarios de despliegue en diferentes tipos de consolas, consulte la sección "Escenarios de implementación".

Acerca del complemento de Kaspersky Security for Mobile (Policies)

El complemento de Kaspersky Security for Mobile (Policies) le permite definir las opciones de configuración para los dispositivos conectados a Kaspersky Security Center mediante el uso de directivas de grupo. El complemento de Kaspersky Security for Mobile (Policies) se puede utilizar para realizar lo siguiente:

- Crear directivas de seguridad de grupo para los dispositivos móviles.
- Definir de forma remota la configuración de la aplicación móvil en dispositivos móviles de los usuarios.
- Recibir informes y estadísticas de funcionamiento de la aplicación móvil en dispositivos móviles de los usuarios.

El complemento de Kaspersky Security for Mobile (Policies) se puede instalar al configurar Kaspersky Security Center Web Console. Si utiliza Kaspersky Security Center Cloud Console, no necesita instalar este complemento. Para obtener más información sobre los escenarios de despliegue en diferentes tipos de consolas, consulte la sección "Escenarios de implementación".

Requisitos de hardware y software

En esta sección, se enumeran los requisitos de hardware y software del equipo del administrador utilizado para instalar los complementos Kaspersky Security for Mobile (Devices) y Kaspersky Security for Mobile (Policies) en Kaspersky Security Center Web Console y Cloud Console, así como los requisitos de hardware y software de las aplicaciones móviles.

Requisitos de hardware y software para el equipo del administrador

Para instalar el complemento de Kaspersky Security for Mobile (Devices) y de Kaspersky Security for Mobile (Policies), el equipo del administrador debe reunir los requisitos de hardware de Kaspersky Security Center. Para obtener más información sobre los requisitos de hardware y software de Kaspersky Security Center, siga los siguientes pasos:

- Si utiliza Kaspersky Security Center Web Console, consulte la *Ayuda de Kaspersky Security Center*.
- Si utiliza Kaspersky Security Center Cloud Console, consulte la *Ayuda de Kaspersky Security Center Cloud Console*.

Para utilizar el complemento de Kaspersky Security for Mobile (Devices) y de Kaspersky Security for Mobile (Policies) en Kaspersky Security Center Web Console, se debe instalar Kaspersky Security Center Web Console en el equipo del administrador.

Para utilizar el complemento de Kaspersky Security for Mobile (Devices) y de Kaspersky Security for Mobile (Policies) en Kaspersky Security Center Cloud Console, debe crear una cuenta en Kaspersky Security Center Cloud Console. Para obtener más información sobre cómo crear una cuenta, consulte la *Ayuda de Kaspersky Security Center Cloud Console*.

La aplicación Kaspersky Endpoint Security para Android puede funcionar en los siguientes sistemas EMM de terceros:

- VMWare AirWatch 9.3 o posterior
- MobileIron 10.0 o posterior
- IBM MaaS360 10.68 o posterior
- Microsoft Intune 1908 o posterior
- SOTI MobiControl 14.1.4 (1693) o posterior

Requisitos de hardware y software para que el dispositivo móvil del usuario admita la instalación de la aplicación Kaspersky Endpoint Security para Android

Estos son los requisitos de hardware y software de la aplicación Kaspersky Endpoint Security para Android:

- 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
- Android 5.0–12 (incluye Android 12L, no incluye la edición Go)
- 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 que el dispositivo móvil del usuario admita la instalación de la aplicación Kaspersky Security para iOS

La aplicación Kaspersky Security para iOS tiene los siguientes requisitos de hardware:

- iPhone 6S o posterior
- iPad Air 2 o posterior

La aplicación Kaspersky Security para iOS tiene los siguientes requisitos de sistema:

- iOS 14.1 o posterior

- iPadOS 14.1 o posterior

La aplicación Kaspersky Security para iOS no puede funcionar debidamente cuando un cliente VPN con una conexión VPN activa se está ejecutando en el mismo dispositivo móvil.

Consideraciones y problemas conocidos

Kaspersky Endpoint Security para Android y Kaspersky Security para iOS tienen varios problemas conocidos, que no son críticos para el funcionamiento de estas aplicaciones.

Problemas conocidos de Kaspersky Security para iOS

- La aplicación Kaspersky Security para iOS no puede funcionar debidamente cuando un cliente VPN con una conexión VPN activa se está ejecutando en el mismo dispositivo móvil.

Problemas conocidos de Kaspersky Endpoint Security para Android

Problemas conocidos al iniciar la administración de dispositivos móviles en Kaspersky Security Center Web Console

- Puede iniciar la administración de dispositivos móviles durante la configuración inicial de la Consola de administración basada en MMC de Kaspersky Security Center (mientras ejecuta el Asistente de inicio rápido) o más tarde al visualizar la carpeta Administración de dispositivos móviles en la Consola de administración.

Problemas conocidos al instalar aplicaciones

- Kaspersky Endpoint Security para Android solo se instala en la memoria principal del dispositivo.
- En dispositivos con Android 7.0, 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 otras empresas (por ejemplo, VMWare AirWatch), solo los componentes Antivirus y Protección Web están disponibles. El administrador puede ajustar la configuración del Antivirus 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).

Problemas conocidos al actualizar la versión de la aplicación

- 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 en la operación del Antivirus

- 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 aplicación omite esos archivos sin notificarle que se omitieron.
- Para el análisis adicional de un dispositivo para amenazas nuevas cuya información todavía no se ha añadido a las bases de datos antivirus, 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 antivirus desde el Servidor de administración en un dispositivo móvil. Si eso sucede, ejecute la tarea de actualización de las bases de datos antivirus en el Servidor de administración.
- En ciertos dispositivos, Kaspersky Endpoint Security para Android no detecta dispositivos conectados por USB al instante. No es posible ejecutar un análisis antivirus en tales dispositivos.
- En dispositivos con Android 11.0 o versiones posteriores, el usuario debe otorgar el permiso "Permitir el acceso para administrar todos los archivos".
- En dispositivos que ejecuten Android 7.0 o versiones posteriores, puede que la ventana de configuración de la planificación de ejecución de análisis antivirus se muestre incorrectamente (no se muestran los elementos de administración). La causa de este problema es un defecto conocido de Android 7.
- En dispositivos que ejecutan Android 7.0, la protección en tiempo real en el modo extendido no detecta amenazas en archivos almacenados en una tarjeta SD externa.
- En dispositivos con Android 6.0, Kaspersky Endpoint Security para Android no detecta la descarga de archivos maliciosos a la memoria del dispositivo. El antivirus puede detectar un archivo malicioso cuando se ejecuta el archivo o durante un análisis antivirus en el dispositivo. La causa de este problema es un defecto conocido de Android 6.0. Para garantizar la seguridad del dispositivo, se recomienda configurar análisis de virus programados.

Problemas conocidos en la operación de Protección web

- La Protección web en los dispositivos Android solo funciona en el navegador Google Chrome (incluida la función de Pestañas personalizadas), el navegador Huawei y el navegador de Internet de Samsung.
- Para que la Protección web funcione, debe habilitar el uso de Kaspersky Security Network. La Protección web bloquea sitios web según los datos que tenga KSN sobre la reputación y categoría de los sitios web.
- Los sitios web bloqueados pueden permanecer desbloqueados por la Protección web en dispositivos Android 6.0 con la versión 51 Google Chrome (o cualquier versión anterior) 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 historial de búsqueda.
- Utilización de la dirección web para completar automáticamente la función.
- 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 aplicaciones de otras empresas, por ejemplo, desde una aplicación del cliente MI. Este problema se relaciona con cómo el servicio de Accesibilidad funciona con la función de Chrome Custom Tabs.
- Los sitios web bloqueados pueden permanecer desbloqueados en el Navegador de Samsung si el usuario los abre en segundo plano desde el menú de contexto o desde aplicaciones de otras empresas, por ejemplo, desde una aplicación del cliente de MI.
- Kaspersky Endpoint Security para Android debe estar configurado como una función de accesibilidad para asegurar el correcto funcionamiento de Protección web.
- Los sitios web permitidos se pueden bloquear en el Navegador de Samsung en el modo de Protección Web **Solo sitios web enumerados están permitidos** cuando la página se actualiza. Los sitios web se bloquean si una expresión habitual contiene la configuración avanzada (por ejemplo, `^https?:\/\/example\.com\/pictures\/`). Se recomienda usar expresiones habituales sin la configuración adicional (por ejemplo, `^https?:\/\/example\.com`).

Problemas conocidos en la operación 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 7.0 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 ha sido confirmado en Alcatel 5080X.
- Para localizar dispositivos con Android 10.0 o posterior, el usuario debe otorgar el permiso "Todo el tiempo" para la ubicación del dispositivo.

Problemas conocidos en la operación Control de apps

- 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

Añadir aplicaciones particulares a las listas de aplicaciones bloqueadas y permitidas. En este caso, KSN no se requiere.

- Al configurar Control de apps, se recomienda desactivar la casilla **Bloquear apps del sistema**. El bloqueo de apps del sistema puede causar problemas en la operación del dispositivo.

Problemas conocidos al configurar la seguridad de la contraseña de desbloqueo del dispositivo

- En dispositivos con Android 10.0 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 o numérica (PIN) con una secuencia que no tenga números repetidos u ordenados (por ejemplo, 1234), o alfanumérica. El PIN o contraseña debe tener al menos 4 caracteres de extensión.

  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). La extensión del PIN debe ser de al menos 8 dígitos; la contraseña debe contar con 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, para cambiar la contraseña de desbloqueo, solo se debe usar la aplicación del sistema Configuración.

- En algunos dispositivos con Android 6.0 o versiones posteriores, puede ocurrir un error cuando se ingresa la contraseña de desbloqueo de la pantalla si los datos del dispositivo están cifrados. Este problema se debe a características específicas del servicio de Accesibilidad con firmware MIUI.

Problemas conocidos con la protección ante la eliminación de la aplicación

- Se debe configurar Kaspersky Endpoint Security para Android como el administrador del dispositivo.

- Para proteger la aplicación contra la eliminación en dispositivos con Android 7.0 o posterior, Kaspersky Endpoint Security para Android debe estar configurado como función de accesibilidad.

- En algunos dispositivos Huawei y Xiaomi, la protección para eliminación Kaspersky Endpoint Security para Android no funciona. Este problema es causado por características específicas del firmware MIUI 7 y 8 en el firmware EMUI y Xiaomi en Huawei.

Problemas conocidos al configurar las restricciones del dispositivo

- En dispositivos con Android 10.0 o una versión posterior, no se admite prohibir el uso de redes Wi-Fi.

- En dispositivos con Android 10.0 o una versión posterior, el uso de la cámara no se puede prohibir completamente.

- En los dispositivos con Android 11 o posterior, Kaspersky Endpoint Security para Android debe estar configurado como una función de accesibilidad. Kaspersky Endpoint Security para Android solicita al usuario que configure la aplicación 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. Si este es el caso, no podrá restringir el uso de la cámara.

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 no más de 30 minutos antes. De lo contrario, el comando **Localizar dispositivo** falla.

Problemas conocidos con 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 que el dispositivo móvil se reinicia. Además, si el dispositivo se ha bloqueado, no puede usar un comando para desbloquear el dispositivo. Puede desbloquear el dispositivo solo usando un código de desbloqueo de uso único.

- En ciertos dispositivos (por ejemplo, Meizu y Asus) que funcionan con Android 6.0 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 Kaspersky Endpoint Security para Android se establece como función de accesibilidad, puede aparecer una advertencia incorrecta sobre la falta de derechos adecuados. Para esconder este mensaje, habilitar la aplicación como aplicación protegida en la configuración del dispositivo.

- En algunos dispositivos Huawei que operan con Android 5. X o 6. X, cuando el modo de Ahorro de Batería se habilita para Kaspersky Endpoint Security para Android, el usuario puede cancelar manualmente la aplicación. El dispositivo del usuario queda sin protección después de esto. 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 7.0, el usuario puede esconder la notificación en cuanto al 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 6.0, el ícono de Kaspersky Endpoint Security para Android se puede esconder 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 7.0 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.

- La Protección web no puede 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 proporcionan la aplicación de pantallas recientes personalizada con privilegios elevados. 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 con Android 11, la aplicación Kaspersky Endpoint Security para Android se bloquea inmediatamente después del inicio. La causa de este problema es un defecto conocido de Android 11.

Implementación de una solución de administración de dispositivos móviles en Kaspersky Security Center Web Console o Cloud Console

Para administrar dispositivos móviles mediante el uso de Kaspersky Security Center Web Console o Cloud Console, debe implementar una solución de administración de dispositivos móviles.

Escenarios de implementación

Implementación en Kaspersky Security Center Web Console

La implementación de la solución de administración de dispositivos móviles en Kaspersky Security Center Web Console consiste en los siguientes pasos:

1. Preparación de Kaspersky Security Center Web Console para la implementación
2. Implementación de complementos de administración

3. Implementación de la aplicación móvil
4. (Opcional, solo para Android) Configuración del intercambio de información con Firebase Cloud Messaging

   Se recomienda realizar este paso para garantizar la entrega de los comandos a los dispositivos móviles y la sincronización forzada al cambiar la configuración de la directiva.

Implementación en Kaspersky Security Center Cloud Console

La implementación de la solución de administración de dispositivos móviles en Kaspersky Security Center Cloud Console consiste en los siguientes pasos:

1. Preparación de Kaspersky Security Center Cloud Console para la implementación
2. Implementación de la aplicación móvil
3. (Opcional, solo para Android) Configuración del intercambio de información con Firebase Cloud Messaging

   Se recomienda realizar este paso para garantizar la entrega de los comandos a los dispositivos móviles y la sincronización forzada al cambiar la configuración de la directiva.

Preparación de Kaspersky Security Center Web Console y Cloud Console para la implementación

Esta sección proporciona instrucciones sobre cómo preparar Kaspersky Security Center Web Console y Cloud Console para la implementación.

Configuración del Servidor de administración para la conexión de dispositivos móviles

Para que los dispositivos móviles puedan conectarse al Servidor de administración, debe definir la configuración de conexión del dispositivo móvil en las propiedades del Servidor de administración antes de instalar la aplicación Kaspersky Endpoint Security para Android o Kaspersky Security para iOS en los dispositivos móviles.

Para definir la configuración del Servidor de administración de la conexión de dispositivos móviles, siga los siguientes pasos:

1. Inicie la administración de dispositivos móviles en el Servidor de administración.

   Puede iniciar la administración de dispositivos móviles durante la configuración inicial de la Consola de administración basada en MMC de Kaspersky Security Center (mientras ejecuta el Asistente de inicio rápido) o más tarde al visualizar la carpeta Administración de dispositivos móviles en la Consola de administración.

2. En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, haga clic en **Configuración** ( ).

   Se abrirá la ventana de propiedades del Servidor de administración.

3. Configure los puertos del Servidor de administración que utilizarán los dispositivos móviles:

   a. Seleccione la sección **Puertos adicionales**.

   b. Habilite el botón de alternancia **Abrir puerto para dispositivos móviles**.

   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.

   d. En el campo **Puerto para la activación de dispositivos móviles**, especifique el puerto que utilizarán los dispositivos móviles para conectarse al Servidor de administración a fin de activar la aplicación móvil.

      El puerto 17100 se utiliza de forma predeterminada.

      Si especifica un puerto de conexión incorrecto, los usuarios de los dispositivos móviles no podrán activar la aplicación móvil mediante el Servidor de administración.

4. 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 que se creó durante su instalación. Si lo desea, reemplace el certificado emitido a través del Servidor de administración por otro certificado o vuelva a emitir el certificado generado con el Servidor de administración.

   Para editar el certificado, siga los siguientes pasos*:*

   a. Seleccione la sección **Certificados**.

   b. Defina la configuración que requiera.

      Para obtener información detallada sobre los certificados, consulte la *Ayuda de Kaspersky Security Center*.

5. Haga clic en el botón **Guardar** para almacenar los cambios de la configuración y salir de la ventana de propiedades del Servidor de administración.

Después de configurar la conexión del dispositivo móvil, puede instalar las aplicaciones Kaspersky Endpoint Security para Android o Kaspersky Security para iOS en los dispositivos móviles y conectarlos al Servidor de administración mediante el uso de la configuración especificada.

Creación de un grupo de administración

Las directivas de grupo se utilizan para centralizar la configuración de las aplicaciones Kaspersky Endpoint Security para Android y Kaspersky Security para iOS instaladas en los dispositivos móviles de los usuarios.

Para aplicar una directiva a un grupo de dispositivos, es aconsejable crear un grupo aparte para los dispositivos en la carpeta **Dispositivos administrados** antes de instalar las aplicaciones móviles en dispositivos de los usuarios.

Después de crear un grupo de administración, se recomienda configurar la opción de asignar automáticamente los dispositivos en los cuales desee instalar las aplicaciones en este grupo. A continuación, configure los parámetros que son comunes para todos los dispositivos mediante el uso de una directiva de grupo.

Para crear un grupo de administración, haga lo siguiente:

1. En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **JERARQUÍA DE GRUPOS**.

2. En la estructura del grupo de administración, seleccione el grupo de administración que incluirá el nuevo grupo de administración.

3. Haga clic en el botón **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.

Creación de una regla para asignar automáticamente un dispositivo a grupos de administración

Cuando las aplicaciones Kaspersky Endpoint Security para Android o Kaspersky Security para iOS están instaladas en los dispositivos móviles, se muestran en la página **DESCUBRIMIENTO E IMPLEMENTACIÓN** > **DISPOSITIVOS NO ASIGNADOS** de Kaspersky Security Center Web Console o Cloud Console. Para administrar los dispositivos recién conectados, puede moverlos a un grupo de administración manualmente o crear una regla para asignarlos de forma automática a los grupos de administración.

Para crear una regla para la asignación automática de dispositivos móviles a grupos de administración, siga los siguientes pasos:

1. En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DESCUBRIMIENTO E IMPLEMENTACIÓN** > **IMPLEMENTACIÓN Y ASIGNACIÓN** > **REGLAS DE MOVIMIENTO**.

2. En la ventana emergente **Nueva regla**, haga clic en el botón **Agregar**.

3. En el campo **Nombre de la regla**, especifique el nombre de la regla.

4. En el campo **Grupo de administración**, seleccione el grupo de administración al que se asignarán los dispositivos móviles después de que se haya instalado la aplicación en ellos.

5. En la sección **Aplicar regla**, seleccione **Ejecutar una vez para cada dispositivo**.

6. Seleccione la casilla de verificación **Mover solo los dispositivos no agregados a un grupo de administración** para evitar que se muevan los dispositivos móviles asignados a otros grupos de administración al aplicar la regla.

7. Seleccione la casilla de verificación **Habilitar regla** para aplicar la regla inmediatamente después de crearla.

   Puede habilitar la regla en cualquier momento posterior con el botón de alternancia en la página **REGLAS DE MOVIMIENTO**.

8. Seleccione **CONDICIONES DE LA REGLA** > **Aplicaciones** y haga lo siguiente:

   a. Habilite el botón de alternancia **Versión del sistema operativo**.

   b. En la lista emergente de sistemas operativos, seleccione **Android** o **iOS**.

La regla se aplicará a los dispositivos correspondientes. Debe especificar al menos una condición para crear una regla.

9. Haga clic en **Guardar** para crear la regla.

   La regla recién creada se muestra en la página **REGLAS DE MOVIMIENTO**. De acuerdo con la regla, Kaspersky Security Center asignará todos los dispositivos recién conectados al grupo de administración seleccionado.

Para obtener más información sobre la gestión y las acciones de grupos de administración con dispositivos no asignados, siga los siguientes pasos:

- Si utiliza Kaspersky Security Center Web Console, consulte la *Ayuda de Kaspersky Security Center*.
- Si utiliza Kaspersky Security Center Cloud Console, consulte la *Ayuda de Kaspersky Security Center Cloud Console*.

Implementación de complementos de administración

Para administrar dispositivos móviles en Kaspersky Security Center Web Console, se deben instalar los siguientes complementos de administración:

- Complemento de Kaspersky Security for Mobile (Devices)
- Complemento de Kaspersky Security for Mobile (Policies)

> Si utiliza Kaspersky Security Center Cloud Console, no necesita instalar los complementos de administración. Solo necesita crear una cuenta en Kaspersky Security Center Cloud Console. Para obtener más información sobre cómo crear una cuenta, consulte la *Ayuda de Kaspersky Security Center Cloud Console*.

Puede utilizar los siguientes métodos para instalar los complementos de administración:

- Con el Asistente de inicio rápido de Kaspersky Security Center Web Console.

  La primera vez que se conecte, Kaspersky Security Center Web Console le solicita automáticamente que ejecute el Asistente de inicio rápido después de instalar el Servidor de administración. También puede iniciar manualmente el Asistente de inicio rápido en cualquier momento.

  Para obtener más información sobre el Asistente de inicio rápido para Kaspersky Security Center, consulte la *Ayuda de Kaspersky Security Center*.

- Con la lista de paquetes de distribución disponibles en Kaspersky Security Center Web Console.

  La lista de paquetes de distribución disponibles se actualiza automáticamente después de lanzar las nuevas versiones de las aplicaciones Kaspersky.

- Descargue los paquetes de distribución de una fuente externa y agregue complementos de administración a Kaspersky Security Center Web Console.

  Por ejemplo, se pueden descargar los paquetes de distribución de complementos de administración desde el sitio web de Kaspersky.

Instalación de complementos de administración a partir de la lista disponible de paquetes de distribución

Para instalar los complementos de administración, siga los siguientes pasos:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **CONFIGURACIÓN DE LA CONSOLA** > **COMPLEMENTOS WEB**.
2. Haga clic en el botón **Agregar**.

   Se abre la lista de versiones actualizadas de las aplicaciones Kaspersky.
3. Para instalar los complementos de administración, siga los siguientes pasos:
   a. En la lista de aplicaciones disponibles, haga clic en la sección **Dispositivos móviles** para expandirla.
   b. Seleccione **Kaspersky Security for Mobile (Devices)** y, a continuación, haga clic en **Instalar complemento**.
   c. Seleccione **Kaspersky Security for Mobile (Policies)** y, a continuación, haga clic en **Instalar complemento**.

Se descargarán los paquetes de distribución y se instalarán los complementos. Cuando cada complemento se instale y agregue a Kaspersky Security Center Web Console, se mostrará una ventana de confirmación.

Instalando los complementos de administración desde el paquete de distribución

Puede descargar el paquete de distribución del sitio web de Kaspersky.

Para instalar el complemento Kaspersky Security for Mobile (Devices) desde el paquete de distribución, siga los siguientes pasos:

1. Copie los archivos `plugin.zip` y `signature.txt` en el archivo comprimido `on_prem_ksm_devices_xx.x.x.x.zip` del paquete de distribución a la estación de trabajo del administrador.
2. En la ventana principal de Kaspersky Security Center Web Console, seleccione **CONFIGURACIÓN DE LA CONSOLA** > **COMPLEMENTOS WEB**.
3. Haga clic en **Agregar desde archivo**.
4. En la ventana emergente **Agregar desde archivo**, haga clic en **Cargar archivo ZIP** y, a continuación, busque el archivo `plugin.zip`.
5. Haga clic en **Cargar firma** y, a continuación, busque el archivo `signature.txt`.
6. Haga clic en el botón **Agregar**.

Se instalará el complemento de Kaspersky Security for Mobile (Devices) y se agregará a Kaspersky Security Center Web Console.

A fin de instalar el complemento de Kaspersky Security for Mobile (Policies) desde el paquete de distribución, siga los siguientes pasos:

1. Copie los archivos `plugin.zip` y `signature.txt` en el archivo comprimido `on_prem_ksm_policies_xx.x.x.x.zip` del paquete de distribución a la estación de trabajo del administrador.
2. En la ventana principal de Kaspersky Security Center Web Console, seleccione **CONFIGURACIÓN DE LA CONSOLA** > **COMPLEMENTOS WEB**.

3. Haga clic en **Agregar desde archivo**.

4. En la ventana emergente **Agregar desde archivo**, haga clic en **Cargar archivo ZIP** y, a continuación, busque el archivo `plugin.zip`.

5. Haga clic en **Cargar firma** y, a continuación, busque el archivo `signature.txt`.

6. Haga clic en el botón **Agregar**.

   Se instalará el complemento Kaspersky Security for Mobile (Policies) y se agregará a Kaspersky Security Center Web Console.

Para asegurarse de que se hayan instalado los complementos de administración, consulte la lista de complementos instalados en la página **CONFIGURACIÓN DE LA CONSOLA** > **COMPLEMENTOS WEB**.

Implementación de la aplicación móvil

Para administrar los dispositivos móviles en Kaspersky Security Center Web Console o Cloud Console, debe implementar la aplicación Kaspersky Endpoint Security para Android o Kaspersky Security para iOS en los dispositivos móviles. Puede implementar aplicaciones en dispositivos móviles mediante el uso de Kaspersky Security Center Web Console o Cloud Console.

Implementación de la aplicación móvil mediante Kaspersky Security Center Web Console o Cloud Console

La aplicación móvil se implementa en los dispositivos móviles de los usuarios que tienen cuentas de usuario agregadas en Kaspersky Security Center. Para obtener más información sobre las cuentas de usuario en Kaspersky Security Center, haga lo siguiente:

- Si utiliza Kaspersky Security Center Web Console, consulte la *Ayuda de Kaspersky Security Center*.
- Si utiliza Kaspersky Security Center Cloud Console, consulte la *Ayuda de Kaspersky Security Center Cloud Console*.

Puede utilizar el complemento Kaspersky Security for Mobile (Devices) a fin de instalar la aplicación desde Kaspersky Security Center Web Console y Cloud Console mediante el envío de un enlace de instalación a un dispositivo móvil.

- En un dispositivo Android, el usuario recibe un enlace de Google Play para descargar la aplicación Kaspersky Endpoint Security para Android. La aplicación puede instalarse si se sigue el procedimiento de instalación estándar en la plataforma Android. Después de instalar la aplicación, el usuario debe proporcionar los permisos necesarios.

  Algunos dispositivos de Huawei y Honor no poseen servicios de Google y, por lo tanto, no tienen acceso a aplicaciones en Google Play. Si algunos usuarios de dispositivos Huawei y Honor no pueden instalar la aplicación desde Google Play, deberían recibir instrucciones para instalar la aplicación desde Huawei App Gallery.

- En un dispositivo iOS, el usuario recibe un enlace de App Store a fin de descargar la aplicación Kaspersky Security para iOS. La aplicación puede instalarse si se sigue el procedimiento de instalación estándar

en la plataforma iOS.

> Antes de conectar un dispositivo iOS, envíe la dirección de Kaspersky Security Center al usuario del dispositivo para mejorar la seguridad de la conexión. El usuario verá esta dirección durante la instalación de la aplicación y podrá cancelar la conexión si la dirección que se muestra no coincide con la dirección que usted envió.

El vínculo incluye los siguientes datos:

- Configuración de sincronización de Kaspersky Security Center
- Certificado general

Para implementar la aplicación en un dispositivo móvil:

1. Inicie el Asistente para conectar un nuevo dispositivo móvil:
   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS** y, a continuación, haga clic en **Agregar**.
   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **USUARIOS Y FUNCIONES** > **USUARIOS**. Haga clic en el nombre del usuario o grupo de usuarios al que desea enviar el enlace para conectar un dispositivo móvil y, a continuación, seleccione **DISPOSITIVOS.** Haga clic en **Agregar dispositivo móvil**. En este caso, omita el paso 3.

   Para continuar con el asistente, utilice el botón **Siguiente**.
2. Seleccione el sistema operativo de los dispositivos que desea agregar:
   - **Android**
   - **iOS y iPadOS**
3. Seleccione los usuarios o grupos de usuarios a los que desee enviar el enlace para conectar un dispositivo móvil.
4. Seleccione las direcciones de correo electrónico a las que se debe enviar el enlace:
   - **Todas las direcciones de correo electrónico**
   - **Dirección de correo electrónico principal**
   - **Dirección de correo electrónico alternativa**
   - **Otra dirección de correo electrónico**

     Si selecciona esta opción, especifique la dirección de correo electrónico a continuación.
5. Se muestra el resumen del enlace.

   Asegúrese de que todos los parámetros del enlace sean correctos y, a continuación, haga clic en **Enviar**.
6. Se abre una ventana con la confirmación de que se ha enviado el enlace para agregar un dispositivo móvil.

   Haga clic en **Aceptar** para finalizar el Asistente.

Cuando el usuario instala la aplicación Kaspersky Endpoint Security para Android o Kaspersky Security para iOS, el dispositivo del usuario se muestra en la pestaña **DISPOSITIVOS** > **MÓVIL** > **DISPOSITIVOS** de Web Console o Cloud Console. Luego de instalar la aplicación en los dispositivos móviles de los usuarios, podrá configurar los parámetros para los dispositivos y aplicaciones mediante directivas de grupo. También podrá enviar comandos a dispositivos móviles (solo para Android) para la protección de datos en caso de robo o pérdida de los dispositivos.

Activación de la aplicación móvil

En Kaspersky Security Center, la licencia puede cubrir varios grupos de funciones. Para asegurarse de que la aplicación Kaspersky Endpoint Security para Android o Kaspersky Security para iOS sean totalmente funcionales, la licencia de Kaspersky Security Center adquirida por la organización debe garantizar la funcionalidad de la **Administración de dispositivos móviles**. El objetivo de la funcionalidad **Administración de dispositivos móviles** es conectar dispositivos móviles con Kaspersky Security Center y administrarlos.

Para obtener información detallada sobre la obtención de licencias de Kaspersky Security Center y las opciones de licencia, haga lo siguiente*:*

- Si utiliza Kaspersky Security Center Web Console, consulte la *Ayuda de Kaspersky Security Center*.
- Si utiliza Kaspersky Security Center Cloud Console, consulte la *Ayuda de Kaspersky Security Center Cloud Console*.

La activación de las aplicaciones Kaspersky Endpoint Security para Android o Kaspersky Security para iOS en un dispositivo móvil se realiza proporcionando información de licencia válida a la aplicación. La información de la licencia se envía al dispositivo móvil junto con 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 el 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 deberá sincronizar manualmente el dispositivo y 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. Abra la ventana Propiedades de la directiva:
   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.
2. En la página Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Licencias**.
3. 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 de verificación **Si la clave del dispositivo es diferente, reemplácela con esta clave**.

4. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Proporcionar los permisos necesarios para la aplicación Kaspersky Endpoint Security para Android

Ciertas funciones de la aplicación Kaspersky Endpoint Security para Android requieren permisos. Kaspersky Endpoint Security para Android solicita permisos obligatorios durante la instalación, así como después de la instalación y antes de utilizar funciones individuales de la aplicación. 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 versiones posteriores, 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 la aplicación Kaspersky Endpoint Security para Android

Permiso	Función de la aplicación
Teléfono (requerido solo para Android 5.0 a 9.X)	Conexión con Kaspersky Security Center (ID del dispositivo)
Almacenamiento (obligatorio)	Antivirus
Acceso para administrar todos los archivos	Antivirus (solo para Android 11 o versiones posteriores)
Dispositivos Bluetooth cercanos (para Android 12 o posterior)	Restricción del uso de Bluetooth
Administrador del dispositivo (obligatorio)	Antirrobo: bloqueo del dispositivo (solo para Android 5.0 a 6.X)
	Antirrobo: tomar una foto de identificación con la cámara frontal

	Aunque la toma de fotos de identificación no es compatible con Kaspersky Security Center Web Console y Cloud Console, la aplicación Kaspersky Endpoint Security para Android requiere este permiso para que todas las consolas de Kaspersky Security Center puedan administrarla.
	Antirrobo: hacer sonar la alarma
	Antirrobo: reinicio completo
	Protección con contraseña
	Protección de eliminación de aplicaciones
	Instalación de certificado de seguridad
	Control de apps
	Restricción del uso de la cámara, Bluetooth y Wi-Fi
Cámara	Antirrobo: tomar una foto de identificación con la cámara frontal Aunque la toma de fotos de identificación no es compatible con Kaspersky Security Center Web Console y Cloud Console, la aplicación Kaspersky Endpoint Security para Android requiere este permiso para que todas las consolas de Kaspersky Security Center puedan administrarla. En los dispositivos con Android 11.0 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 10.0 o posterior, el usuario debe conceder el permiso "Todo el tiempo" cuando se solicite.
Accesibilidad	Antirrobo: bloqueo del dispositivo (solo para Android 7.0 y versiones posteriores)
	Protección web
	Control de apps
	Protección de eliminación de aplicaciones (solo para Android 7.0 y versiones posteriores)
	Visualización de advertencias de Kaspersky Endpoint Security para Android (solo para Android 10.0 o versiones posteriores)
	Restringir el uso de la cámara (solo para Android 11 o posterior)

Administración de certificados

Los certificados móviles se utilizan con el fin de identificar a los usuarios de los dispositivos móviles en el Servidor de administración.

Kaspersky Security Center Web Console y Cloud Console permiten realizar las siguientes acciones con los certificados móviles de usuario:

- Vea los certificados y sus estados.
- Cree nuevos certificados.
- Renueve los certificados que caduquen.
- Elimine los certificados.

Para obtener más información sobre los certificados de Kaspersky Security Center, haga lo siguiente:

- Si utiliza Kaspersky Security Center Web Console, consulte la *Ayuda de Kaspersky Security Center*.
- Si utiliza Kaspersky Security Center Cloud Console, consulte la *Ayuda de Kaspersky Security Center Cloud Console*.

Visualización de la lista de certificados

Kaspersky Security Center Web Console y Cloud Console permiten ver los certificados móviles de usuario aplicados, sus estados y propiedades.

Para ver la lista de certificados móviles de usuario aplicados, haga lo siguiente:

1. En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVIL** > **DISPOSITIVOS**.
2. Seleccione **Administrar certificados**.

Se abre la página **Certificados móviles** con información sobre los certificados móviles de usuario aplicados. Para ver los detalles de un certificado, haga clic en este en la columna **Nombre de usuario**.

Definición de la configuración de certificados

Puede utilizar Kaspersky Security Center Web Console o Cloud Console para configurar la vigencia, las actualizaciones automáticas y la protección con contraseña de los certificados móviles.

Para definir la configuración del certificado móvil, siga los siguientes pasos:

1. En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVIL** > **DISPOSITIVOS**.
2. Seleccione **Administrar certificados**.
3. Seleccione **Configuración de certificados**.
4. En la ventana emergente **Generar certificados móviles**, puede configurar lo siguiente:
   - **Período de validez de la contraseña (días)**

     Período de validez 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.

- **Reemitir el certificado cuando esté por caducar en (días)**

  Cantidad de días que quedan hasta que caduque el certificado actual durante la cual 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 1.

- **Reemitir el certificado automáticamente, si es posible**

  Si es posible, los certificados se volverán a emitir automáticamente. Si esta opción está deshabilitada, los certificados se deben volver a emitir manualmente a medida que caducan. Esta opción está deshabilitada de forma predeterminada.

- **Solicitar contraseña durante la instalación del certificado**

  Se le pedirá al usuario una contraseña cuando se instale el certificado 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**.

5. Haga clic en **Guardar** para aplicar los cambios y cerrar la ventana.

Kaspersky Security Center utilizará la configuración especificada para crear, actualizar y proteger los certificados móviles.

Creación de un certificado

Puede crear certificados móviles en Kaspersky Security Center Web Console y Cloud Console con el fin de identificar a los usuarios de los dispositivos móviles.

Para crear un certificado móvil, siga los siguientes pasos:

1. En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVIL** > **DISPOSITIVOS**.

2. Seleccione **Administrar certificados**.

3. En la emergente **Certificados móviles**, haga clic en **Agregar** para iniciar el **Asistente de creación de certificado móvil**. Para continuar con el asistente, utilice el botón **Siguiente**.

4. Seleccione los usuarios o grupos de usuarios cuyos dispositivos móviles desee administrar con un nuevo certificado.

5. Especifique los **Parámetros de publicación**:

   - Si desea notificar a los usuarios sobre el nuevo certificado, seleccione la casilla de verificación **Notificar al usuario acerca del certificado nuevo**.

   - Si desea permitir el uso de un certificado varias veces en el mismo dispositivo, seleccione la casilla de verificación **Permitir el uso de un certificado en varias ocasiones dentro del mismo dispositivo (solo para dispositivos con Kaspersky Endpoint Security para Android instalado)**.

6. Seleccione el **Tipo de autenticación**:

   - Seleccione **Credenciales (nombre de usuario o inicio de sesión en el dominio)** si desea que los usuarios accedan al certificado mediante sus credenciales.

- Seleccione **Contraseña de un solo uso** si desea que los usuarios accedan al certificado mediante el uso de una contraseña de un solo uso.

  Esta opción está disponible si no seleccionó la casilla de verificación **Permitir el uso de un certificado en varias ocasiones dentro del mismo dispositivo (solo para dispositivos con Kaspersky Endpoint Security para Android instalado)** en el paso anterior.

- Seleccione **Contraseña** si desea que los usuarios accedan al certificado mediante el uso de una contraseña.

  Esta opción está disponible si seleccionó la casilla de verificación **Permitir el uso de un certificado en varias ocasiones dentro del mismo dispositivo (solo para dispositivos con Kaspersky Endpoint Security para Android instalado)** en el paso anterior.

7. Especifique el método de envío del certificado en el campo **Envío del certificado**:

   - Si seleccionó **Contraseña de un solo uso** en el paso anterior, seleccione una de las siguientes opciones:

     - Si desea enviar la contraseña por correo electrónico, seleccione **Notificar al usuario por correo electrónico**.

       A continuación, seleccione qué dirección de correo electrónico usar o seleccione **Otra dirección de correo electrónico** para especificar otra.

     - Si desea notificar a los usuarios sobre la contraseña por otros medios, seleccione **Mostrar el certificado luego de finalizar el Asistente**.

   - Si seleccionó **Credenciales (nombre de usuario o inicio de sesión en el dominio)** en el paso anterior, seleccione qué dirección de correo electrónico usar o seleccione **Otra dirección de correo electrónico** para especificar otra.

8. Se mostrará el resumen del certificado.

   Asegúrese de que todos los parámetros sean correctos y, a continuación, haga clic en **Crear**.

Al hacerlo, el **Asistente de creación de certificado móvil** genera un certificado que los usuarios pueden instalar en los dispositivos móviles. El certificado estará disponible después de la próxima sincronización de dispositivos móviles con Kaspersky Security Center.

Para obtener más información sobre la creación de certificados y la configuración de reglas para su emisión, siga los siguientes pasos:

- Si utiliza Kaspersky Security Center Web Console, consulte la *Ayuda de Kaspersky Security Center*.
- Si utiliza Kaspersky Security Center Cloud Console, consulte la *Ayuda de Kaspersky Security Center Cloud Console*.

Renovación de un certificado

Si alguno de los certificados móviles aplicados está a punto de caducar, puede renovarlo mediante el uso de Kaspersky Security Center Web Console o Cloud Console.

Para renovar un certificado móvil, haga lo siguiente:

1. En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVIL** > **DISPOSITIVOS**.

2. Seleccione **Administrar certificados**.

3. Seleccione el certificado que desea renovar y, a continuación, haga clic en **Reemitir**.

   El estado del certificado cambia a **El certificado se reemitió**.

Eliminación de un certificado

Puede eliminar certificados móviles mediante el uso de Kaspersky Security Center Web Console o Cloud Console.

Si elimina un certificado móvil, el dispositivo ya no podrá sincronizarse con el Servidor de administración y no podrá administrarse mediante Kaspersky Security Center. Para comenzar a administrar el dispositivo móvil nuevamente, deberá reinstalar la aplicación Kaspersky Endpoint Security para Android en este.

Para eliminar un certificado móvil, haga lo siguiente:

1. En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVIL** > **DISPOSITIVOS**.
2. Seleccione **Administrar certificados**.
3. Seleccione el certificado que desea eliminar y, a continuación, haga clic en **Eliminar**.

   El certificado se elimina y se quita de la lista de certificados.

Intercambio de información con Firebase Cloud Messaging

Kaspersky Endpoint Security para Android usa el servicio Firebase Cloud Messaging (FCM) para asegurar la entrega oportuna de los comandos a los dispositivos móviles y la sincronización forzada cuando se cambia la configuración de la directiva.

Para usar el servicio Firebase Cloud Messaging, debe configurar el servicio en Kaspersky Security Center Web Console o Cloud Console.

Para habilitar Firebase Cloud Messaging en Kaspersky Security Center Web Console o Cloud Console, haga lo siguiente:

1. En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **SINCRONIZACIÓN DE DISPOSITIVOS ANDROID**.

   Se abrirá la ventana **Sincronización de dispositivos Android**.
2. En los campos **Id. del remitente** y **Clave del servidor**, especifique la configuración de Firebase Cloud Messaging: SENDER_ID y Clave de la API.

   Firebase Cloud Messaging está habilitado.

Para obtener un ID del remitente y la Clave del servidor, haga lo siguiente:

1. Regístrese en el Portal de Google.
2. Vaya a Google Cloud Platform.
3. Cree un nuevo proyecto.

Espere a que se cree el proyecto.

4. Busque el SENDER_ID relevante del proyecto.

5. Habilite Google Firebase Cloud Messaging para Android.

6. Siga las instrucciones en pantalla para crear credenciales.

7. Recupere la Clave de la API de las propiedades de las credenciales recién creadas.

Para obtener información detallada sobre las operaciones en Google Cloud Platform, consulte su documentación.

Ya tiene un **Id. del remitente** y una **Clave del servidor** para ajustar la configuración de Firebase Cloud Messaging.

Si no se configura Firebase Cloud Messaging, los comandos en el dispositivo móvil y la configuración de las directivas se enviarán cuando el dispositivo se sincronice con Kaspersky Security Center según el cronograma establecido en la directiva (por ejemplo, cada 24 horas). En otras palabras, los comandos y la configuración de las directivas se enviarán con un retraso.

Con el fin de contribuir al funcionamiento principal del producto, se compromete a proporcionar automáticamente al servicio Firebase Cloud Messaging el ID único de la instalación de la aplicación (ID del caso), y los siguientes datos:

- Información sobre el software instalado: versión de la aplicación, ID de la aplicación, versión de la aplicación, nombre del paquete de la aplicación.
- Información sobre el equipo en el cual el software se instala: versión del SO, ID del dispositivo, versión de los servicios de Google.
- Información sobre FCM: ID de la aplicación en FCM, ID del usuario de FCM, versión del protocolo.

Los datos se transmiten a los servicios Firebase mediante una conexión segura. El acceso y la protección de la información se rigen conforme a las condiciones de uso pertinentes de los servicios de Firebase: Términos de seguridad y procesamiento de datos de Firebase, Privacidad y seguridad en Firebase.

Para evitar el intercambio de información con el servicio de Firebase Cloud Messaging:

1. En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **SINCRONIZACIÓN DE DISPOSITIVOS ANDROID**.

   Se abrirá la ventana **Sincronización de dispositivos Android**.

2. Haga clic en **Restablecer**.

3. En la ventana que se abre, haga clic en el botón **Aceptar** para confirmar el restablecimiento.

Se borra la configuración de Firebase Cloud Messaging.

Administración de dispositivos móviles en Kaspersky Security Center Web Console y Cloud Console

Puede administrar los dispositivos móviles en Kaspersky Security Center Web Console y Cloud Console mediante el uso de las directivas de grupo y el envío comandos a dispositivos móviles (solo para Android).

Para administrar dispositivos móviles en Kaspersky Security Center Web Console, debe instalar los complementos de administración.

Conexión de dispositivos móviles a Kaspersky Security Center

Para administrar un dispositivo móvil con Kaspersky Security Center Web Console o Cloud Console, el dispositivo debe estar conectado a Kaspersky Security Center. Puede ver la lista de dispositivos móviles conectados a Kaspersky Security Center en la pestaña **DISPOSITIVOS** > **MÓVIL** > **DISPOSITIVOS** de Web Console o Cloud Console.

Antes de conectar un dispositivo iOS, envíe la dirección de Kaspersky Security Center al usuario del dispositivo para mejorar la seguridad de la conexión. El usuario verá esta dirección durante la instalación de la aplicación y podrá cancelar la conexión si la dirección que se muestra no coincide con la dirección que usted envió.

Para conectar un dispositivo móvil a Kaspersky Security Center, siga los siguientes pasos:

1. Inicie el Asistente para conectar un nuevo dispositivo móvil:

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS** y, a continuación, haga clic en **Agregar**.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **USUARIOS Y FUNCIONES** > **USUARIOS**. Haga clic en el nombre del usuario o grupo de usuarios al que desea enviar el enlace para conectar un dispositivo móvil y, a continuación, seleccione **DISPOSITIVOS.** Haga clic en **Agregar dispositivo móvil**. En este caso, omita el paso 3.

   Para continuar con el asistente, utilice el botón **Siguiente**.

2. Seleccione el sistema operativo de los dispositivos que desea agregar:

   - **Android**

   - **iOS y iPadOS**

3. Seleccione los usuarios o grupos de usuarios a los que desee enviar el enlace para conectar un dispositivo móvil.

4. Seleccione las direcciones de correo electrónico a las que se debe enviar el enlace:

   - **Todas las direcciones de correo electrónico**

   - **Dirección de correo electrónico principal**

   - **Dirección de correo electrónico alternativa**

   - **Otra dirección de correo electrónico**

     Si selecciona esta opción, especifique la dirección de correo electrónico a continuación.

5. Se muestra el resumen del enlace.

   Asegúrese de que todos los parámetros del enlace sean correctos y, a continuación, haga clic en **Enviar**.

6. Se abre una ventana con la confirmación de que se ha enviado el enlace para agregar un dispositivo móvil.

   Haga clic en **Aceptar** para finalizar el Asistente.

Cuando el usuario instala la aplicación Kaspersky Endpoint Security para Android o Kaspersky Security para iOS, el dispositivo del usuario se mostrará en la pestaña **DISPOSITIVOS** > **MÓVIL** > **DISPOSITIVOS** de Web Console o Cloud Console.

Movimiento de dispositivos móviles no asignados a grupos de administración

Cuando las aplicaciones Kaspersky Endpoint Security para Android o Kaspersky Security para iOS están instaladas en los dispositivos móviles, se muestran en la página **DESCUBRIMIENTO E IMPLEMENTACIÓN** > **DISPOSITIVOS NO ASIGNADOS** de Kaspersky Security Center Web Console o Cloud Console. 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 Security Center Web Console o Cloud Console, seleccione **DESCUBRIMIENTO E IMPLEMENTACIÓN** > **DISPOSITIVOS NO ASIGNADOS**.

2. Seleccione el dispositivo que desee mover a un grupo de administración y, a continuación, haga clic en **Mover al grupo**.

3. En el árbol emergente de grupos de administración, seleccione el grupo objetivo al que desee mover el dispositivo.

   Puede crear un grupo de administración nuevo mediante la selección de un grupo existente y, a continuación, haciendo 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 de grupo.

Envío de comandos a dispositivos móviles

Puede enviar los comandos a los dispositivos móviles Android para proteger los datos de un dispositivo móvil perdido o robado, o para realizar una sincronización forzada de un dispositivo móvil con Kaspersky Security Center.

No puede enviar comandos a dispositivos iOS.

Los siguientes comandos están admitidos:

- **Bloquear dispositivo**

  El dispositivo móvil se bloquea.

- **Desbloquear dispositivo**

El dispositivo móvil se desbloquea. Después de desbloquear un dispositivo móvil con Android 5.0 a 6.X, la contraseña de desbloqueo de pantalla (el código PIN) se restablece en "1234". Después de desbloquear un dispositivo con Android 7.0 o posterior, la contraseña de desbloqueo de pantalla no se cambia.

- **Restablecer ajustes de fábrica**

  Se eliminan todos los datos del dispositivo móvil y se restablecen los valores predeterminados.

- **Eliminar datos corporativos**

  Los datos en contenedores y la cuenta de correo electrónico corporativa se borran del dispositivo móvil.

- **Localizar dispositivo**

  Se localiza el dispositivo y se muestra su ubicación en Google Maps. El proveedor de servicios móviles puede cobrar una tarifa por el acceso a Internet.

  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 no más de 30 minutos antes. De lo contrario, el comando **Localizar dispositivo** falla.

- **Activar alarma**

  El dispositivo móvil suena como una alarma. La alarma suena durante 5 minutos (o durante 1 minuto si la carga de la batería del dispositivo es baja).

- **Sincronizar dispositivo**

  El dispositivo móvil se sincroniza con Kaspersky Security Center.

La aplicación Kaspersky Endpoint Security para Android requiere permisos específicos para ejecutar los comandos. 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. Si este es el caso, será imposible ejecutar comandos.

En dispositivos con Android 10.0 o posterior, el usuario debe otorgar el permiso "Todo el tiempo" para la acceder a la ubicación. En dispositivos con Android 11.0 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 enviar un comando a un dispositivo móvil, siga los siguientes pasos:

1. En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**.
2. Seleccione el dispositivo al que desee enviar el comando y, a continuación, haga clic en **Control** o **Administrar**.
3. Seleccione el comando requerido en la lista **Comandos disponibles** y, a continuación, haga clic en **Aceptar**.
4. Haga clic en **Aceptar** si se le pide que confirme la operación.

El comando especificado se enviará al dispositivo móvil y se mostrará la ventana de confirmación.

Eliminación de dispositivos móviles de Kaspersky Security Center

Si ya no necesita administrar un dispositivo móvil, puede eliminarlo de Kaspersky Security Center con Web Console o Cloud Console.

Para eliminar un dispositivo móvil de Kaspersky Security Center, siga los siguientes pasos:

1. Elimine la aplicación móvil del dispositivo o asegúrese de que el usuario haya eliminado la aplicación del dispositivo requerido.
2. En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**.
3. Seleccione el dispositivo móvil que desee eliminar y, a continuación, haga clic en **Eliminar**.
4. Haga clic en **Aceptar** para confirmar la operación.

El dispositivo se eliminará de Kaspersky Security Center.

Administración de directivas de grupo

En esta sección se describe cómo administrar directivas de grupo en Kaspersky Security Center Web Console y Cloud Console.

Directivas de grupo para administrar dispositivos móviles

Una *directiva de grupo* es un paquete de configuración para administrar dispositivos móviles que pertenecen a un grupo de administración y para administrar las aplicaciones móviles instaladas en los dispositivos.

Puede usar una directiva para cambiar la configuración tanto de dispositivos individuales como de un grupo de dispositivos. Para un grupo de dispositivos, las opciones de administración pueden configurarse en la ventana de propiedades de la directiva de grupo.

Cada parámetro representado en una directiva tiene un atributo de bloqueo, que muestra si la opción se puede modificar en las directivas de los niveles jerárquicos anidados (para los grupos anidados y los Servidores de administración secundarios), en la configuración de la aplicación local.

Los valores de las opciones configurados en la directiva y en la configuración de la aplicación local 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. Si el usuario ha especificado otros valores de opciones de configuración que no han sido bloqueadas, durante la siguiente sincronización del dispositivo con el Servidor de administración, los nuevos valores de las opciones de configuración se transmiten al Servidor de administración y se guardan en la configuración local de la aplicación en lugar de los valores que el administrador había especificado previamente.

Para mantener actualizada la seguridad corporativa de los dispositivos móviles Android, puede supervisar los dispositivos de los usuarios a fin de verificar su cumplimiento con los requisitos de seguridad corporativa.

Para obtener más información sobre la administración de directivas y grupos de administración en Kaspersky Security Center Web Console y Cloud Console, siga los siguientes pasos:

- Si utiliza Kaspersky Security Center Web Console, consulte la *Ayuda de Kaspersky Security Center*.
- Si utiliza Kaspersky Security Center Cloud Console, consulte la *Ayuda de Kaspersky Security Center Cloud Console*.

Visualización de la lista de directivas de grupo

Kaspersky Security Center Web Console y Cloud Console le permiten ver las directivas de grupo, sus estados y propiedades.

Para ver la lista de directivas de grupo, siga los siguientes pasos,

En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**.

Se abrirá la lista de directivas de grupo con una breve información sobre estas. En esta página, puede crear, modificar, copiar, mover y eliminar las directivas de grupo.

Visualización de los resultados de la distribución de directivas

Kaspersky Security Center Web Console y Cloud Console le permiten ver el gráfico de distribución de una directiva de grupo y la información sobre todos los dispositivos que se incluyen en esa directiva.

Para ver los resultados de distribución de una directiva de grupo, siga los siguientes pasos:

1. En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**.
2. En la lista emergente de directivas de grupo, seleccione la casilla de verificación junto al nombre de la directiva para la que desee ver los resultados de distribución y, a continuación, haga clic en **Distribución**.

   Se abrirá la página de resultados de distribución de las directivas. Esta página contiene el resumen de la directiva, su gráfico de distribución y la tabla con información sobre todos los dispositivos que se incluyen en dicha directiva. Puede abrir la ventana de propiedades de la directiva si hace clic en el botón **Configurar directiva**.

Creación de directivas de grupo

Kaspersky Security Center Web Console y Cloud Console le permiten crear directivas de grupo con el fin de administrar dispositivos móviles.

Para crear una directiva de grupo, siga los siguientes pasos:

1. En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**.
2. En la lista emergente de directivas de grupo de Kaspersky Security Center, haga clic en **Ruta actual** para seleccionar el grupo de administración para el que desee crear una directiva.

   De forma predeterminada, la nueva directiva de grupo se aplicará al grupo de **dispositivos administrados**.

3. Haga clic en **Agregar** para iniciar el Asistente de creación de directivas. Para continuar con el asistente, utilice el botón **Siguiente**.

4. Seleccione una aplicación en función de la plataforma:

   - **Kaspersky Endpoint Security para Android**
   - **Kaspersky Security para iOS**

5. Escriba el nombre de la nueva directiva en el campo **Nombre**. Si especifica el nombre de una directiva existente, se le añadirá un (1) al final de manera automática.

6. Seleccione el estado de la directiva:

   - **Activa**

     El asistente guarda la directiva creada en el Servidor de administración. En la siguiente sincronización del dispositivo móvil con el Servidor de administración, la directiva se usará como directiva activa en el dispositivo.

   - **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.

7. Puede habilitar o deshabilitar dos opciones de herencia, **Heredar la configuración de la directiva principal** y **Forzar la herencia de la configuración en las directivas secundarias**:

   - Si habilita **Heredar la configuración de la directiva principal** para un grupo de administración secundario y bloquea algunas configuraciones en la directiva principal, no podrá cambiar esta configuración en la directiva del grupo secundario. Sin embargo, puede cambiar la configuración que no está bloqueada en la directiva principal.

   - Si deshabilita **Heredar la configuración de la directiva principal** para un grupo de administración secundario, podrá cambiar todas las configuraciones del grupo secundario, incluso si algunas están bloqueadas en la directiva principal.

   - Si habilita **Forzar la herencia de la configuración en las directivas secundarias** en el grupo de administración principal, esto activa la opción **Heredar la configuración de la directiva principal** 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.

   - En las directivas para el grupo de **Dispositivos administrados**, la opción **Heredar la configuración de la directiva principal** no afecta ninguna configuración, porque el grupo de **Dispositivos administrados** no tiene ningún grupo que precede y, por lo tanto, no hereda ninguna directiva.

   De forma predeterminada, la opción **Heredar la configuración de la directiva principal** está habilitada y la opción **Forzar la herencia de la configuración en las directivas secundarias** está deshabilitada.

8. Si lo desea, puede definir la configuración de la directiva que creó recientemente. Para hacerlo, seleccione la pestaña **CONFIGURACIÓN DE LA APLICACIÓN** y, a continuación, proceda como se describe en la sección "Definición de la configuración de directivas".

Si no, puede hacerlo más tarde.

9. Haga clic en **Guardar** para crear la directiva.

Se creará una nueva directiva de grupo para administrar dispositivos móviles.

Modificación de una directiva de grupo

Kaspersky Security Center Web Console y Cloud Console le permiten modificar la configuración de las directivas de grupo.

Para modificar una directiva de grupo, siga los siguientes pasos:

1. Abra la ventana Propiedades de la directiva:

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la ventana de propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** y, a continuación, defina la configuración de la directiva como se describe en la sección "Definición de la configuración de directivas".

   Además, puede definir la configuración general, la herencia de la configuración, las notificaciones y el registro de eventos y los perfiles de la directiva, y ver el historial de revisión. Para obtener más información, consulte la *Ayuda de Kaspersky Security Center*.

3. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Copia de una directiva de grupo

Kaspersky Security Center Web Console y Cloud Console le permiten crear una copia de una directiva de grupo.

Para crear una copia de una directiva de grupo, siga los siguientes pasos:

1. En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**.

2. En la lista emergente de directivas de grupo, seleccione la casilla de verificación junto al nombre de la directiva para la que desee crear una copia y, a continuación, haga clic en **Copiar**.

3. En el árbol emergente de grupos de administración, seleccione el grupo objetivo en el que desee crear una copia de la directiva.

   Puede crear un grupo de administración nuevo mediante la selección de un grupo existente y, a continuación, haciendo 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 índice (<next sequence number>) al nombre de la directiva que se creó o movió recientemente, por ejemplo: (1).

Movimiento de una directiva a otro grupo de administración

Kaspersky Security Center Web Console y Cloud Console le permiten 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 Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**.

2. En la lista emergente de directivas de grupo, seleccione la casilla de verificación 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.

   Puede crear un grupo de administración nuevo mediante la selección de un grupo existente y, a continuación, haciendo 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 esta 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 índice (<next sequence number>) al nombre de la directiva que se creó o movió recientemente, por ejemplo: (1).

Eliminación de una directiva de grupo

Kaspersky Security Center Web Console y Cloud Console le permiten eliminar directivas de grupo.

Puede eliminar solo una directiva que no se herede 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 de grupo, siga los siguientes pasos:

1. En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**.
2. En la lista emergente de directivas de grupo, seleccione la casilla de verificación junto al nombre de la directiva que desee eliminar y, a continuación, haga clic en **Eliminar**.
3. Haga clic en **Aceptar** para confirmar la operación.

Se eliminará la directiva de grupo.

Definición de la configuración de directivas

En esta sección, se describe cómo establecer la configuración de las directivas de Kaspersky Security Center para administrar dispositivos móviles.

Puede definir la configuración de una directiva al crearla o modificarla.

Configuración de la protección antivirus

Puede definir estos parámetros de directivas solo para dispositivos Android.

Para la detección oportuna de amenazas, virus y otras aplicaciones maliciosas, debe configurar la protección en tiempo real y la ejecución automática de análisis antivirus.

Kaspersky Endpoint Security para Android detecta los siguientes tipos de objetos:

- Virus, gusanos informáticos, troyanos y herramientas maliciosas
- Adware
- Aplicaciones que pueden utilizar delincuentes para dañar su dispositivo o sus datos personales

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 aplicación omite archivos grandes y no envía notificaciones sobre dichas omisiones.

Configuración de la protección en tiempo real

Puede definir estos parámetros de directivas solo para dispositivos Android.

Para configurar protección en tiempo real:

1. Abra la ventana Propiedades de la directiva:

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la ventana Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Protección esencial**.

3. En la sección **Antivirus**, configure las opciones de protección del sistema de archivos del dispositivo móvil:

   - Para habilitar la protección en tiempo real del dispositivo móvil frente a amenazas, active la casilla **Activar la protección antivirus en tiempo real**.

   - Especifique el nivel de protección:

     - Si desea que Kaspersky Endpoint Security para Android analice solo las aplicaciones y archivos nuevos en la carpeta Descargas, seleccione **Analizar solo las aplicaciones nuevas**.

     - Para habilitar la protección extendida del dispositivo móvil frente a amenazas, seleccione **Analizar todas las aplicaciones y supervisar las acciones con archivos**.

       Kaspersky Endpoint Security para Android analizará todos los archivos que el usuario abra, modifique, mueva, copie, inicie o guarde en el dispositivo, así como las aplicaciones móviles recién instaladas.

       En dispositivos Android con ejecución 8.0 o posterior, Kaspersky Endpoint Security para Android analiza archivos que el usuario modifica, mueve, instala y guarda, y realiza una copia de todos los archivos. Kaspersky Endpoint Security para Android no analiza archivos cuando se abren o archivos de origen cuando se copian.

   - Para habilitar el análisis adicional de las nuevas aplicaciones antes de su primer uso en el dispositivo del usuario con el servicio en nube de Kaspersky Security Network, seleccione la casilla **Protección adicional de Kaspersky Security Network**.

   - Para bloquear adware y aplicaciones que pueden usar delincuentes para dañar el dispositivo o los datos del usuario, seleccione la casilla de verificación **Detectar software publicitario, marcadores automáticos y apps que los ciberdelincuentes pueden usar para causar daños al dispositivo y los datos del usuario**.

4. En la sección **Configuración del Antivirus**, seleccione la acción que se realizará al detectar una amenaza:

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

Los objetos detectados se eliminarán automáticamente. El usuario no deberá realizar ninguna acción avanzada. Antes de eliminar un objeto, Kaspersky Endpoint Security para Android creará una copia de seguridad del archivo y la guardará en Cuarentena.

- **Eliminar**

  Los objetos detectados se eliminarán automáticamente. El usuario no deberá realizar ninguna acción avanzada. Antes de eliminar un objeto, Kaspersky Endpoint Security para Android mostrará una notificación temporal para indicar la detección del objeto.

- **Omitir**

  Si las amenazas se han omitido, Kaspersky Endpoint Security para Android le advertirá al usuario sobre problemas en la protección del dispositivo. La información sobre amenazas omitidas se muestra en la sección **Estado** de la aplicación. Para cada amenaza omitida, la aplicación proporciona acciones que el usuario puede realizar para eliminar la amenaza. La lista de amenazas omitidas puede cambiar, por ejemplo, si un archivo sospechoso se eliminara o se moviera. Para recibir una lista actualizada de amenazas, ejecute un análisis completo del dispositivo. Para garantizar la protección confiable de sus datos, elimine todas las amenazas detectadas.

5. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Configuración de la ejecución automática de análisis antivirus en el dispositivo móvil

Puede definir estos parámetros de directivas solo para dispositivos Android.

Para configurar una ejecución automática de análisis antivirus en un dispositivo móvil, haga lo siguiente:

1. Abra la ventana Propiedades de la directiva:

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la ventana Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Protección esencial**.

3. Para bloquear adware y aplicaciones que pueden usar delincuentes para dañar el dispositivo o los datos del usuario, seleccione la casilla de verificación **Detectar software publicitario, marcadores automáticos y apps que los ciberdelincuentes pueden usar para causar daños al dispositivo y los datos del usuario** en la sección **Análisis del dispositivo**.

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

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

  Los objetos detectados se eliminarán automáticamente. El usuario no deberá realizar ninguna acción avanzada. Antes de eliminar un objeto, Kaspersky Endpoint Security para Android creará una copia de seguridad del archivo y la guardará en Cuarentena.

- **Eliminar**

  Los objetos detectados se eliminarán automáticamente. El usuario no deberá realizar ninguna acción avanzada. Antes de eliminar un objeto, Kaspersky Endpoint Security para Android mostrará una notificación temporal para indicar la detección del objeto.

- **Omitir**

  Si las amenazas se han omitido, Kaspersky Endpoint Security para Android le advertirá al usuario sobre problemas en la protección del dispositivo. La información sobre amenazas omitidas se muestra en la sección **Estado** de la aplicación. Para cada amenaza omitida, la aplicación proporciona acciones que el usuario puede realizar para eliminar la amenaza. La lista de amenazas omitidas puede cambiar, por ejemplo, si un archivo sospechoso se eliminara o se moviera. Para recibir una lista actualizada de amenazas, ejecute un análisis completo del dispositivo. Para garantizar la protección confiable de sus datos, elimine todas las amenazas detectadas.

- **Preguntar al usuario**

  La aplicación Kaspersky Endpoint Security para Android muestra una notificación que le solicita al usuario que elija la acción que se debe realizar con el objeto detectado: **Omitir** o **Eliminar**.

  Cuando la aplicación detecta varias amenazas, la opción **Preguntar al usuario** permite que el usuario del dispositivo aplique una acción seleccionada a cada archivo usando la casilla **Aplicar a todas las amenazas**.

  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 10.0 o posterior. Kaspersky Endpoint Security para Android solicita al usuario que configure la aplicación 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.

5. En la sección **Análisis programado**, puede configurar el análisis completo y automático del sistema de archivos del dispositivo.

   Seleccione una de las siguientes opciones:

- **Deshabilitado**

  El análisis del sistema de archivos del dispositivo no se iniciará automáticamente.

- **Tras la actualización de las bases de datos**

  El sistema de archivos del dispositivo se analizará automáticamente en cada actualización de las bases de datos antivirus.

- **A diario**

  El sistema de archivos del dispositivo se analizará automáticamente todos los días.

  Si selecciona esta opción, también puede especificar la hora del análisis en el campo **Hora de inicio**.

- **Semanalmente los**

  El sistema de archivos del dispositivo se analizará automáticamente una vez por semana.

  Si elige esta opción, también puede seleccionar el día de la semana en el que desee ejecutar el análisis, a través de la lista desplegable y la hora del análisis en el campo **Hora de inicio**.

En Android 12 o una versión posterior, la aplicación puede realizar esta tarea más tarde de lo especificado si el dispositivo está en modo de ahorro de batería.

6. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Configuración de las actualizaciones de las bases de datos antivirus

Puede definir estos parámetros de directivas solo para dispositivos Android.

Para configurar las actualizaciones de las bases de datos antivirus, haga lo siguiente:

1. Abra la ventana Propiedades de la directiva:

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la ventana Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Actualización de bases de datos**.

3. En la sección **Actualización de bases de datos**, configure la planificación de las actualizaciones automáticas de las bases de datos en el dispositivo del usuario.

   Seleccione una de las siguientes opciones:

   - **Deshabilitado**

     Se deshabilitarán las actualizaciones automáticas de las bases de datos antivirus.

   - **A diario**

     Las bases de datos antivirus se actualizarán todos los días.

     Si selecciona esta opción, también puede especificar la hora en el campo **Horario de actualización**.

   - **Semanal**

     Las bases de datos antivirus se actualizarán una vez por semana.

Si selecciona esta opción, también puede especificar la hora en el campo **Horario de actualización** y el día de la semana en el que desee ejecutar la actualización en la lista desplegable **Día de la semana**.

En Android 12 o una versión posterior, la aplicación puede realizar esta tarea más tarde de lo especificado si el dispositivo está en modo de ahorro de batería.

4. En la sección **Origen de actualizaciones de las bases de datos**, especifique el origen de las actualizaciones desde donde Kaspersky Endpoint Security para Android recibe e instala las actualizaciones de las bases de datos antivirus:

   - **Servidores de Kaspersky**

     Kaspersky Endpoint Security para Android utilizará un servidor de actualización de Kaspersky como origen de la actualización a fin de descargar las bases de datos antivirus en el dispositivo del usuario.

   - **Servidor de administración**

     Disponible solo si usa Kaspersky Security Center Web Console.

     Kaspersky Endpoint Security para Android utilizará el repositorio del Servidor de administración de Kaspersky Security Center como origen de la actualización a fin de descargar las bases de datos antivirus en el dispositivo del usuario.

   - **Otro origen**

     Kaspersky Endpoint Security para Android utilizará un servidor de terceros como origen de la actualización a fin de descargar las bases de datos antivirus en el dispositivo del usuario.

     Si selecciona esta opción, debe especificar la dirección de un servidor HTTP en el campo **Usar otro servidor como origen de la actualización para las bases de datos antivirus**.

5. Si desea que Kaspersky Endpoint Security para Android descargue actualizaciones de las bases de datos antivirus según el programa de actualización cuando el dispositivo del usuario está en roaming, seleccione la casilla **Permitir actualización de las bases de datos en itinerancia**, en la sección **Actualizar las bases de datos antivirus en itinerancia**.

6. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Definición de la configuración de desbloqueo del dispositivo

Puede definir estos parámetros de directivas solo para dispositivos Android.

Para mantener un dispositivo móvil seguro, se debe configurar una contraseña que se le solicita al usuario cuando el dispositivo sale del modo de reposo.

Puede imponer restricciones a la actividad del usuario en el dispositivo si la contraseña de desbloqueo es débil (por ejemplo, bloqueo del dispositivo). Puede aplicar restricciones con el componente Control de cumplimiento.

En ciertos dispositivos Samsung con Android 7.0 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.

Para configurar la seguridad de la contraseña de desbloqueo del dispositivo, haga lo siguiente:

1. Abra la ventana Propiedades de la directiva:

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la ventana Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Protección esencial**.

3. Si desea que la aplicación compruebe si se estableció una contraseña de desbloqueo, seleccione la casilla **Exigir que se defina una contraseña de desbloqueo de pantalla**, en la sección **Protección con contraseña**.

   Si la aplicación detecta que no se ha establecido 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.

4. Especifique la cantidad mínima de caracteres que tendrá la contraseña del usuario.

   Valores posibles: entre 4 y 16 caracteres.

   De forma predeterminada, la contraseña del usuario tiene una longitud de cuatro caracteres.

   En dispositivos con Android 10.0 o posterior, Kaspersky Endpoint Security establece los requerimientos de seguridad de la contraseña en uno de los sistemas de valores: media o alta.

   Los valores para dispositivos con Android 10.0 o posterior se determinan en base a las siguientes reglas:

   - 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 (por ejemplo, 1234), o alfanumérica. El PIN o contraseña debe tener al menos 4 caracteres de extensión.

   - 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 numérica (PIN) con una secuencia que no tenga números repetidos u ordenados, o alfanumérica (contraseña). La extensión del PIN debe ser de al menos 8 dígitos; la contraseña debe contar con al menos 6 caracteres.

5. Si desea que el usuario pueda usar las huellas digitales para desbloquear la pantalla, seleccione la casilla **Permitir el uso de huellas digitales (para dispositivos que ejecutan Android 9 o anterior)**. Si la contraseña de desbloqueo no cumple con los requisitos de seguridad corporativa, no se puede usar un escáner de huellas digitales para desbloquear la pantalla.

   En dispositivos con Android 10.0 o una versión posterior, no se admite usar una huella digital para desbloquear la pantalla.

Kaspersky Endpoint Security para Android no restringe el uso de un escáner de huellas digitales para iniciar sesión en aplicaciones o confirmar compras.

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

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.

Después de agregar una huella digital en la configuración del dispositivo, el usuario puede desbloquear la pantalla usando los siguientes métodos:

- Presionar el dedo en el escáner de huellas digitales (método principal).
- Escribir la contraseña de desbloqueo (método secundario).

6. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Configuración de la protección de datos de dispositivos robados o perdidos

Puede definir estos parámetros de directivas solo para dispositivos Android.

Para proteger los datos corporativos en caso del robo o pérdida de un dispositivo móvil, debe configurar la protección para el acceso no autorizado.

A fin de garantizar la protección de los datos del dispositivo robado o perdido, se debe configurar Kaspersky Endpoint Security para Android como una función de Accesibilidad. Kaspersky Endpoint Security para Android solicita al usuario que configure la aplicación 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.

Para configurar la protección de datos de dispositivos robados o perdidos, haga lo siguiente:

1. Abra la ventana Propiedades de la directiva:
   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva

que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la ventana Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Protección esencial**.

3. En la sección **Antirrobo**, configure el bloqueo del dispositivo:

   - Especifique la cantidad de caracteres del código de desbloqueo.

   - Detalle el texto que se mostrará cuando el dispositivo esté bloqueado.

4. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Configuración del Control de apps

Puede definir estos parámetros de directivas solo para dispositivos Android.

Control de apps comprueba que las aplicaciones instaladas en un dispositivo móvil cumplan con los requisitos de seguridad corporativa. En Kaspersky Security Center, el administrador crea listas de apps permitidas, bloqueadas, obligatorias y recomendadas según los requisitos de seguridad corporativa. Como resultado de Control de apps, Kaspersky Endpoint Security le solicita al usuario instalar aplicaciones obligatorias y recomendadas, y eliminar aplicaciones bloqueadas. Es imposible iniciar aplicaciones bloqueadas en el dispositivo móvil del usuario.

En Web Console y Cloud Console de Kaspersky Security Center, puede administrar aplicaciones en los dispositivos de los usuarios mediante reglas predefinidas. Puede configurar dos tipos de reglas de **Control de aplicaciones**: reglas de implementación y reglas de categoría.

Una **Regla de la aplicación** se aplica a una aplicación específica, mientras que una **Regla de categoría** se aplica a cualquier aplicación que pertenezca a una categoría predefinida. Los expertos de Kaspersky son quienes especifican las categorías de aplicaciones.

*Para configurar **Control de aplicaciones**, haga lo siguiente:*

1. Abra la ventana Propiedades de la directiva:

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la página Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Controles de seguridad**.

3. En la tabla, en la sección **Control de aplicaciones**, agregue las reglas que definirán qué aplicaciones se controlarán.

   - Para agregar una regla para una aplicación específica, haga lo siguiente:

     a. En la tabla, haga clic en **Regla de la aplicación**.

     b. En la ventana emergente **Regla de la aplicación**, elija la acción que se realizará con las aplicaciones a las que se aplica la regla creada.

     c. Especifique la aplicación sujeta a la regla. Para ello, complete los campos **Enlace al paquete de instalación (por ejemplo, https://play.google.com/store/apps/details?id=com.kaspersky.kes)**, **Nombre del paquete (por ejemplo, katana.facebook.com)** y **Nombre de la aplicación**.

     d. Haga clic en **Guardar**.

     La regla se agregará a la lista de reglas de **Control de aplicaciones**.

   - Para agregar una regla para una categoría de aplicaciones, haga lo siguiente:

     a. En la tabla, en la sección **Control de aplicaciones**, haga clic en **Regla de categoría**.

     b. En la ventana emergente **Regla de categoría**, seleccione la categoría de la aplicación en la lista desplegable.

     Las aplicaciones de la categoría seleccionada estarán sujetas a la regla que se creó.

     c. En la sección **Modo de operación**, seleccione la acción que se realizará cuando cualquier aplicación de la categoría seleccionada intente iniciarse: **Aplicaciones bloqueadas** o **Aplicaciones permitidas**.

     d. Si es necesario, complete **Comentario adicional que se muestra en el dispositivo del usuario cuando se detecta una aplicación de una categoría específica**.

     e. Haga clic en **Guardar**.

     La regla se agregará a la lista de reglas de **Control de aplicaciones**.

4. En la sección **Acciones con aplicaciones bloqueadas**, elija qué acción se realizará para las aplicaciones bloqueadas:

   - Si desea que Kaspersky Endpoint Security para Android bloquee el inicio de aplicaciones bloqueadas en el dispositivo móvil del usuario, seleccione **Bloquear el lanzamiento de aplicaciones**.

   - Si desea que Kaspersky Endpoint Security para Android envíe datos sobre aplicaciones bloqueadas al registro de eventos sin bloquearlas, seleccione la casilla **No bloquear las aplicaciones bloqueadas, solo informar**.

5. En la sección **Modo de operación**, elija si las reglas que agregue definirán aplicaciones permitidas o bloqueadas:

   - Si desea que las reglas definan qué aplicaciones están permitidas, seleccione **Aplicaciones bloqueadas**.

     Si desea que Kaspersky Endpoint Security para Android bloquee el inicio de apps del sistema en el dispositivo móvil del usuario (como Calendario, Cámara y Configuración) en el modo **Aplicaciones bloqueadas**, seleccione la casilla **Bloquear apps del sistema**.

     Los expertos de Kaspersky recomiendan no usar aplicaciones de sistema de bloqueo porque esto podría causar fallos en el funcionamiento del dispositivo.

- Si desea que las reglas definan qué aplicaciones están bloqueadas, seleccione **Aplicaciones permitidas**.

6. Para recibir información sobre todas las aplicaciones instaladas en los dispositivos móviles, en la sección **Informe de aplicaciones**, active la casilla **Enviar una lista de apps instaladas en todos los dispositivos móviles**.

   Kaspersky Endpoint Security para Android envía datos al registro de eventos cada vez que se instala o elimina una aplicación del dispositivo.

7. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Configuración del control de cumplimiento de dispositivos móviles con requisitos de seguridad corporativa

Puede definir estos parámetros de directivas solo para dispositivos Android.

El control de cumplimiento le permite supervisar los dispositivos Android para verificar que cumplan con los requisitos de seguridad corporativa y tomar medidas en caso de incumplimiento. Los requisitos de seguridad corporativa regulan cómo el usuario puede operar con el dispositivo. Por ejemplo, la protección en tiempo real se debe habilitar en el dispositivo, las bases de datos antivirus se deben actualizar y la contraseña del dispositivo debe ser suficientemente segura. El control de cumplimiento se basa en una lista de reglas. Una regla de cumplimiento incluye los siguientes componentes:

- Criterio para dispositivo en incumplimiento.
- La acción que se tomará en un dispositivo si el usuario no soluciona el incumplimiento dentro del período establecido.
- Período asignado para que el usuario solucione instancias de incumplimiento (por ejemplo, 24 horas).

  Cuando finaliza el período especificado, se realizará la acción seleccionada en el dispositivo del usuario.

  En Android 12 o una versión posterior, la aplicación puede realizar esta tarea más tarde de lo especificado si el dispositivo está en modo de ahorro de batería.

Para configurar el control de cumplimiento, puede realizar las siguientes acciones:

- Habilitar o deshabilitar las reglas de cumplimiento existentes.
- Editar una regla de cumplimiento existente.
- Agregar una nueva regla.
- Eliminar una regla.

Habilitación y deshabilitación de las reglas de cumplimiento

Puede definir estos parámetros de directivas solo para dispositivos Android.

Para habilitar o deshabilitar las reglas existentes del control de cumplimiento para dispositivos móviles con requisitos de seguridad corporativa, haga lo siguiente:

1. Abra la ventana Propiedades de la directiva:

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la página Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Controles de seguridad**.

3. En la sección **Control de cumplimiento**, habilite o deshabilite las reglas de cumplimiento existentes mediante los botones de alternancia de la columna **Estado**.

4. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Edición de reglas de cumplimiento

Puede definir estos parámetros de directivas solo para dispositivos Android.

Para editar una regla a fin de controlar que los dispositivos móviles cumplan con los requisitos de seguridad corporativa, haga lo siguiente:

1. Abra la ventana Propiedades de la directiva:

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la página Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Controles de seguridad**.

3. En la sección **Control de cumplimiento**, seleccione la regla que desee editar y, luego, haga clic en **Editar**.

4. En la ventana emergente **Regla**, edite la regla de la siguiente manera:

   a. En la columna **Acción**, configure la lista de acciones que se realizarán en caso de incumplimiento de la regla. Para ello, agregue nuevas acciones, edite las acciones existentes o elimínelas.

   b. También puede especificar el período en el que un usuario puede corregir el incumplimiento en la columna **Tiempo hasta la rectificación** para cada acción.

   c. Haga clic en el botón **Guardar** para guardar la regla.

5. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Adición de reglas de cumplimiento

Puede definir estos parámetros de directivas solo para dispositivos Android.

Para agregar una regla a fin de controlar que los dispositivos móviles cumplan con los requisitos de seguridad corporativa, haga lo siguiente:

1. Abra la ventana Propiedades de la directiva:

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la página Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Controles de seguridad**.

3. En la sección **Control de cumplimiento**, haga clic en **Regla**.

4. En la ventana emergente **Regla**, defina la regla de la siguiente manera:

   a. Seleccione el criterio de incumplimiento para la regla.

   b. Haga clic en **Agregar** y, luego, seleccione la acción que se realizará en caso de incumplimiento para la regla en la columna **Acción**.

   Puede agregar varias acciones.

c. Especifique el período en el que un usuario puede corregir el incumplimiento en la columna **Tiempo hasta la rectificación** para cada acción.

d. Haga clic en el botón **Guardar** para guardar la regla.

5. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Eliminación de reglas de cumplimiento

Puede definir estos parámetros de directivas solo para dispositivos Android.

Para eliminar una regla a fin de controlar que los dispositivos móviles cumplan con los requisitos de seguridad corporativa, haga lo siguiente:

1. Abra la ventana Propiedades de la directiva:

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la página Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Controles de seguridad**.

3. En la sección **Control de cumplimiento**, seleccione la regla que desee eliminar y, luego, haga clic en **Eliminar**.

4. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Lista de criterios de incumplimiento

Puede definir estos parámetros de directivas solo para dispositivos Android.

Para asegurarse de que un dispositivo Android cumpla con los requisitos de seguridad corporativa, Kaspersky Endpoint Security para Android puede verificar los siguientes criterios en el dispositivo:

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

  Debe habilitarla.

  Para obtener más información sobre la configuración de la protección en tiempo real, consulte la sección Configuración de la protección en tiempo real.

- **Las bases de datos antivirus están desactualizadas**.

  Las bases de datos antivirus de Kaspersky Endpoint Security para Android deben actualizarse con regularidad.

  Para obtener más información sobre cómo definir la configuración de las actualizaciones de las bases de datos antivirus, consulte la sección Configuración de la protección antivirus.

- **Se instalaron aplicaciones bloqueadas**.

  El dispositivo no debe tener aplicaciones instaladas que estén clasificadas como **Bloquear el lanzamiento**, como se especifica en la sección **Control de aplicaciones**.

  Para obtener más información sobre la creación de reglas para aplicaciones, consulte la sección Configuración del Control de apps.

- **Se instalaron aplicaciones de categorías bloqueadas**.

  El dispositivo no debe tener aplicaciones instaladas que tengan una categoría clasificada como **Bloquear el lanzamiento**, como se especifica en la sección **Control de aplicaciones**.

  Para obtener más información sobre la creación de reglas para categorías de aplicaciones, consulte la sección Configuración del Control de apps.

- **No se instalaron todas las aplicaciones necesarias**.

  El dispositivo debe tener aplicaciones específicas instaladas que estén clasificadas como **Forzar instalación**, como se especifica en la sección **Control de aplicaciones**.

  Para obtener más información sobre la creación de reglas para aplicaciones, consulte la sección Configuración del Control de apps.

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

  El dispositivo debe contar con una versión del sistema operativo permitida.

  Para aplicar este criterio de incumplimiento, debe especificar el rango de versiones del sistema operativo permitidas en las listas desplegables **Versión mínima del sistema operativo** y **Versión máxima del sistema operativo**.

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

  Debe sincronizarse con el Servidor de administración periódicamente.

  Para aplicar este criterio de incumplimiento, debe especificar el intervalo de tiempo máximo entre sincronizaciones de dispositivos en la lista desplegable **Período de sincronización**.

- **El dispositivo ha sido rooteado**.

  El dispositivo no debe liberarse.

  Para obtener más información, consulte la sección Detección de ataques de hackers en el dispositivo (root).

- **La contraseña de desbloqueo no cumple con los requisitos de seguridad**.

  El dispositivo debe estar protegido con una contraseña de desbloqueo que cumpla con sus requisitos de seguridad.

Lista de acciones en caso de incumplimiento

Puede definir estos parámetros de directivas solo para dispositivos Android.

Si el usuario no soluciona un problema de incumplimiento durante el período especificado, las siguientes opciones están disponibles:

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

  Se bloquea el inicio de todas las aplicaciones del dispositivo móvil del usuario, excepto las aplicaciones del sistema.

- **Bloquear dispositivo**.

  El dispositivo móvil se bloquea. Para obtener acceso a los datos, debe desbloquear el dispositivo. Si no se rectifica el motivo de bloqueo del dispositivo después de que se desbloquea, el dispositivo se bloqueará de nuevo después del período especificado.

- **Eliminar datos corporativos**.

  Elimine los datos en contenedores, la cuenta de correo electrónico corporativa, la configuración para conectarse a la red Wi-Fi y VPN corporativas, y el nombre del punto de acceso (APN).

- **Restablecer la configuración de fábrica del dispositivo**.

  Todos los datos se eliminan del dispositivo móvil y la configuración se restablece a sus valores de fábrica.

Configuración de acceso de usuarios a sitios web

Puede definir estos parámetros de directivas para dispositivos Android y iOS.

Para proteger los datos personales y corporativos almacenados en dispositivos móviles durante la navegación por Internet, puede configurar el acceso de los usuarios a sitios web a través de Protección web. Protección web analiza los sitios web antes de que un usuario los abra y bloquea los que distribuyen códigos maliciosos y los sitios web de phishing diseñados para robar datos confidenciales y obtener acceso a cuentas financieras.

Para dispositivos Android, esta función también permite filtrar sitios web por categorías definidas en el servicio en la nube de Kaspersky Security Network. El filtrado permite restringir el acceso a determinados sitios web o categorías de sitios web (por ejemplo, los de las categorías "**Juegos de azar, loterías, sorteos**" o "**Comunicación por Internet**").

En dispositivos Android, Protección web en dispositivos Android solo funciona en el navegador Google Chrome, el navegador de Huawei y el navegador de Samsung.

Para garantizar que Protección web funcione correctamente, Kaspersky Endpoint Security para Android debe configurarse como una función de Accesibilidad. Kaspersky Endpoint Security para Android solicita al usuario que configure la aplicación 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 dispositivos iOS, el usuario debe permitir que la aplicación Kaspersky Security para iOS añada una configuración de VPN para que Protección web funcione.

Para configurar el acceso de usuarios a sitios web, haga lo siguiente:

1. Abra la ventana Propiedades de la directiva:

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la página Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Controles de seguridad**.

3. En la sección **Protección web**, active la casilla **Habilitar protección web**.

4. Para dispositivos Android, puede seleccionar una de las siguientes opciones:

   - Para restringir el acceso de usuarios a sitios web según el contenido, haga lo siguiente:

     a. Seleccione **Bloquear sitios web de categorías especificadas**.

     b. Seleccione las casillas junto a las categorías de sitios web para las que Kaspersky Endpoint Security para Android bloqueará el acceso.

     > Si la Protección web está activada, el acceso del usuario a los sitios web de las categorías **Phishing** y **Sitios de malware** siempre está bloqueado.

   - Para especificar la lista de sitios web permitidos, haga lo siguiente:

     a. Seleccione **Permitir solo los sitios web especificados**.

     b. Cree una lista de sitios web agregando direcciones de sitios web para los que la aplicación no bloqueará el acceso. Kaspersky Endpoint Security para Android solo admite expresiones regulares. Al escribir la dirección de un sitio web permitido, utilice las siguientes plantillas:

        - `http:\/\/www\.example\.com.*`: Todas las páginas secundarias del sitio web están permitidas (por ejemplo, `http://www.example.com/about`).

        - `https:\/\/.*example\.com`—Todas las páginas del subdominio del sitio web están permitidas (por ejemplo, `https://pictures.example.com`).

     c. También puede usar la expresión `https?` para seleccionar HTTP y HTTPS. Para obtener más información sobre las expresiones regulares, consulte el sitio web de soporte técnico de Oracle.

   - Para bloquear el acceso de los usuarios a todos los sitios web, seleccione **Bloquear todos los sitios web**.

5. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Configuración de restricciones para las funciones

Puede definir estos parámetros de directivas solo para dispositivos Android.

Web Console de Kaspersky Security Center le permite configurar el acceso de los usuarios a las siguientes funciones de los dispositivos móviles:

- Wi-Fi
- Cámara
- Bluetooth

De forma predeterminada, el usuario puede usar el Wi-Fi, la cámara y el Bluetooth en el dispositivo sin restricciones.

Para configurar las restricciones de utilización de Wi-Fi, de la cámara y de Bluetooth en el dispositivo:

1. Abra la ventana Propiedades de la directiva:
   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.
   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.
2. En la página Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Controles de seguridad**.
3. En la sección **Administración de funciones**, configure el uso de Wi-Fi, de la cámara y de Bluetooth:
   - Para deshabilitar el módulo Wi-Fi en el dispositivo móvil del usuario, active la casilla **Prohibir el uso de Wi-Fi**.

     En dispositivos con Android 10.0 o una versión posterior, no se admite prohibir el uso de redes Wi-Fi.

   - Para deshabilitar la cámara en el dispositivo móvil del usuario, active la casilla **Prohibir el uso de la cámara**.

     En dispositivos con Android 10.0 o una versión posterior, el uso de la cámara no se puede prohibir completamente.

     En los dispositivos con Android 11 o posterior, Kaspersky Endpoint Security para Android debe estar configurado como una función de accesibilidad. Kaspersky Endpoint Security para Android solicita al usuario que configure la aplicación 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. Si este es el caso, no podrá restringir el uso de la cámara.

- Para deshabilitar el Bluetooth en el dispositivo móvil del usuario, active la casilla **Prohibir el uso de Bluetooth**.

  En Android 12 o versiones posteriores, el uso de Bluetooth puede deshabilitarse solo si el usuario del dispositivo otorgó el permiso **Dispositivos Bluetooth cercanos**. El usuario puede otorgar este permiso durante el Asistente de configuración inicial o posteriormente.

4. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Protección de Kaspersky Endpoint Security para Android contra eliminación

Para protección del dispositivo móvil y cumplimiento de 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 al usuario deshabilitar los derechos de administrador para Kaspersky Endpoint Security para Android. Después de deshabilitar los derechos, el dispositivo móvil se bloqueará.

Para habilitar la protección contra la eliminación de Kaspersky Endpoint Security para Android, haga lo siguiente:

1. Abra la ventana Propiedades de la directiva:

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la página Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Controles de seguridad**.

3. En la sección **Administrar la app en el dispositivo móvil**, desactive la casilla **Permitir la eliminación de Kaspersky Endpoint Security para Android del dispositivo**.

   Para proteger la aplicación contra la eliminación en dispositivos con Android 7.0 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. Si hace esto, la aplicación no estará protegida contra la eliminación.

4. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Si se hace un intento de eliminar la aplicación, el dispositivo móvil se bloqueará.

Configuración de la sincronización de dispositivos móviles con Kaspersky Security Center

Puede definir estos parámetros de directivas para dispositivos Android y iOS.

Para administrar dispositivos móviles y recibir informes o estadísticas desde dispositivos móviles, deberá definir la configuración de sincronización. La sincronización de los dispositivos móviles con Kaspersky Security Center se puede realizar de las siguientes formas:

- **Por programación**. La sincronización por programación se realiza mediante HTTP. Puede configurar la programación de sincronización en Propiedades de la directiva. Las modificaciones en la configuración de la directiva, los comandos y las tareas se realizan cuando los dispositivos móviles se sincronizan con Kaspersky Security Center según la programación, es decir con un retraso. De forma predeterminada, los dispositivos móviles se sincronizan automáticamente con Kaspersky Security Center cada seis horas.

  En Android 12 o una versión posterior, la aplicación puede realizar esta tarea más tarde de lo especificado si el dispositivo está en modo de ahorro de batería.

- **Forzada** (para dispositivos Android). La sincronización forzada se realiza mediante notificaciones push del servicio de FCM (Firebase Cloud Messaging). La sincronización forzada se realiza principalmente para enviar comandos a un dispositivo móvil en tiempo y forma. Si desea usar la sincronización forzada, asegúrese de que los ajustes de FCM estén configurados en Kaspersky Security Center.

Para configurar la sincronización de dispositivos móviles con Kaspersky Security Center, haga lo siguiente:

1. Abra la ventana Propiedades de la directiva:

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la página Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Sincronización**.

3. En la sección **Iniciar sincronización con el Servidor de administración**, utilice la lista desplegable **Período de sincronización** para seleccionar el que desee.

   De forma predeterminada, la sincronización se realiza cada seis horas.

4. Para dispositivos Android, puede desactivar la sincronización cuando el dispositivo está en roaming. Para ello, seleccione la casilla **No sincronizar en itinerancia**.

   De forma predeterminada, la sincronización en roaming está habilitada.

5. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Kaspersky Security Network

Para proteger dispositivos móviles con mayor eficacia, Kaspersky Endpoint Security para Android y Kaspersky Security para iOS utilizan datos recopilados 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 en línea 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 recopilar información en tiempo real acerca de los tipos y las fuentes de las nuevas amenazas, a desarrollar métodos para neutralizar esas amenazas y a reducir el número de falsas alarmas. Participar en Kaspersky Security Network también le permite acceder a estadísticas de reputación de aplicaciones y sitios web.

Cuando participa en Kaspersky Security Network, se obtienen ciertas estadísticas mientras la aplicación móvil está en ejecución, y estas se envían de manera automática 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.

Los siguientes componentes de la aplicación utilizan el servicio en la nube de Kaspersky Security Network:

- Los componentes Antivirus, Protección web y Control de apps en la aplicación Kaspersky Endpoint Security para Android.
- El componente Protección web en la aplicación Kaspersky Security para iOS.

Para comenzar a utilizar KSN, debe aceptar los términos y condiciones del Contrato de licencia del usuario final. Para obtener más información acerca del envío de datos a KSN, consulte Intercambio de información con Kaspersky Security Network.

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 mejorar el rendimiento de la aplicación móvil, también puede proporcionar datos estadísticos a Kaspersky Security Network.

El envío de información a Kaspersky Security Network es voluntario.

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 el funcionamiento de los siguientes componentes:

- **Antivirus.** La aplicación obtiene acceso a la base de conocimientos de Kaspersky para consultar por la reputación de los archivos y aplicaciones. El análisis se realiza para amenazas cuya información aún no se ha añadido a las bases de datos antivirus, pero que ya está disponible en KSN. El servicio en la nube de Kaspersky Security Network permite el funcionamiento completo del antivirus y reduce la posibilidad de falsas alarmas.

- **Protección 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 aplicaciones 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 Antivirus y Control de apps 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.

Para obtener más información acerca de la provisión de datos a KSN, consulte 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 Security para iOS

Para mejorar la protección en tiempo real, Kaspersky Security 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.

Para obtener más información acerca de la provisión de datos a KSN, consulte Provisión de datos en Kaspersky Security 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

Para intercambiar datos con KSN con el propósito de mejorar el rendimiento de la aplicación, se deben cumplir las condiciones siguientes:

- El usuario del dispositivo debe leer y aceptar los términos de la Declaración de Kaspersky Security Network.

- 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 uso de la aplicación móvil.

Habilitación y deshabilitación de Kaspersky Security Network

De forma predeterminada, el uso de Kaspersky Security Network está habilitado.

Si el uso de Kaspersky Security Network está deshabilitado, Protección web, Control de apps y otros servicios de protección adicional en Kaspersky Security Network se desactivan de forma automática y sus configuraciones dejarán de estar disponibles.

Para habilitar o deshabilitar el uso de Kaspersky Security Network:

1. Abra la ventana Propiedades de la directiva:

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la página Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **KSN y Estadísticas**.

3. Para habilitar o deshabilitar el uso de Kaspersky Security Network, active o desactive la casilla **Usar Kaspersky Security Network**.

4. Si el uso de Kaspersky Security Network está habilitado y acepta enviar datos a Kaspersky, seleccione la casilla **Permitir el envío de estadísticas a Kaspersky Security Network**. Estos datos ayudarán a que la aplicación móvil responda a amenazas con mayor rapidez, mejore el rendimiento de los componentes de protección y disminuya la probabilidad de falsas alarmas.

5. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Intercambio de información con Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics

Puede definir estos parámetros de directivas solo para dispositivos Android.

Kaspersky Endpoint Security para Android intercambia datos con los servicios de Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics con el fin de mejorar la calidad, la apariencia y el rendimiento del software, los productos, los servicios y la infraestructura de Kaspersky mediante el análisis de la experiencia de los usuarios, las funciones, el estado y la configuración del dispositivo utilizado.

El intercambio de información con los servicios de Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics está deshabilitado de manera predeterminada.

Para habilitar el intercambio de datos:

1. Abra la ventana Propiedades de la directiva:

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la página Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **KSN y Estadísticas**.

3. En la sección **Envío de estadísticas**, seleccione la casilla **Permita la transferencia de datos para ayudar a mejorar la calidad, la apariencia y el rendimiento de la aplicación**.

4. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Configuración de notificaciones en dispositivos móviles

Puede definir estos parámetros de directivas solo para dispositivos Android.

Si no desea que el usuario del dispositivo móvil se distraiga con las notificaciones de Kaspersky Endpoint Security para Android, puede deshabilitar ciertas notificaciones.

Kaspersky Endpoint Security utiliza las siguientes herramientas para mostrar el estado de protección del dispositivo:

- **Notificación del estado de protección**. Esta notificación está anclada a la barra de notificaciones. La notificación del estado de protección no se puede eliminar. La notificación muestra el estado de protección del dispositivo (por ejemplo,) y el número de problemas, si los hubiera. El usuario del dispositivo puede presionar el estado de protección del dispositivo y ver la lista de problemas en la aplicación.

- **Notificaciones de la app**. Estas notificaciones informan al usuario del dispositivo sobre la aplicación (por ejemplo, detección de amenazas).

- **Mensajes emergentes**. Los mensajes emergentes requieren una acción del usuario del dispositivo (por ejemplo, una acción para realizar cuando se detecta una amenaza).

Todas las notificaciones de Kaspersky Endpoint Security para Android están activadas de forma predeterminada.

Un usuario del dispositivo Android puede desactivar todas las notificaciones de Kaspersky Endpoint Security para Android en la configuración de la barra de notificaciones. Si las notificaciones están desactivadas, el usuario no podrá controlar el funcionamiento la aplicación y se perderá de 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 en un dispositivo móvil, haga lo siguiente:

1. Abra la ventana Propiedades de la directiva:

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la página Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Notificaciones e informes**.

3. En la sección **Notificaciones**, configure la visualización de las notificaciones:

   - Para ocultar todas las notificaciones y los mensajes emergentes, desactive el botón **Mostrar 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. La aplicación también muestra notificaciones mientras el usuario trabaja con la aplicación (por ejemplo, el usuario actualiza las bases de datos antivirus manualmente).

     Los expertos de Kaspersky recomiendan habilitar las notificaciones y los mensajes emergentes. Si desactiva 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. Los usuarios de dispositivos móviles pueden conocer el estado de protección del dispositivo únicamente cuando abren la aplicación.

   - En **Lista de problemas de seguridad que se muestra en los dispositivos de los usuarios**, seleccione los problemas de Kaspersky Endpoint Security para Android que desee que se muestren en el dispositivo móvil del usuario.

4. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Detección de ataques de hackers en el dispositivo

Kaspersky Security Center Web Console le permite detectar actos de piratería en el dispositivo (acceso root) en dispositivos Android y liberaciones en dispositivos iOS. Los archivos de sistema están desprotegidos en un dispositivo atacado por hackers y, por lo tanto, pueden ser modificados. Además, las aplicaciones de otras empresas de fuentes desconocidas se podrían instalar en dispositivos atacados. Después de la detección de un intento de ataque de hackers, recomendamos que inmediatamente restaure el funcionamiento normal del dispositivo.

Kaspersky Endpoint Security para Android utiliza los siguientes servicios para detectar cuando un usuario obtiene privilegios de root:

- *El servicio incorporado de Kaspersky Endpoint Security para Android.* Un servicio de Kaspersky que comprueba si un usuario de dispositivo móvil obtuvo privilegios de root (SDK de Kaspersky Mobile Security).

- *Certificación de SafetyNet.* Un servicio de Google que comprueba la integridad del sistema operativo, analiza el hardware del dispositivo y software e identifica otros problemas de seguridad. Para obtener más información sobre la Certificación de SafetyNet, visite el sitio web del Servicio de soporte técnico de Android.

Kaspersky Security para iOS utiliza el siguiente servicio para detectar una liberación:

- *El servicio incorporado de Kaspersky Security para iOS.* Un servicio de Kaspersky que comprueba si se liberó un dispositivo móvil (Kaspersky Mobile Security SDK).

Si el dispositivo se corta, recibe una notificación. Puede ver las notificaciones de piratería en Web Console de Kaspersky Security Center, en la pestaña **SUPERVISIÓN E INFORMES** > **TABLERO**. 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 aplicar restricciones con el componente Control de cumplimiento. Para ello, cree una regla de cumplimiento con el criterio **El dispositivo ha sido rooteado**.

Definición de la configuración de las licencias

Puede definir estos parámetros de directivas para dispositivos Android y iOS.

Para administrar los dispositivos móviles en Kaspersky Security Center Web Console o Cloud Console, debe activar la aplicación móvil en los dispositivos móviles. La activación de las aplicaciones Kaspersky Endpoint Security para Android o Kaspersky Security para iOS en un dispositivo móvil se realiza proporcionando información de licencia válida a la aplicación. La información de la licencia se envía al dispositivo móvil junto con 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 el 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 deberá sincronizar manualmente el dispositivo y Kaspersky Security Center.

Para definir la configuración de las licencias de una directiva de grupo, siga los siguientes pasos:

1. Abra la ventana Propiedades de la directiva:

- En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **DIRECTIVAS Y PERFILES**. En la lista de directivas de grupo que se abre, haga clic en el nombre de la directiva que desee configurar.

- En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Seleccione el dispositivo móvil al que se aplica la directiva que desee configurar y, luego, la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la página Propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Licencias**.

3. 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 de verificación **Si la clave del dispositivo es diferente, reemplácela con esta clave**.

4. Haga clic en el botón **Guardar** para guardar los cambios hechos en la directiva y abandonar la ventana Propiedades de la directiva.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Configuración de eventos

Puede definir estos parámetros de directivas para dispositivos Android y iOS.

Puede definir la configuración de almacenamiento y notificación de los eventos que ocurren en los dispositivos de sus usuarios y que se envían a Kaspersky Security Center.

Puede configurar eventos solo al modificar una directiva.

Los eventos se distribuyen por nivel de importancia en las siguientes pestañas:

- **Críticos**

  Un evento crítico indica un problema que puede provocar la pérdida de datos, un mal funcionamiento operativo o un error crítico.

- **Falla funcional**

  Una falla funcional indica un problema grave, un error o un mal funcionamiento que ocurrió durante el funcionamiento de la aplicación.

- **Advertencia**

  Una advertencia no es necesariamente grave, pero indica un posible problema futuro.

- **Información**

Un evento informativo notifica sobre la correcta finalización de una operación o un procedimiento, o el correcto funcionamiento de la aplicación.

En cada sección, la lista muestra los tipos de eventos y el plazo predeterminado de almacenamiento de eventos en Kaspersky Security Center (en días).

Desde la lista de eventos, puede hacer lo siguiente:

- Agregar o eliminar un tipo de evento de la lista de tipos de eventos que se envían a Kaspersky Security Center.
- Definir la configuración de almacenamiento y notificación para cada tipo de evento, por ejemplo: cuánto tiempo deben almacenarse los eventos de este tipo en la base de datos del Servidor de administración o si recibirá notificaciones sobre eventos de este tipo por correo electrónico.

Para obtener más detalles sobre la configuración de eventos en Kaspersky Security Center Web Console y Cloud Console:

- Si utiliza Kaspersky Security Center Web Console, consulte la *Ayuda de Kaspersky Security Center*.
- Si utiliza Kaspersky Security Center Cloud Console, consulte la *Ayuda de Kaspersky Security Center Cloud Console*.

Configuración de eventos sobre la instalación, actualización y eliminación de aplicaciones en los dispositivos de los usuarios

Puede definir estos parámetros de directivas para dispositivos Android y iOS.

Si utiliza Kaspersky Security Center Cloud Console, la lista de tipos de eventos que ocurren en los dispositivos de sus usuarios y que se envían a Kaspersky Security Center no incluye la instalación, actualización ni eliminación de aplicaciones en los dispositivos. Esto se debe a que dichos eventos ocurren con frecuencia y pueden reemplazar a otros eventos importantes en la base de datos de Kaspersky Security Center cuando se alcanza el límite de recuento de eventos. También pueden afectar el rendimiento del Servidor de administración o el DBMS, y el ancho de banda de la conexión a Internet con Kaspersky Security Center Cloud Console.

No obstante, si desea almacenar eventos de este tipo y recibir notificaciones sobre ellos, proceda como se describe en esta sección.

Para configurar eventos sobre la instalación, actualización y eliminación de aplicaciones en los dispositivos de los usuarios:

1. En la configuración de una directiva, en la pestaña **CONFIGURACIÓN DE EVENTOS**, agregue el tipo de evento informativo **Se instaló o eliminó la aplicación (lista de aplicaciones instaladas)** a la lista de eventos que se almacenan en la base de datos del Servidor de administración.

   Para obtener más detalles sobre la configuración de eventos, consulte la *Ayuda de Kaspersky Security Center Cloud Console*.

2. Habilite la opción **Enviar una lista de apps instaladas en todos los dispositivos móviles**.

Los eventos sobre la instalación, actualización y eliminación de aplicaciones en los dispositivos de los usuarios se almacenan en la base de datos de Kaspersky Security Center. Usted recibe notificaciones sobre estos eventos.

Carga de red

Esta sección contiene información sobre el volumen de tráfico de red que se intercambia entre dispositivos móviles y Kaspersky Security Center.

Volumen de tráfico

Tarea	Tráfico saliente	Tráfico entrante	Tráfico Total
Uso inicial de la aplicación, MB	0,08	17,76	17,84
Actualización inicial de las bases de datos antivirus (el volumen de tráfico se puede diferenciar debido al tamaño de las bases de datos antivirus), MB	0,04	2,21	2,25
Sincronización del dispositivo móvil con Kaspersky Security Center, MB	0,03	0,02	0,05
Actualización habitual de las bases de datos antivirus (el volumen de tráfico se puede diferenciar debido al tamaño de las bases de datos antivirus), MB	0,08	3,06	3,14
Ejecución de comandos Antirrobo. Localice el dispositivo (el volumen de tráfico se puede diferenciar debido a las especificaciones de la cámara incorporada y la calidad de imágenes), MB	0,09	0,8	0,17
Ejecución de comandos Antirrobo. Foto de identificación, MB	1,0	0,02	1,02
Ejecución de comandos Antirrobo. Bloqueo del dispositivo, MB	0,06	0,05	0,11
Volumen promedio diario, MB	0,22	6,96	7,18

Trabajar en la consola de administración basada en MMC

En esta sección Ayuda, se describe la protección y administración de dispositivos móviles con la Consola de administración basada en MMC de Kaspersky Security Center.

Casos prácticos más importantes

INSTALACIÓN

¿Cómo instalo remotamente Kaspersky Endpoint Security para Android?

¿Cómo puedo bloquear a un usuario para que no elimine Kaspersky Endpoint Security para Android?

¿Cómo activo Kaspersky Endpoint Security para Android?

PROTECCIÓN

¿Cómo bloqueo un dispositivo que se ha perdido o ha sido robado?

¿Cómo me protejo contra amenazas de Internet?

¿Cómo prohíbo el uso de una contraseña vacía?

USO DE SOLUCIONES DE TERCEROS

Android Enterprise (Aplicaciones con el icono de un maletín, Configuración del perfil de trabajo de Android)

VMware AirWatch, MobileIron, IBM Maas360, SOTI MobiControl

CONTROL

¿Cómo bloqueo a un usuario para que no juegue en un dispositivo?

¿Cómo configuro el acceso a sitios web en un dispositivo?

¿Cómo puedo detectar ataques de hackers (root)?

ADMINISTRACIÓN

¿Cómo configuro un buzón de correo en un dispositivo?

¿Cómo conecto un dispositivo móvil a Wi-Fi?

¿Cómo instalo una aplicación corporativa?

Acerca de Kaspersky Security para dispositivos móviles

Kaspersky Security para dispositivos móviles es una solución integrada para proteger y administrar los dispositivos móviles corporativos, así como los dispositivos móviles personales que utilizan los empleados de la empresa con fines corporativos.

Kaspersky Security para dispositivos móviles incluye los componentes siguientes:

- App móvil 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.

- Complemento de administración de Kaspersky Endpoint Security para Android

El complemento de administración Kaspersky Endpoint Security para Android incluye la interfaz para administrar los dispositivos móviles y las aplicaciones móviles instaladas en ellos mediante la Consola de administración de Kaspersky Security Center.

- Complemento de Administración de Kaspersky Device Management para iOS

  El Complemento de Administración Kaspersky Device Management para iOS permite definir los ajustes de configuración para dispositivos conectados a Kaspersky Security Center mediante los protocolos MDM de iOS (en lo sucesivo "dispositivos MDM de iOS") y Exchange ActiveSync (en lo sucesivo "dispositivos EAS"), sin usar la Utilidad de configuración de iPhone ni la Consola de gestión de Exchange.

Los complementos de administración están integrados en el *sistema de administración remota de Kaspersky Security Center*. El administrador puede utilizar una única Consola de administración de Kaspersky Security Center para administrar todos los dispositivos móviles de la red corporativa, así como los equipos cliente y los sistemas virtuales. Los dispositivos móviles pasan a estar administrados tras conectarlos al Servidor de Administración. El administrador puede supervisar de forma remota los dispositivos administrados.

La aplicación móvil Kaspersky Endpoint Security para Android también puede funcionar como parte del *sistema de administración remota de Kaspersky Endpoint Security Cloud*. Para obtener más información sobre cómo trabajar con aplicaciones mediante Kaspersky Endpoint Security Cloud, consulte la *ayuda en línea de Kaspersky Endpoint Security Cloud*.

La aplicación móvil Kaspersky Endpoint Security para Android también puede operar como parte de las soluciones EMM de otras empresas de los participantes de AppConfig Community (Comunidad de AppConfig).

Funciones clave de administración de dispositivos móviles en la Consola de administración basada en MMC

Kaspersky Security para dispositivos móviles presta las siguientes funciones:

- Distribución de mensajes de correo electrónico para conectar dispositivos Android a Kaspersky Security Center mediante enlaces de Google Play.
- Conexión remota de dispositivos móviles a Kaspersky Security Center y otros sistemas de EMM externos (por ejemplo, VMWare AirWatch, MobileIron, IBM Maas360, SOTI MobiControl).
- Configuración remota de la app Kaspersky Endpoint Security para Android, así como configuración remota de servicios, aplicaciones y funciones de dispositivos Android.
- Configuración remota de los dispositivos móviles de acuerdo con los requerimientos de seguridad corporativa.
- Prevención de la fuga de información corporativa almacenada en los dispositivos móviles en caso de pérdida o robo (Antirrobo).
- Control de cumplimiento con los requisitos corporativos de seguridad (Control de cumplimiento).
- Control del uso de Internet en los dispositivos móviles (Protección web).
- Configuración del correo corporativo en dispositivos móviles, incluidas las organizaciones con un servidor de correo de Microsoft Exchange implementado en la empresa (solo para dispositivos iOS y Samsung).
- Configuración de la red corporativa (Wi-Fi, VPN) que permite utilizar la VPN en los dispositivos móviles. La VPN solo se puede configurar en dispositivos iOS y Samsung.

- Configuración del estado del dispositivo móvil a mostrar en Kaspersky Security Center cuando se infringen las reglas de la directiva: Crítico, Advertencia, Sin inconvenientes.
- Configuración de las notificaciones que se muestran al usuario en la aplicación Kaspersky Endpoint Security para Android.
- Configuración de configuraciones en dispositivos compatibles con Samsung KNOX 2.6 o posterior.
- Configuración de ajustes en dispositivos compatibles con perfiles de trabajo de Android.
- Despliegue de la aplicación Kaspersky Endpoint Security para Android a través de la consola Samsung KNOX Mobile Enrollment. Samsung KNOX Mobile Enrollment está diseñado para la instalación por lotes y la configuración inicial de aplicaciones en dispositivos Samsung comprados a proveedores oficiales.
- Se puede realizar una actualización de la aplicación Kaspersky Endpoint Security para Android a la versión especificada mediante las directivas de Kaspersky Security Center.
- Las notificaciones de administrador sobre el estado y los eventos de la aplicación Kaspersky Endpoint Security para Android pueden comunicarse en Kaspersky Security Center o por correo electrónico.
- Control de cambios para la configuración de la directiva (historial de revisiones).

Kaspersky Security para dispositivos móviles incluye los siguientes componentes de protección y administración:

- Antivirus (para dispositivos con Android)
- Antirrobo (para dispositivos con Android)
- Protección web (en dispositivos con Android y iOS)
- Control de apps (en dispositivos Android)
- Control de cumplimiento (en dispositivos con Android)
- Detección de privilegios de root en dispositivos (para dispositivos 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 app Kaspersky Endpoint Security para Android incluye los componentes siguientes:

- **Antivirus**. Permite detectar y neutralizar amenazas en el dispositivo mediante el uso de las bases de datos antivirus de la aplicación y del servicio en la nube de Kaspersky Security Network. Antivirus incluye los siguientes componentes:
  - Protección. Detecta amenazas en archivos abiertos, analiza las nuevas aplicaciones 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 para un archivo o carpeta previamente seleccionados.
  - Actualizar. Actualizar permite descargar nuevas bases de datos antivirus para la aplicación.

- **Antirrobo.** El componente protege 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** para obtener las coordenadas de la ubicación del dispositivo.
  - **Alarma** para hacer que el dispositivo active una alarma sonora.
  - **Foto de identificación** para hacer que el dispositivo tome fotos con la cámara frontal si alguien intenta desbloquearlo.
  - **Eliminar** datos corporativos para proteger información confidencial de la empresa.
- **Protección web.** Este componente bloquea los sitios maliciosos diseñados para propagar un código malicioso. Protección Web también bloquea sitios web falsos (suplantación de identidad) diseñados para robar datos confidenciales del usuario (por ejemplo, contraseñas de servicios bancarios en línea o de 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. Protección web también permite filtrar sitios web por 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, páginas web con las categorías "Juegos de azar, loterías, sorteos" o "Comunicación por Internet").
- **Control de apps.** Este componente le 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 apps permite eliminar aplicaciones bloqueadas que infrinjan 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.

Acerca de Kaspersky Device Management para iOS

Kaspersky Device Management para iOS asegura la protección y el control de dispositivos móviles conectados a Kaspersky Security Center e incluye funciones de administración de dispositivos, tales como:

- **Protección con contraseña**. Esta función le permite establecer requerimientos de complejidad de contraseña para que los usuarios utilicen contraseñas complejas que cumplan con las políticas corporativas de contraseñas.
- **Administración de redes**. Esta función le permite agregar redes VPN y de Wi-Fi aprobadas o bien restringir acceso a otras.
- **Eliminar datos corporativos**. Ante el robo o pérdida del dispositivo, puede enviarle la orden Eliminar datos corporativos, para proteger información confidencial de la empresa.
- **Protección web**. Este componente bloquea los sitios maliciosos diseñados para propagar un código malicioso. Protección Web también bloquea sitios web falsos (suplantación de identidad) diseñados para robar datos confidenciales del usuario (por ejemplo, contraseñas de servicios bancarios en línea o de 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. Protección web también permite filtrar sitios web por 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, páginas web con las categorías "Juegos de azar, loterías, sorteos" o "Comunicación por Internet").

- **Restricciones de aplicaciones.** Este componente le permite controlar el uso de aplicaciones nativas como iTunes, Safari o Game Center en un dispositivo supervisado.

- **Restricciones para las funciones.** 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.

Acerca de un buzón de correo de Exchange

Un *buzón de correo de Exchange* es una aplicación cliente del servicio de Exchange ActiveSync. La app está pensada para ayudar a los usuarios corporativos a trabajar con correo electrónico, calendario, contactos y tareas. Un buzón de correo de Exchange le permite conectar un dispositivo móvil a un servidor de Microsoft Exchange. Para obtener más información sobre el servicio de Exchange ActiveSync, visite el *sitio web del servicio de soporte técnico de Microsoft*.

Para administrar dispositivos móviles mediante el protocolo de Exchange ActiveSync, el Servidor Exchange debe estar instalado en el servidor de Microsoft Exchange. Para obtener más información acerca de cómo instalar un servidor Exchange, consulte la *ayuda de Kaspersky Security Center*. No se requiere ninguna configuración adicional en dispositivos móviles.

Mediante un buzón de correo de Exchange, puede configurar de forma remota los dispositivos EAS usando directivas de grupo y puede enviar el comando de borrado de datos. Los sistemas operativos siguientes admiten el protocolo de Exchange ActiveSync:

- Windows Mobile
- Windows CE
- Windows Phone
- Android
- Bada
- BlackBerry 10
- iOS
- Symbian

El conjunto de ajustes de administración para un dispositivo de Exchange ActiveSync depende del sistema operativo que se ejecuta en el dispositivo móvil. Para obtener más información sobre las funciones de compatibilidad con el protocolo de Exchange ActiveSync para un sistema operativo específico, consulte la documentación del sistema operativo específico.

Instalar el complemento de administración Kaspersky Endpoint Security para Android

El complemento de administración Kaspersky Endpoint Security para Android incluye la interfaz para administrar los dispositivos móviles y las aplicaciones móviles instaladas en ellos mediante la Consola de administración de Kaspersky Security Center. El complemento de administración Kaspersky Endpoint Security para Android se puede utilizar para las siguientes acciones:

- 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.

El complemento de administración Kaspersky Endpoint Security para Android se instala de forma predeterminada al implementar Kaspersky Security Center. El complemento no requiere una instalación individual.

Complemento de administración Kaspersky Device Management para iOS

El complemento de administración Kaspersky Device Management para iOS ofrece una interfaz para administrar los dispositivos móviles conectados a través del servidor de MDM de iOS y el protocolo Exchange ActiveSync mediante la Consola de administración de Kaspersky Security Center. Se puede utilizar el complemento de administración Kaspersky Device Management para iOS para hacer lo siguiente:

- Crear directivas de seguridad de grupo para los dispositivos móviles.
- Configurar de forma remota dispositivos conectados mediante el protocolo Exchange ActiveSync (en lo sucesivo, "dispositivos EAS").
- Configurar de forma remota dispositivos conectados mediante el protocolo MDM de iOS (en lo sucesivo "dispositivos iOS con MDM").
- Reciba informes y estadísticas sobre el funcionamiento de los dispositivos móviles de los usuarios.

Para obtener más información sobre la conexión de los dispositivos móviles a Kaspersky Security Center mediante los protocolos Exchange ActiveSync y MDM para iOS, consulte la *ayuda de Kaspersky Security Center*.

El complemento de administración Kaspersky Device Management para iOS se instala de forma predeterminada al implementar Kaspersky Security Center. El complemento no requiere una instalación independiente.

Requisitos de hardware y software

En esta sección se enumeran los requisitos de hardware y software que debe reunir el equipo del administrador que se utiliza para implementar las aplicaciones en dispositivos móviles, así como los sistemas operativos de dispositivos móviles que admite Kaspersky Security para dispositivos móviles.

Requisitos de hardware y software para el equipo del administrador

Para implementar la solución completa Kaspersky Security para dispositivos móviles, el equipo del administrador debe cumplir los requisitos de hardware de Kaspersky Security Center. Para obtener más información acerca del uso de los requisitos de hardware de Kaspersky Security Center, consulte la *Ayuda de Kaspersky Security Center*.

Para funcionar con el complemento de administración de Kaspersky Endpoint Security para Android, la Consola de administración de Kaspersky Security Center versión 12 se debe instalar en el equipo del administrador.

Para funcionar con el complemento de administración de Kaspersky Device Management para iOS, el equipo del administrador debe cumplir los siguientes requisitos de software:

- Consola de administración de Kaspersky Security Center 12 o versiones posteriores
- Componente del Servidor Exchange
- Componente del Servidor de MDM para iOS
- Conjunto de instrucciones de la versión SSE2 o de una versión más reciente

Para implementar la aplicación móvil Kaspersky Endpoint Security para Android a través del Servidor de Administración, el equipo del administrador debe reunir los requisitos de software que se indican a continuación:

- Kaspersky Security Center 12 o versiones posteriores
- Complemento de Administración de Kaspersky Endpoint Security para Android

No hay requisitos de software para el equipo del administrador cuando la aplicación móvil Kaspersky Endpoint Security para Android se implementa desde las tiendas en línea correspondientes.

La aplicación móvil Kaspersky Endpoint Security para Android también puede funcionar como parte del sistema de administración remota de Kaspersky Endpoint Security Cloud (Versión 6.0 y superior). Para obtener más información sobre cómo trabajar con aplicaciones mediante Kaspersky Endpoint Security Cloud, consulte la *Ayuda de Kaspersky Endpoint Security Cloud*.

La aplicación móvil Kaspersky Endpoint Security para Android puede funcionar en un sistema de terceros EMM:

- VMware AirWatch 9.3 o posterior
- MobileIron 10.0 o posterior
- IBM MaaS360 10.68 o posterior
- Microsoft Intune 1908 o posterior
- SOTI MobiControl 14.1.4 (1693) o posterior

Requisitos de hardware y software para que el dispositivo móvil del usuario admita la instalación de la aplicación Kaspersky Endpoint Security para Android

Estos son los requisitos de hardware y software de la aplicación Kaspersky Endpoint Security para Android:

- 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
- Android 5.0–12 (incluye Android 12L, no incluye la edición Go)
- 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 un perfil de MDM para iOS.

Para un perfil de MDM para iOS, el dispositivo debe cumplir los siguientes requisitos de hardware y software:

- iOS 10.0–15.0 o iPadOS 13–15
- Conexión a Internet

Consideraciones y problemas conocidos

Kaspersky Endpoint Security para Android cuenta con un número de problemas conocidos que no resultan críticos para el funcionamiento de la aplicación.

Problemas conocidos al instalar aplicaciones

- Kaspersky Endpoint Security para Android solo se instala en la memoria principal del dispositivo.
- En dispositivos con Android 7.0, 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 otras empresas (por ejemplo, VMWare AirWatch), solo los componentes Antivirus y Protección Web están disponibles. El administrador puede ajustar la configuración del Antivirus 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).

Problemas conocidos al actualizar la versión de la aplicación

- 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.
- Para actualizar Kaspersky Endpoint Security for Android usando un paquete de instalación independiente, se debe permitir la instalación de las aplicaciones desde fuentes desconocidas en el dispositivo móvil del usuario.
- Si Kaspersky Endpoint Security para Android se instaló desde Google Play, puede actualizar la aplicación a través de Google Play. Si la aplicación se instaló con otro método, no puede actualizarla a través de Google Play.
- Puede actualizar a través de Kaspersky Security Center si Kaspersky Endpoint Security para Android se instaló desde Kaspersky Security Center. Si se instaló desde Google Play, no puede actualizar la aplicación a través de Kaspersky Security Center.
- Después de actualizar los complementos de administración a la versión técnica 33, la aplicación Kaspersky Endpoint Security para Android también se debe actualizar a la versión técnica 33. De lo contrario, no podrá

activar Samsung KNOX en algunos de los dispositivos de sus usuarios.

Problemas conocidos en la operación del Antivirus

- 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 aplicación omite esos archivos sin notificarle que se omitieron.
- Para el análisis adicional de un dispositivo para amenazas nuevas cuya información todavía no se ha añadido a las bases de datos antivirus, 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 antivirus desde el Servidor de administración en un dispositivo móvil. Si eso sucede, ejecute la tarea de actualización de las bases de datos antivirus en el Servidor de administración.
- En ciertos dispositivos, Kaspersky Endpoint Security para Android no detecta dispositivos conectados por USB al instante. No es posible ejecutar un análisis antivirus en tales dispositivos.
- En dispositivos con Android 11.0 o versiones posteriores, el usuario debe otorgar el permiso "Permitir el acceso para administrar todos los archivos".
- En dispositivos que ejecuten Android 7.0 o versiones posteriores, puede que la ventana de configuración de la planificación de ejecución de análisis antivirus se muestre incorrectamente (no se muestran los elementos de administración). La causa de este problema es un defecto conocido de Android 7.
- En dispositivos que ejecutan Android 7.0, la protección en tiempo real en el modo extendido no detecta amenazas en archivos almacenados en una tarjeta SD externa.
- En dispositivos con Android 6.0, Kaspersky Endpoint Security para Android no detecta la descarga de archivos maliciosos a la memoria del dispositivo. El antivirus puede detectar un archivo malicioso cuando se ejecuta el archivo o durante un análisis antivirus en el dispositivo. La causa de este problema es un defecto conocido de Android 6.0. Para garantizar la seguridad del dispositivo, se recomienda configurar análisis de virus programados.

Problemas conocidos en la operación de Protección web

- La Protección web en los dispositivos Android solo funciona en el navegador Google Chrome (incluida la función de Pestañas personalizadas), el navegador Huawei y el navegador de Internet de Samsung. La Protección web para el Navegador de Samsung no bloquea sitios en un dispositivo móvil si se utiliza un perfil de trabajo y la Protección web está habilitada solo para el perfil de trabajo.
- Kaspersky Endpoint Security en el perfil de trabajo analiza solo el dominio del sitio web en el tráfico HTTPS. Los sitios web maliciosos y de phishing pueden permanecer desbloqueados si la app se instala en el perfil de trabajo. Si el dominio es de confianza, la Protección web puede omitir una amenaza (por ejemplo, `https://trusted.domain.com/phishing/`). Si el dominio no es de confianza, la Protección web bloquea los sitios web maliciosos y de phishing.
- Para que la Protección web funcione, debe habilitar el uso de Kaspersky Security Network. La Protección web bloquea sitios web según los datos que tenga KSN sobre la reputación y categoría de los sitios web.
- Los sitios web bloqueados pueden permanecer desbloqueados por la Protección web en dispositivos Android 6.0 con la versión 51 Google Chrome (o cualquier versión anterior) 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 historial de búsqueda.
- Utilización de la dirección web para completar automáticamente la función.
- 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 aplicaciones de otras empresas, por ejemplo, desde una aplicación del cliente MI. Este problema se relaciona con cómo el servicio de Accesibilidad funciona con la función de Chrome Custom Tabs.
- Los sitios web bloqueados pueden permanecer desbloqueados en el Navegador de Samsung si el usuario los abre en segundo plano desde el menú de contexto o desde aplicaciones de otras empresas, por ejemplo, desde una aplicación del cliente de MI.
- Kaspersky Endpoint Security para Android debe estar configurado como una función de accesibilidad para asegurar el correcto funcionamiento de Protección web.
- Al escribir una dirección de sitio web en la configuración de Protección web, adhiérase a las siguientes reglas:
  - Para dispositivos Android, especifique la dirección en el formato de expresiones habitual (por ejemplo, `http:\/\/www\.example\.com.*`).
  - Para dispositivos MDM iOS, especifique el HTTP o protocolo de transporte de datos de HTTPS (por ejemplo, `http://www.example.com`).
- Los sitios web permitidos se pueden bloquear en el Navegador de Samsung en el modo de Protección Web **Solo sitios web enumerados están permitidos** cuando la página se actualiza. Los sitios web se bloquean si una expresión habitual contiene la configuración avanzada (por ejemplo, `^https?:\/\/example\.com\/pictures\/`). Se recomienda usar expresiones habituales sin la configuración adicional (por ejemplo, `^https?:\/\/example\.com`).

Problemas conocidos en la operación 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 7.0 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 ha sido confirmado en Alcatel 5080X.

- Para localizar dispositivos con Android 10.0 o posterior, el usuario debe otorgar el permiso "Todo el tiempo" para la ubicación del dispositivo.
- Para tomar una foto de identificación en dispositivos con Android 11.0 o posterior, el usuario debe otorgar el permiso "Mientras se usa la aplicación" para acceder a la cámara.

Problemas conocidos en la operación Control de apps

- 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 Añadir aplicaciones particulares a las listas de aplicaciones bloqueadas y permitidas. En este caso, KSN no se requiere.
- Al configurar Control de apps, se recomienda desactivar la casilla **Bloquear apps del sistema**. El bloqueo de apps del sistema puede causar problemas en la operación del dispositivo.

Problemas conocidos al configurar el correo electrónico

- La configuración remota de un buzón de correo solo está disponible en los siguientes dispositivos:
  - Dispositivos iOS con MDM.
  - Dispositivos Samsung (Exchange ActiveSync).
  - Dispositivos Android con el cliente de correo electrónico TouchDown instalado.

    En las versiones anteriores de Kaspersky Endpoint Security para Android, puede utilizar Kaspersky Security Center para configurar de forma remota la configuración del perfil de TouchDown en el dispositivo de un usuario. El soporte de TouchDown se ha discontinuado en Kaspersky Endpoint Security para Android para Service Pack 4. Para obtener más información, visite el *sitio web del Soporte Técnico de Symantec*.

    Después de actualizar el complemento de administración Kaspersky Endpoint Security para Android, los ajustes de TouchDown en la directiva se ocultan pero se guardan. Cuando se conectan nuevos dispositivos, los ajustes de TouchDown se configurarán después de aplicar la directiva.

    Después de que la directiva se modifique y se guarde, los ajustes de TouchDown se eliminarán. La configuración de TouchDown en el dispositivo de un usuario se borrará después la aplicación de una directiva.

Problemas conocidos al configurar la seguridad de la contraseña de desbloqueo del dispositivo

- En dispositivos con Android 10.0 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 o numérica (PIN) con una secuencia que no tenga números repetidos u ordenados (por ejemplo, 1234), o alfanumérica. El PIN o contraseña debe tener al menos 4 caracteres de extensión.

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). La extensión del PIN debe ser de al menos 8 dígitos; la contraseña debe contar con al menos 6 caracteres.

- En dispositivos con Android 10.0 o posterior, el uso de la huella digital para desbloquear la pantalla solo puede configurarse para un perfil de trabajo.
- 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, para cambiar la contraseña de desbloqueo, solo se debe usar la aplicación del sistema Configuración.
- En algunos dispositivos con Android 6.0 o versiones posteriores, puede ocurrir un error cuando se ingresa la contraseña de desbloqueo de la pantalla si los datos del dispositivo están cifrados. Este problema se debe a características específicas del servicio de Accesibilidad con firmware MIUI.

Problemas conocidos al configurar el Wi-Fi

- En dispositivos la versión 8.0 de Android en ejecución o posterior, la configuración del servidor proxy para Wi-Fi no se puede redefinir con la directiva. Sin embargo, puede configurar manualmente la configuración del servidor proxy para una red Wi-Fi en el dispositivo móvil.

Problemas conocidos en la configuración de APN

- La configuración remota de APN solo está disponible en dispositivos MDM con iOS o en dispositivos Samsung.
- Configure APN para dispositivos iOS con MDM en la sección **Comunicaciones móviles**. La sección **APN** está desactualizada. Antes de ajustar la configuración APN, asegúrese de que la sección **Aplicar en** la casilla del dispositivo **APN** esté libre.

Problemas conocidos con el Firewall

- El uso de Firewall solo está disponible en dispositivos Samsung.

Problemas conocidos al configurar una VPN

- La configuración remota de VPN solo está disponible en los siguientes dispositivos:
  - Dispositivos iOS con MDM.
  - Dispositivos Samsung.

Problemas conocidos al funcionar con contenedores

- En Kaspersky Security para dispositivos móviles Service Pack 3 Maintenance Release 2, ya no se admite la creación de contenedores para aplicaciones móviles. Sin embargo, los contenedores que se crearon en versiones anteriores de la aplicación se pueden añadir a dispositivos Android.
- Para instalar aplicaciones en contenedores, debe permitir la instalación de aplicaciones de orígenes desconocidos en el dispositivo móvil del usuario. Para obtener información sobre la instalación de aplicaciones sin Google Play, consulte la *Guía de ayuda de Android*.
- En dispositivos con Android, los contenedores no pueden albergar aplicaciones con más de 65 536 métodos (configuración multidex).

Problemas conocidos con la protección ante la eliminación de la aplicación

- Se debe configurar Kaspersky Endpoint Security para Android como el administrador del dispositivo.
- Para proteger la aplicación contra la eliminación en dispositivos con Android 7.0 o posterior, Kaspersky Endpoint Security para Android debe estar configurado como función de accesibilidad.
- En algunos dispositivos Huawei y Xiaomi, la protección para eliminación Kaspersky Endpoint Security para Android no funciona. Este problema es causado por características específicas del firmware MIUI 7 y 8 en el firmware EMUI y Xiaomi en Huawei.

Problemas conocidos al configurar las restricciones del dispositivo

- En dispositivos con Android 10.0 o una versión posterior, no se admite prohibir el uso de redes Wi-Fi.
- En dispositivos con Android 10.0 o una versión posterior, el uso de la cámara no se puede prohibir completamente.
- En los dispositivos con Android 11 o posterior, Kaspersky Endpoint Security para Android debe estar configurado como una función de accesibilidad. Kaspersky Endpoint Security para Android solicita al usuario que configure la aplicación 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. Si este es el caso, no podrá restringir el uso de la cámara.

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 no más de 30 minutos antes. De lo contrario, el comando **Localizar dispositivo** falla.

Problemas conocidos en perfiles de trabajo de Android

- Si crea un perfil de trabajo de Android con una directiva, el usuario debe otorgar el permiso "Permitir el acceso para administrar todos los archivos" a Kaspersky Endpoint Security para Android que esté instalado en los dispositivos con Android 11 o versiones posteriores y que esté relacionado con el perfil de trabajo.

Problemas conocidos con 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 que el dispositivo móvil se reinicia. Además, si el dispositivo se ha bloqueado, no puede usar un comando para desbloquear el dispositivo. Puede desbloquear el dispositivo solo usando un código de desbloqueo de uso único.

- En ciertos dispositivos (por ejemplo, Meizu y Asus) que funcionan con Android 6.0 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 Kaspersky Endpoint Security para Android se establece como función de accesibilidad, puede aparecer una advertencia incorrecta sobre la falta de derechos adecuados. Para esconder este mensaje, habilitar la aplicación como aplicación protegida en la configuración del dispositivo.

- En algunos dispositivos Huawei que operan con Android 5. X o 6. X, cuando el modo de Ahorro de Batería se habilita para Kaspersky Endpoint Security para Android, el usuario puede cancelar manualmente la aplicación. El dispositivo del usuario queda sin protección después de esto. 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 7.0, el usuario puede esconder la notificación en cuanto al 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 6.0, el ícono de Kaspersky Endpoint Security para Android se puede esconder 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 7.0 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.

- La Protección web no puede 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.

- Después de ejecutar comandos Antirrobo (por ejemplo Localizar, Bloqueo del dispositivo, Desbloquear y Foto de identificación), se puede eliminar el certificado general y el certificado de VPN en algunos dispositivos de Samsung. Se deben reinstalar los certificados para continuar. Este problema ocurre debido a la norma de seguridad del perfil de protección fundamental de dispositivos móviles (Mobile Device Fundamentals Protection Profile, MDFPP).

- 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 algunos dispositivos Samsung, después de instalar o actualizar Kaspersky Endpoint Security desde un paquete de instalación independiente, la activación del perfil KNOX MDM no está disponible.

- 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 proporcionan la aplicación de pantallas recientes personalizada con privilegios elevados. 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 con Android 11, la aplicación Kaspersky Endpoint Security para Android se bloquea inmediatamente después del inicio. La causa de este problema es un defecto conocido de Android 11.

Despliegue

Esta sección de la Ayuda está destinada a especialistas que instalan Kaspersky Security para dispositivos móviles, así como también a especialistas que proporcionan servicio de soporte técnico a organizaciones que usan Kaspersky Security para dispositivos móviles.

Arquitectura de solución

Kaspersky Security para dispositivos móviles incluye los componentes siguientes:

- App móvil 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. Admite la interacción entre el dispositivo móvil y el Servidor de administración de Kaspersky Security Center usando Firebase Cloud Messaging.

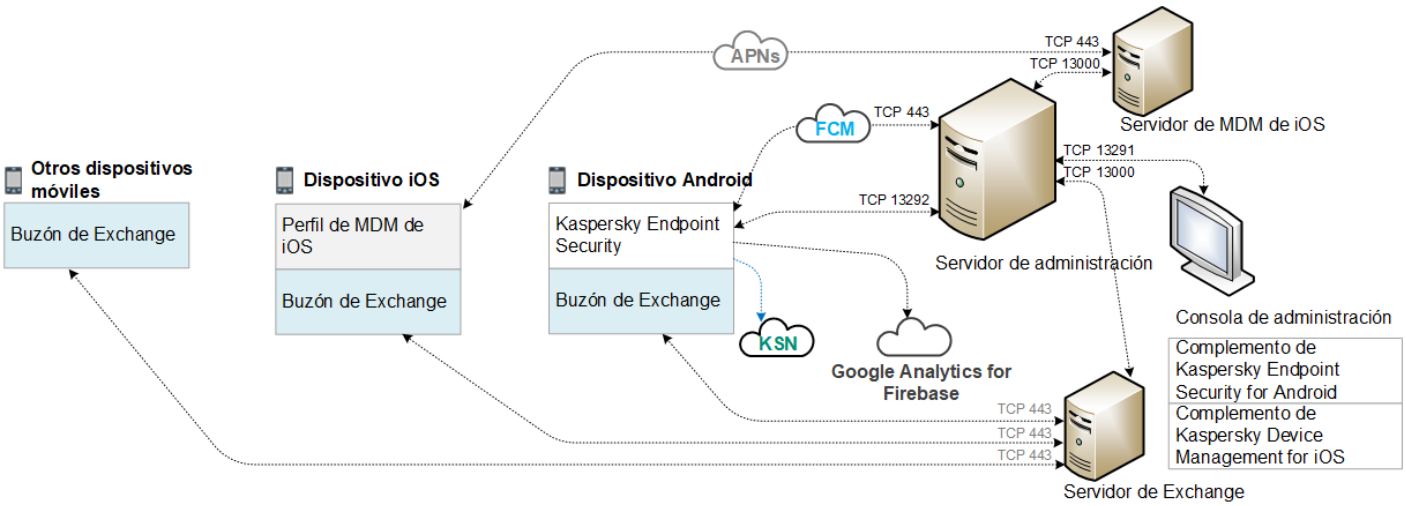
- Complemento de administración de Kaspersky Endpoint Security para Android

  El complemento de administración Kaspersky Endpoint Security para Android incluye la interfaz para administrar los dispositivos móviles y las aplicaciones móviles instaladas en ellos mediante la Consola de administración de Kaspersky Security Center.

- Complemento de Administración de Kaspersky Device Management para iOS

El complemento de administración Kaspersky Device Management para iOS ofrece una interfaz para administrar los dispositivos móviles conectados a través del servidor de MDM de iOS y el protocolo Exchange ActiveSync mediante la Consola de administración de Kaspersky Security Center.

La arquitectura de la solución integrada Kaspersky Security para dispositivos móviles se muestra en la figura a continuación.



La arquitectura de Kaspersky Security para dispositivos móviles

Para obtener más información sobre la Consola de administración, el Servidor de administración, el Servidor Exchange y el servidor de MDM para iOS, consulte la *Ayuda de Kaspersky Security Center*.

Escenarios comunes de despliegue de la solución integrada

En esta sección se describen los escenarios comunes de despliegue de la solución integrada Kaspersky Security para dispositivos móviles.

Se pueden utilizar diferentes escenarios de despliegue para instalar la solución integrada en dispositivos Android y dispositivos iOS. Si la organización usa dispositivos móviles que ejecutan varios sistemas operativos, las aplicaciones se deben instalar para cada sistema operativo por separado siguiendo el escenario de despliegue correspondiente.

Escenarios de despliegue de Kaspersky Endpoint Security para Android

Kaspersky Endpoint Security para Android se puede implementar en dispositivos móviles de la red corporativa de diferentes formas. Puede usar el escenario de despliegue más adecuado para su organización o combinar varios escenarios de despliegue.

Para obtener más información sobre la implementación de Kaspersky Endpoint Security para Android en Kaspersky Endpoint Security Cloud, consulte la *ayuda de Kaspersky Endpoint Security Cloud*.

Implementación de Kaspersky Endpoint Security para Android mediante Kaspersky Security Center

Puede implementar Kaspersky Endpoint Security para Android mediante Kaspersky Security Center usando los métodos siguientes:

- Entregue mensajes con el enlace de Google Play (recomendado)
- Entregue mensajes con un enlace al paquete de aplicación independiente

El despliegue de Kaspersky Endpoint Security para Android usando Google Play se realiza mediante el envío de mensajes que contienen el enlace de Google Play a usuarios de dispositivos desde la Consola de administración.

Para implementar Kaspersky Endpoint Security para Android mediante la entrega de un paquete independiente, el administrador debe seguir estos pasos:

1. Creación de un paquete de instalación de la aplicación.
2. Configuración del paquete de instalación.
3. Creación de un paquete de instalación independiente.
4. Envío de mensajes con un enlace para descargar un paquete de instalación independiente a los usuarios de dispositivos Android. Está disponible el envío masivo de correos.

El usuario instala Kaspersky Endpoint Security para Android en un dispositivo móvil después de recibir un mensaje con un enlace de Google Play o un enlace para descargar el paquete de instalación desde el Servidor web de Kaspersky Security Center. No se requiere ninguna preparación adicional para empezar a utilizar la aplicación.

Implementación de Kaspersky Endpoint Security para Android desde Google Play

Se recomienda emplear el escenario de despliegue de Google Play si no es posible la instalación remota.

Los usuarios de dispositivos instalan de forma independiente Kaspersky Endpoint Security para Android desde Google Play. Los usuarios descargan el paquete de distribución de la aplicación móvil desde Google Play e instalan la aplicación en sus dispositivos. Después de que la aplicación se ha instalado en el dispositivo, se deben realizar preparaciones adicionales antes de poder comenzar a usarlo: configurar la conexión con el Servidor de administración e instalar un certificado general.

Implementación de Kaspersky Endpoint Security para Android a través de KNOX Mobile Enrollment

El despliegue de Kaspersky Endpoint Security para Android consiste en agregar un perfil MDM KNOX a dispositivos móviles. El perfil MDM KNOX contiene un vínculo a una aplicación instalada en el Servidor web de Kaspersky Security Center u otro servidor. Después de que la aplicación se instala en el dispositivo móvil, también debe instalar un certificado general.

Puede leer acerca de la instalación a través de KNOX Mobile Enrollment en la sección Samsung KNOX.

Escenarios de despliegue para el perfil de MDM para iOS

Un *perfil de MDM para iOS* es un perfil que contiene la configuración para conectar dispositivos móviles con iOS a Kaspersky Security Center. Después de instalar un perfil de MDM para iOS y sincronizar con Kaspersky Security Center, el dispositivo pasa a ser un dispositivo administrado. Los dispositivos móviles se administran a través del servicio Apple Push Notification (APN). Para obtener más información sobre cómo instalar un perfil de MDM para iOS y trabajar con APN, consulte la *ayuda de Kaspersky Security Center*.

Con un perfil de MDM para iOS, puede hacer lo siguiente:

- Configurar de forma remota dispositivos iOS con MDM mediante directivas de grupo.
- Enviar comandos de bloqueo del dispositivo y borrado de datos.
- Instalar remotamente aplicaciones de Kaspersky y otras aplicaciones de otras empresas.

Un perfil de MDM para iOS se puede implementar en dispositivos móviles de la red corporativa de diferentes formas. Puede usar el escenario de despliegue más adecuado para su organización o combinar varios escenarios de despliegue.

Antes de implementar un perfil de MDM para iOS, el administrador debe hacer lo siguiente:

1. Instalar un Servidor de MDM para iOS.
2. Obtener un certificado del servicio Apple Push Notification (certificado de APNs).
3. Instalar un certificado de APNs en el Servidor de MDM para iOS.

Para obtener más información acerca de cómo instalar un servidor de MDM para iOS y trabajar con un certificado de APNs, consulte la *ayuda de Kaspersky Security Center*.

Para obtener más información sobre la implementación de un perfil de MDM para iOS en Kaspersky Endpoint Security Cloud, consulte la *ayuda de Kaspersky Endpoint Security Cloud*.

Implementación de un perfil de MDM para iOS a través de Kaspersky Security Center

El despliegue de un perfil de MDM para iOS a través de Kaspersky Security Center se puede llevar a cabo enviando mensajes que contengan un enlace para descargar el perfil de MDM para iOS. Está disponible el envío masivo de correos.

El usuario instala el perfil de MDM para iOS en un dispositivo móvil después de recibir el mensaje con un enlace al Servidor web de Kaspersky Security Center. No se requiere ninguna preparación adicional para el perfil de MDM para iOS.

Para obtener más información acerca de cómo crear un perfil de MDM para iOS, consulte la *ayuda de Kaspersky Security Center*.

Preparación de la Consola de administración para el despliegue de la solución integrada

En esta sección se incluyen instrucciones sobre la preparación de la Consola de administración para el despliegue de la solución integrada.

Configuración del Servidor de Administración para la conexión de dispositivos móviles

Para que los dispositivos móviles puedan conectarse al Servidor de administración, antes de instalar la aplicación móvil Kaspersky Endpoint Security configure la conexión del dispositivo móvil en las propiedades del Servidor de administración.

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

1. En el menú contextual del Servidor de Administración, seleccione **Propiedades**.

   Se abrirá la ventana de configuración del Servidor de Administración.

2. Seleccione **Configuración de conexión del servidor → Puertos adicionales**.

3. Seleccione la casilla **Puerto abierto para dispositivos móviles**.

4. En el campo **Puerto para 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 la casilla de verificación **Abrir puerto para dispositivos móviles** está desactivada o se ha seleccionado un puerto de conexión equivocado, los dispositivos móviles no se podrán conectar al Servidor de Administración.

5. En el campo **Puerto para activar a clientes móviles**, especifique el puerto que utilizarán los dispositivos móviles para conectarse al Servidor de administración y activar la aplicación Kaspersky Endpoint Security para Android. El puerto 17100 se utiliza de forma predeterminada.

6. Haga clic en **Aceptar**.

Visualización de la carpeta de Mobile Device Management en la Consola de administración

Al visualizar la carpeta **Administración de dispositivos móviles** en la Consola de administración, puede ver la lista de dispositivos móviles administrados por el Servidor de Administración, configurar la administración de dispositivos móviles e instalar certificados en los dispositivos móviles de los usuarios.

*Para activar la visualización de la carpeta **Administración de dispositivos móviles** en la Consola de administración, siga estos pasos:*

1. En el menú contextual del Servidor de Administración, seleccione **Ver → Interfaz de configuración**.

2. En la ventana emergente, seleccione la casilla **Mostrar gestión de dispositivos móviles**.

3. Haga clic en **Aceptar**.

   La carpeta **Administración de dispositivos móviles** se muestra en el árbol de la Consola de administración después de reiniciarla.

Creación de un grupo de administración

Si desea configurar de manera centralizada la aplicación Kaspersky Endpoint Security para Android instalada en los dispositivos móviles de los usuarios, debe aplicar las directivas de grupo a los dispositivos.

Para aplicar la directiva a un grupo de dispositivos, es aconsejable crear un grupo aparte para los dispositivos en la carpeta **Dispositivos administrados** antes de instalar las aplicaciones móviles en dispositivos de los usuarios.

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. Los parámetros de configuración que son comunes para todos los dispositivos utilizando una directiva de grupo.

Para crear un grupo de administración, siga estos pasos:

1. En el árbol de la consola, seleccione la carpeta **Dispositivos administrados**.
2. En el espacio de trabajo de la carpeta o subcarpeta **Dispositivos administrados**, seleccione la pestaña **Dispositivos**.
3. Haga clic en el botón **Nuevo grupo**.

   Esto abre la ventana en la cual puede crear un nuevo grupo.
4. En la ventana **Nombre del grupo**, escriba un nombre y haga clic en **Aceptar**.

Aparecerá una nueva carpeta de grupo de administración con el nombre especificado en el árbol de la consola. Para obtener más información sobre el uso de los grupos de administración, consulte la *ayuda de Kaspersky Security Center*.

Creación de una regla para asignación automática de dispositivos a grupos de administración

Puede administrar de manera centralizada la configuración de la aplicación Kaspersky Endpoint Security para Android instalada en los dispositivos móviles de los usuarios solo si los dispositivos pertenecen a un grupo de administración creado previamente en el cual se haya configurado una directiva de grupo.

Si no se ha establecido automáticamente una regla para asignar los dispositivos móviles detectados en la red al grupo de administración, durante la primera sincronización con el Servidor de administración, el dispositivo se envía automáticamente a la Consola de administración en la carpeta **Adicional** → **Grupo de redes** → **Dominios** → **KES10**. No se aplica una directiva de grupo a este dispositivo.

Para crear la regla de asignación automática de dispositivos móviles al grupo de administración, siga estos pasos:

1. En el árbol de la consola, seleccione la carpeta **Dispositivos no asignados**.
2. En el menú contextual de la carpeta **Dispositivos no asignados**, seleccione **Propiedades**.

   Se abrirá la ventana **Propiedades: Dispositivos no asignados**.
3. En la sección **Mover dispositivos**, haga clic en **Agregar** para iniciar la creación de la regla y asignar automáticamente dispositivos a grupos de administración.

   Se abre la ventana **Nueva regla**.
4. Escriba el nombre de la regla.
5. Especifique el grupo de administración al que deben asignarse los dispositivos móviles después de haber instalado en ellos la aplicación móvil Kaspersky Endpoint Security para Android. Para ello, haga clic en **Seleccionar** a la derecha del campo **Grupo donde migrar los dispositivos** y seleccione el grupo en la ventana que aparece.
6. En la sección **Implementar regla**, seleccione **Ejecutar una vez para cada dispositivo**.
7. Seleccione la casilla **Mover solo los dispositivos no agregados a los** grupos de administración para evitar que se asignen al grupo seleccionado los dispositivos móviles asignados a otros grupos de administración al aplicar

la regla.

8. Seleccione la casilla **Habilitar regla** para que pueda aplicarse a dispositivos que se detecten posteriormente.

9. Abra la sección **Aplicaciones** y haga lo siguiente:

   a. Seleccione la casilla **Versión del sistema operativo**.

   b. Seleccione uno o más tipos de sistemas operativos de los dispositivos que se van a asignar al grupo especificado: Android o iOS.

10. Haga clic en **Aceptar**.

Una vez que se ha creado, la regla aparece en la lista de reglas de asignación de dispositivos de la sección **Mover dispositivos** en la ventana de propiedades de la carpeta **Dispositivos no asignados**.

De acuerdo con esta regla, Kaspersky Security Center asigna al grupo seleccionado todos los dispositivos que cumplen los requisitos especificados en la carpeta **Dispositivos no asignados**. Los dispositivos móviles asignados anteriormente a la carpeta **Dispositivos no asignados** también se pueden asignar manualmente al grupo de administración requerido de la carpeta **Dispositivos administrados**. Para obtener más información sobre la gestión y las acciones de los grupos de administración con dispositivos no distribuidos, consulte la *ayuda de Kaspersky Security Center*.

Creación de un certificado general

Para identificar al usuario de un dispositivo móvil, debe crear un certificado general en la Consola de administración.

Para crear un certificado general:

1. En el árbol de la consola, seleccione la carpeta **Administración de dispositivos móviles** → **Certificados**.

2. En el espacio de trabajo de la carpeta **Certificados**, haga clic en el botón **Agregar certificado** para iniciar el asistente de instalación de certificados.

3. En la ventana **Tipo de certificado** del asistente, seleccione la opción **Certificado general**.

4. En la ventana **Selección de usuario** del asistente, especifique para qué usuarios desea crear un certificado general.

5. En la ventana **Origen del certificado** del asistente, seleccione el método de creación del certificado general.

   - Para crear un certificado general automáticamente utilizando las herramientas del Servidor de Administración, seleccione **Especificar el certificado con las herramientas del Servidor de Administración**.

   - Para asignar un certificado previamente creado a un usuario, seleccione la opción **Especificar archivo de certificado**. Haga clic en el botón **Especificar** para abrir la ventana **Certificado** y especificar en ella el archivo de certificado.

     Si no desea especificar el tipo de dispositivo móvil ni el método de notificación al usuario la creación del certificado, desactive la casilla de verificación **Publicar certificado**.

6. En la ventana **Método de notificación al usuario** del asistente, defina la configuración de los parámetros de notificación de la creación del certificado al usuario del dispositivo móvil por mensaje de texto o correo electrónico.

7. En la ventana **Generar certificado** del asistente, haga clic en el botón **Finalizar** para terminar el asistente de instalación de certificados.

   Al hacerlo, el asistente de creación de certificados crea un certificado general que el usuario puede instalar en el dispositivo móvil. Para conseguir el certificado, inicie la sincronización del dispositivo móvil con el Servidor de Administración. Para obtener más información sobre la creación de certificados y la configuración de reglas para emitirlos, consulte la *ayuda de Kaspersky Security Center*.

Instalación de Kaspersky Endpoint Security para Android

En esta sección se describen los métodos de implementación de Kaspersky Endpoint Security para Android en una red corporativa.

Permisos

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, 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 versiones posteriores, 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.

Ya no hay soporte para el Filtro de llamadas y texto o el Seguimiento de SIM en Kaspersky Endpoint Security para Android Service Pack 4 Actualización 4 (Compilación 10.8.0.103). En este caso, Kaspersky Endpoint Security para Android no solicita al usuario los permisos de administración de SMS. Para habilitar el Filtro de llamadas y texto y todas las funciones de Seguimiento de SIM, debe usar una versión anterior de Kaspersky Endpoint Security para Android.

Permisos solicitados por Kaspersky Endpoint Security para Android

Permiso	Función de la aplicación
Teléfono (requerido solo para Android 5.0 a 9.X)	Conexión con Kaspersky Security Center (ID del dispositivo)
Almacenamiento (obligatorio)	Antivirus
Acceso para administrar todos los archivos	Antivirus (solo para Android 11 o versiones posteriores)
Dispositivos Bluetooth cercanos (para Android 12 o posterior)	Restricción del uso de Bluetooth

Administrador del dispositivo (obligatorio)	Antirrobo: bloqueo del dispositivo (solo para Android 5.0 a 6.X)
	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 11.0 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 10.0 o posterior, el usuario debe conceder el permiso "Todo el tiempo" cuando se solicite.
Accesibilidad	Antirrobo: bloqueo del dispositivo (solo para Android 7.0 y versiones posteriores)
	Protección web
	Control de apps
	Protección de eliminación de aplicaciones (solo para Android 7.0 y versiones posteriores)
	Visualización de advertencias de Kaspersky Endpoint Security para Android (solo para Android 10.0 o versiones posteriores)
	Restringir el uso de la cámara (solo para Android 11 o posterior)

Instalación de Kaspersky Endpoint Security para Android mediante un enlace de Google Play

Kaspersky Endpoint Security para Android se instala en los dispositivos móviles de usuarios con cuentas de usuario añadidas en Kaspersky Security Center. Para obtener más información sobre las cuentas de usuario en Kaspersky Security Center, consulte la ayuda de Kaspersky Security Center.

Kaspersky Security para dispositivos móviles le permite instalar la aplicación mediante Kaspersky Security Center utilizando un enlace de Google Play (método recomendado).

El usuario recibirá un enlace a Google Play. La aplicación puede instalarse si se sigue el procedimiento de instalación estándar en la plataforma Android. Después de la instalación, no se requiere configuración adicional de Kaspersky Endpoint Security para Android.

Algunos dispositivos de Huawei y Honor no poseen servicios de Google y, por lo tanto, no tienen acceso a aplicaciones en Google Play. Si algunos usuarios de dispositivos Huawei y Honor no pueden instalar la aplicación desde Google Play, deberían recibir instrucciones para instalar la aplicación desde Huawei App Gallery.

El vínculo incluye los siguientes datos:

- Configuración de sincronización de Kaspersky Security Center.
- Certificado general.
- Indicador de aceptación de los Términos y condiciones del Contrato de licencia de usuario final para Kaspersky Endpoint Security para Android y las Declaraciones adicionales. Si el administrador acepta los términos del Contrato de licencia y las declaraciones adicionales en la Consola de administración, Kaspersky Endpoint Security para Android omite el paso de aceptación durante la instalación de la aplicación.

Para instalar Kaspersky Endpoint Security para Android a través de Kaspersky Security Center usando un enlace de Google Play:

1. En el árbol de la consola, seleccione la carpeta **Administración de dispositivos móviles → Dispositivos móviles**.
2. En el espacio de trabajo de la carpeta **Dispositivos móviles**, haga clic en el botón **Añadir dispositivo móvil**.

   Esto inicia el Asistente de Nueva conexión de dispositivo móvil. Siga las instrucciones del asistente.
3. En la ventana **Sistema operativo** del Asistente, seleccione **Android**.

   Kaspersky Security Center busca actualizaciones para los complementos de administración. Si Kaspersky Security Center detecta actualizaciones, puede instalar la nueva versión del complemento de administración. Cuando el complemento de administración se actualice, podrá aceptar los Términos y condiciones del Contrato de licencia de usuario final (EULA) y las declaraciones adicionales para Kaspersky Endpoint Security para Android. Si el administrador acepta el Contrato de licencia y las declaraciones adicionales en la Consola de administración, Kaspersky Endpoint Security para Android omite el paso de aceptación durante la instalación de la aplicación. Esta función está disponible en la versión 12 de Kaspersky Security Center.
4. En la página del **método de instalación de Kaspersky Endpoint Security para Android**, seleccione el método de instalación de la aplicación **utilizando un enlace de Google Play**.
5. En la página **Seleccionar usuarios** del Asistente, seleccione uno o más usuarios para la instalación de Kaspersky Endpoint Security para Android en sus dispositivos móviles.

   Si un usuario no está en la lista, puede añadir una nueva cuenta de usuario sin salir del Asistente de Nueva conexión de dispositivo móvil.
6. En la página **Origen del certificado** del Asistente, seleccione el origen del certificado para la protección de la transferencia de datos entre Kaspersky Endpoint Security para Android y Kaspersky Security Center:

   - **Emitir certificado mediante herramientas del Servidor de Administración.** En este caso, el certificado se creará automáticamente.

- **Especificar el archivo del certificado**. En este caso, su propio certificado debe estar preparado con adelanto y luego seleccionarse en la ventana del Asistente. Esta opción no se puede utilizar para instalar Kaspersky Endpoint Security para Android en varios dispositivos móviles. Se debe crear un certificado independiente para cada usuario.

7. En la página **Método de notificación del usuario** del Asistente, seleccione el canal utilizado para reenviar el vínculo de instalación de la aplicación:

   - Para enviar el enlace por correo electrónico, seleccione **Enviar enlace a Kaspersky Endpoint Security** y configure los ajustes en la sección **Por correo electrónico**. Asegúrese de que la dirección de correo electrónico se especifique en la configuración de cuentas de usuario.

   - Para enviar el enlace por mensaje de texto, seleccione **Enviar enlace a Kaspersky Endpoint Security** y configure los ajustes en la sección **Por SMS**. Asegúrese de que el número de teléfono esté especificado en la configuración de cuentas de usuario.

   - Para instalar Kaspersky Endpoint Security para Android usando un código QR, seleccione **Mostrar enlace a paquete de instalación** y escanee el QR usando la cámara del dispositivo móvil.

   - Si ninguno de los métodos citados es conveniente, seleccione **Mostrar enlace a paquete de instalación** → **Copiar** para copiar al portapapeles el enlace de instalación de Kaspersky Endpoint Security para Android. Use cualquier método disponible para distribuir el enlace de instalación de la aplicación. También puede utilizar otros métodos de instalación de Kaspersky Endpoint Security para Android.

8. Haga clic en **Finalizar** para cerrar el Asistente de Nueva conexión de dispositivo móvil.

Después de instalar Kaspersky Endpoint Security para Android en los dispositivos móviles de los usuarios, podrá ajustar la configuración para dispositivos y aplicaciones mediante las directivas de grupo. También podrá enviar comandos a dispositivos móviles para la protección de datos en caso de que los dispositivos se pierdan o sean robados.

Otros métodos de instalación de Kaspersky Endpoint Security para Android

Puede instalar Kaspersky Endpoint Security para Android mediante un enlace a su propio servidor web o indicar a los usuarios que instalen la aplicación manualmente.

Instalación manual desde Google Play o Huawei AppGallery

Los usuarios pueden instalar Kaspersky Endpoint Security para Android manualmente desde Google Play o Huawei AppGallery. La aplicación puede instalarse siguiendo el procedimiento de instalación estándar de la plataforma Android. Para instalar la aplicación, los usuarios utilizan sus propias cuentas de Google.

Para obtener más información sobre el procedimiento de instalación de Kaspersky Endpoint Security para Android desde Google Play, consulte el sitio web del servicio de soporte técnico de Google.

Para obtener más información sobre el procedimiento de instalación de Kaspersky Endpoint Security para Android desde Huawei AppGallery, consulte el sitio web del servicio de soporte técnico de HUAWEI.

Algunos dispositivos de Huawei y Honor no poseen servicios de Google y, por lo tanto, no tienen acceso a aplicaciones en Google Play. Si algunos usuarios de dispositivos Huawei y Honor no pueden instalar la aplicación desde Google Play, deberían recibir instrucciones para instalar la aplicación desde Huawei App Gallery.

Después de instalar Kaspersky Endpoint Security para Android desde Google Play o Huawei AppGallery, debe preparar la aplicación para su uso. El proceso de preparar la aplicación para su uso incluye los pasos siguientes:

1. El administrador envía la configuración de la sincronización del dispositivo móvil con el Servidor de Administración (dirección del servidor y número de puerto) usando cualquier método disponible (por ejemplo, enviando un mensaje de correo electrónico).

2. El usuario puede configurar las opciones de sincronización del dispositivo móvil con el Servidor de Administración durante el funcionamiento del Asistente de configuración inicial o en la configuración de Kaspersky Endpoint Security para Android.

3. El administrador crea un certificado general para el usuario del dispositivo móvil.

4. El usuario recibe una notificación automática con una solicitud para instalar el certificado general. Una vez que se ha confirmado la instalación, el certificado general se instala en el dispositivo móvil.

El acceso a Internet debe estar activado en el dispositivo móvil para la sincronización con el Servidor de Administración.

En la Ayuda de Kaspersky Security Center encontrará información para configurar las opciones de sincronización del dispositivo móvil con el Servidor de Administración y recibir un certificado general.

Durante la siguiente sincronización del dispositivo móvil con el Servidor de Administración, el dispositivo móvil del usuario que tiene instalado Kaspersky Endpoint Security para Android se traslada a la carpeta **Adicional** → **Grupo de redes** → **Dominios** del grupo de administración especificado durante la instalación de la aplicación (el grupo predeterminado es **KES10**). Puede mover un dispositivo móvil al grupo de administración que creó en la carpeta Dispositivos administrados manualmente o mediante las reglas de asignación automática.

Este método de instalación es conveniente si desea instalar una versión específica de Kaspersky Endpoint Security para Android.

Para instalar Kaspersky Endpoint Security para Android usando un enlace a su propio servidor web:

1. Cree un paquete de instalación y configure sus ajustes.

   El *paquete de instalación* es un conjunto de archivos creado para la instalación remota de la aplicación Kaspersky mediante Kaspersky Security Center.

2. Cree un paquete de instalación independiente.

   Un *paquete de instalación independiente* es el archivo de instalación de una aplicación móvil que contiene la configuración para conectar la aplicación al Servidor de administración y un indicador de aceptación de los Términos y condiciones del Contrato de licencia de usuario final (EULA) para la aplicación Kaspersky Endpoint Security para Android. Se crea sobre la base del paquete de instalación de Kaspersky Endpoint Security para Android. El paquete de instalación independiente es un caso especial de un paquete de instalación.

El usuario recibirá un enlace al servidor web que aloja al paquete de instalación independiente de Kaspersky Endpoint Security para Android. Para instalar la aplicación, el usuario debe ejecutar el archivo APK. Después de la instalación, no se requiere configuración adicional de Kaspersky Endpoint Security para Android.

Para instalar Kaspersky Endpoint Security for Android usando un enlace a su propio servidor web, se debe permitir la instalación de las aplicaciones desde fuentes desconocidas en el dispositivo móvil del usuario.

Crear y configurar un paquete de instalación

El paquete de instalación de Kaspersky Endpoint Security para Android es el archivo comprimido de autoextracción `sc_package.exe`. El archivo incluye los archivos necesarios para la instalación de las aplicaciones móviles en los dispositivos:

- `adb.exe`, `AdbWinApi.dll` y `AdbWinUsbApi.dll`: Conjunto de archivos necesarios para la instalación de Kaspersky Endpoint Security para Android.
- `installer.ini`: El archivo de configuración que contiene la configuración de conexión del Servidor de administración.
- `KES10_xx_xx_xxx.apk`: Archivo de configuración para Kaspersky Endpoint Security para Android.
- `kmlisten.exe`: Herramienta para enviar el paquete de instalación de la aplicación a través de una estación de trabajo.
- `kmlisten.ini`: Archivo de configuración que contiene los parámetros para la herramienta de envío del paquete de instalación.
- `kmlisten.kpd`: Archivo de descripción de la aplicación.

Para crear el paquete de instalación de Kaspersky Endpoint Security para Android:

1. En el árbol de la consola, seleccione la carpeta **Adicional** → **Instalación remota** → **Paquetes de instalación**.
2. En el espacio de trabajo de la carpeta **Paquetes de instalación**, haga clic en el botón **Crear paquete de instalación**.

   Se inicia el asistente de creación de paquetes de instalación. Siga las instrucciones del asistente.
3. En la ventana **Seleccionar el tipo de paquete de instalación**, haga clic en **Crear paquete de instalación para una aplicación Kaspersky**.
4. En la ventana **Definir nombre del paquete de instalación** del Asistente, ingrese el nombre del paquete de instalación que se mostrará en el espacio de trabajo de la carpeta **Instalación de paquetes**.
5. En la ventana **Seleccionar el paquete de instalación de la aplicación** del asistente, seleccione el archivo comprimido de autoextracción `sc_package.exe` incluido en el kit de distribución.

   Si ya ha descomprimido dicho archivo, elija el archivo de descripción de la aplicación, `kmlisten.kpd`. El nombre de la aplicación y el número de versión aparecen en el campo de entrada.
6. En la ventana **Aceptar EULA** del asistente, lea, entienda y acepte los términos y condiciones del Contrato de licencia de usuario final.

   Debe aceptar los términos y condiciones del Contrato de licencia de usuario final para crear el paquete de instalación. Si acepta los términos del Contrato de licencia en la Consola de administración, Kaspersky Endpoint Security para Android omite el paso de aceptación durante la instalación de la aplicación.

   Si decide detener la protección de los dispositivos móviles, puede desinstalar la aplicación Kaspersky Endpoint Security para Android y revocar el Contrato de licencia de usuario final (EULA) para la aplicación. Para obtener más información sobre cómo revocar el EULA, consulte la *ayuda de Kaspersky Security Center*.

Al finalizar el procedimiento del asistente, el paquete de instalación creado aparece en el espacio de trabajo de la carpeta **Paquetes de instalación**. Los paquetes de instalación se guardan en la carpeta Paquetes que se encuentra en la carpeta pública compartida del Servidor de Administración.

Para configurar el paquete de instalación:

1. En el árbol de la consola, seleccione la carpeta **Adicional** → **Instalación remota** → **Paquetes de instalación**.
2. En el menú contextual del paquete de instalación de Kaspersky Endpoint Security para Android, seleccione **Propiedades**.
3. En la pestaña **Configuración**, especifique la configuración de conexión del Servidor de Administración para dispositivos móviles y el nombre del grupo de administración al que se agregarán automáticamente los dispositivos móviles tras la primera sincronización con el Servidor de Administración. Siga los pasos detallados a continuación:
   - En la sección **Conexión al Servidor de administración**, en el campo **Dirección del servidor**, escriba el nombre del Servidor de Administración para dispositivos móviles con el formato usado para instalar **Compatibilidad con dispositivos móviles** durante el despliegue del Servidor de Administración.

     Según el formato del nombre de Servidor de Administración para el componente **Soporte para dispositivos móviles**, especifique el nombre DNS o la dirección IP del Servidor de Administración. En el campo **Número de puerto SSL**, especifique el número de puerto abierto en el Servidor de Administración para conectar dispositivos móviles. El puerto 13292 se utiliza de forma predeterminada.
   - En la sección **Asignación de equipos a grupos**, en el campo **Nombre del grupo**, escriba el del grupo al que se agregarán los dispositivos móviles tras la primera sincronización con el Servidor de Administración (**KES10** se usa de forma predeterminada).

     El grupo especificado se creará automáticamente en la carpeta **Adicional** → **Sondeo de red** → **Dominios**.
   - En la sección **Acciones durante la instalación**, seleccione la casilla **Solicitar correo electrónico** si desea que la aplicación pida que usuarios proporcionen su dirección de correo electrónico corporativa cuando la aplicación se inicia por primera vez.

     La dirección de correo electrónico del usuario se emplea para asignar un nombre al dispositivo móvil cuando se agrega al grupo de administración.
4. Para implementar las configuraciones especificadas, haga clic en **Aplicar**.

Creación de un paquete de instalación independiente

Para crear un paquete de instalación independiente, siga los pasos detallados a continuación:

1. En el árbol de la consola, seleccione la carpeta **Adicional** → **Instalación remota** → **Paquetes de instalación**.
2. Elija el paquete de instalación de Kaspersky Endpoint Security para Android.
3. En el menú contextual del paquete de instalación, seleccione **Crear un paquete de instalación independiente**.

   Se iniciará el asistente a cargo de la creación del paquete de instalación independiente. Siga las instrucciones del asistente.
4. Configure las formas en que se distribuye el paquete de instalación independiente:
   - Para facilitar a los usuarios la ruta al paquete de instalación independiente creado mediante correo electrónico, en la sección **Más acciones**, haga clic en el enlace **Enviar enlace al paquete de instalación independiente por correo electrónico**.

     Se abrirá la ventana del editor de mensajes y el texto en la ventana incluirá la ruta a la carpeta compartida con el paquete de instalación independiente.

- Para publicar en su sitio web corporativo el enlace al paquete de instalación independiente creado, haga clic en el enlace **Código HTML de ejemplo para publicar el enlace en el sitio web**.

  Se abrirá un archivo TMP con enlaces HTML_RJL.

5. Para publicar el paquete de instalación independiente creado en el Servidor web de Kaspersky Security Center y ver toda la lista de paquetes independientes para el paquete de instalación seleccionado, seleccione en la ventana **Asistente de paquete de instalación independiente finalizado correctamente** la casilla de verificación **Abrir la lista de paquetes independientes**.

Cuando se cierra el asistente, se abre la ventana **Lista de paquetes independientes para el paquete de instalación <Installation package name>**.

La ventana **Lista de paquetes independientes para el paquete de instalación <Installation package name>** contiene la información siguiente:

- Una lista de paquetes de instalación independientes.
- La ruta de red a la carpeta compartida en el campo **Ruta**.
- La dirección del paquete independiente en el Servidor web de Kaspersky Security Center en el campo **URL**.

Al enviar las notificaciones de correo electrónico, puede especificar la dirección en el campo **URL** o la ruta en **Ruta** como un recurso desde el que los usuarios puedan descargar el archivo de configuración de la aplicación. Al enviar las notificaciones de mensaje de texto a los usuarios, debe especificar el enlace de descarga que aparecerá en el campo **URL**.

Se recomienda copiar al portapapeles la dirección del paquete independiente creado y, a continuación, pegarla en la notificación de mensaje de correo electrónico o de texto que se destinará a los usuarios.

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 del dispositivo móvil con Kaspersky Security Center se puede realizar de las siguientes formas:

- **Por programación**. La sincronización por programación se realiza mediante el protocolo HTTP. Puede configurar la programación de sincronización en la configuración de las políticas de grupo. Las modificaciones en la configuración de la política de grupo, los comandos y las tareas se realizarán cuando el dispositivo se sincronice con Kaspersky Security Center según la programación, es decir con un retraso. De forma predeterminada, los dispositivos móviles se sincronizan automáticamente con Kaspersky Security Center cada seis horas.

  En Android 12 o una versión posterior, la aplicación puede realizar esta tarea más tarde de lo especificado si el dispositivo está en modo de ahorro de batería.

- **Forzada**. La sincronización forzada se realiza mediante notificaciones push del servicio de FCM (Firebase Cloud Messaging). La sincronización forzada se realiza principalmente para enviar comandos a un dispositivo móvil en tiempo y forma. Si desea usar la sincronización forzada, asegúrese de que los ajustes de GSM estén configurados en Kaspersky Security Center. Para obtener más información, consulte la ayuda de Kaspersky Security Center.

Para definir la configuración de sincronización de dispositivos móviles con Kaspersky Security Center, siga estos pasos:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Sincronización**.
5. Seleccione la frecuencia de sincronización en la lista desplegable **Sincronizar**.
6. Para desactivar la sincronización de un dispositivo con Kaspersky Security Center en itinerancia, seleccione la casilla **No sincronizar en roaming**.

   El usuario del dispositivo puede realizar la sincronización manualmente en la configuración de la aplicación (→ **Configuración** → **Sincronización** → **Sincronizar**).
7. Para ocultar la configuración de sincronización (dirección del servidor, puerto y grupo de administración) del usuario en la configuración de la aplicación, desactive la casilla **Mostrar la configuración de sincronización en el dispositivo**. Es imposible modificar la configuración oculta.
8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil. Puede sincronizar manualmente el dispositivo móvil usando un comando especial. Para obtener más información sobre el funcionamiento de los comandos para dispositivos móviles, consulte la *ayuda de Kaspersky Security Center*.

Activación de la aplicación 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 proporcionar la funcionalidad de **Administración de dispositivos móviles**. El objetivo de la funcionalidad **Administración de dispositivos móviles** es conectar dispositivos móviles con Kaspersky Security Center y administrarlos.

Para obtener información detallada sobre las licencias de Kaspersky Security Center y las opciones de licencia, consulte la *Ayuda de Kaspersky Security Center*.

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 móvil junto con la directiva al sincronizar el dispositivo con Kaspersky Security Center.

Si la activación de la aplicación Kaspersky Endpoint Security para Android no se completa en 30 días a partir del momento de la instalación 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 el 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 deberá sincronizar manualmente el dispositivo y Kaspersky Security Center.

Si Kaspersky Security Center no está implementado en su organización o no es accesible para los dispositivos móviles, los usuarios pueden activar la aplicación Kaspersky Endpoint Security para Android en sus dispositivos manualmente.

Para activar la aplicación Kaspersky Endpoint Security para Android, siga los siguientes pasos:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Licencia**.
5. En la sección **Obtención de licencia**, abra la lista desplegable **Clave** y seleccione la clave de activación de la aplicación requerida del almacenamiento de claves del Servidor de administración de Kaspersky Security Center.

   Los detalles de la aplicación para la cual se ha comprado la licencia aparecen en el siguiente campo.
6. Seleccione la casilla de verificación **Activar con una clave del almacenamiento de Kaspersky Security Center**.

   Si la aplicación se ha activado sin una clave almacenada en Kaspersky Security Center, Kaspersky Security para dispositivos móviles sustituye esta clave por la clave de activación seleccionada en la lista desplegable **Clave**.
7. Para activar la aplicación en el dispositivo móvil del usuario, bloquee los cambios en la configuración.
8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

   Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Instalación de un perfil de MDM para iOS

En esta sección se describen los métodos de implementación de perfiles de MDM para iOS en una red corporativa.

Antes de implementar un perfil de MDM para iOS, el administrador debe hacer lo siguiente:

1. Instalar un Servidor de MDM para iOS.
2. Obtener un certificado del servicio Apple Push Notification (certificado de APNs).
3. Instalar un certificado de APNs en el Servidor de MDM para iOS.

Para obtener más información acerca de cómo instalar un servidor de MDM para iOS y trabajar con un certificado de APNs, consulte la *ayuda de Kaspersky Security Center*.

Para obtener más información sobre la implementación de un perfil de MDM para iOS en Kaspersky Endpoint Security Cloud, consulte la *ayuda de Kaspersky Endpoint Security Cloud*.

Acerca de los modos de administración de dispositivos iOS

Puede desplegar un sistema de administración de dispositivos iOS de varias formas diferentes. El modo de administración depende del propietario del dispositivo móvil (personal o corporativo) y los requisitos corporativos de seguridad. Puede elegir el modo de administración que sea más conveniente para la empresa y usar varios modos al mismo tiempo.

Dispositivos no supervisados

Los *dispositivos iOS no supervisados* son los dispositivos personales de los empleados que se conectan a Kaspersky Security Center. En este modo, el usuario tiene permiso para usar un ID de Apple personal, trabajar con cualquier aplicación y almacenar datos personales en el dispositivo. Puede usar una directiva de grupo de Kaspersky Device Management para iOS para configurar el acceso a los recursos corporativos, la configuración de seguridad y otra configuración. De forma predeterminada, todos los dispositivos iOS no se supervisan.

Dispositivos supervisados

Los *dispositivos iOS supervisados* son los dispositivos corporativos que se conectan a Kaspersky Security Center. La configuración inicial del dispositivo móvil se realiza en Apple Configurator. *Apple Configurator* es una aplicación diseñada para preparar y configurar dispositivos iOS. Apple Configurator se instala en un equipo que ejecuta OS X. Para obtener más información sobre el funcionamiento de Apple Configurator, consulte el sitio web del Servicio de soporte técnico de Apple. Puede usar una directiva de grupo de Kaspersky Device Management para iOS para la configuración adicional. En dispositivos supervisados, puede acceder a una selección ampliada de configuración. Por ejemplo, puede configurar un proxy HTTP global y restricciones adicionales (por ejemplo, bloquear el uso de iMessage y Game Center), y puede bloquear las modificaciones de las cuentas de usuario.

Para que funcione con dispositivos iOS supervisados y no supervisados, el Servidor de dispositivos móviles de MDM de iOS debe tener un certificado de APN instalado, y un perfil de MDM de iOS debe estar instalado en los dispositivos móviles de usuarios.

Instalación a través de Kaspersky Security Center

El perfil de MDM para iOS se instala en los dispositivos móviles de usuarios cuyas cuentas de usuario se han añadido en Kaspersky Security Center. Para obtener más información sobre las cuentas de usuario en Kaspersky Security Center, consulte la *ayuda de Kaspersky Security Center*.

Para instalar un perfil de MDM para iOS:

1. En el árbol de la consola, seleccione la carpeta **Administración de dispositivos móviles → Dispositivos móviles**.
2. En el espacio de trabajo de la carpeta **Dispositivos móviles**, haga clic en el botón **Añadir dispositivo móvil**.

   Esto inicia el Asistente de Nueva conexión de dispositivo móvil. Siga las instrucciones del asistente.
3. En la ventana **Sistema operativo** del Asistente, seleccione **iOS**.
4. En la ventana del **método de protección del dispositivo iOS con MDM** del Asistente, seleccione la opción **Usar el perfil de MDM para iOS del Servidor de MDM para iOS** y especifique el perfil de MDM para iOS en la lista.

5. En la ventana **Seleccionar usuarios** del Asistente, seleccione uno o varios usuarios para la instalación del perfil de MDM para iOS en sus dispositivos móviles.

   Si el usuario no está en la lista, puede añadir una nueva cuenta de usuario sin salir del Asistente de Nueva conexión de dispositivo móvil.

6. En la ventana **Origen del certificado** del Asistente, seleccione el origen del certificado para la protección de la transferencia de datos entre el dispositivo móvil y Kaspersky Security Center:

   - **Emitir certificado mediante herramientas del Servidor de Administración**. En este caso, el certificado se creará automáticamente.

   - **Especificar el archivo del certificado**. En este caso, su propio certificado debe estar preparado con adelanto y luego seleccionarse en la ventana del Asistente. Esta opción no se puede utilizar para instalar el perfil de MDM para iOS en varios dispositivos móviles. Se debe crear un certificado independiente para cada usuario.

7. En la ventana **Método de notificación del usuario** del Asistente, seleccione el canal utilizado para reenviar el enlace de instalación de la aplicación:

   - Para enviar el enlace por correo electrónico, seleccione **Enviar enlace a perfil de MDM para iOS** y configure los ajustes en la sección **Por correo electrónico**. Asegúrese de que la dirección de correo electrónico se especifique en la configuración de cuentas de usuario.

   - Para enviar el enlace por mensaje de texto, seleccione **Enviar enlace a Perfil de MDM para iOS** y configure los ajustes en la sección **Por mensaje de texto**. Asegúrese de que el número de teléfono esté especificado en la configuración de cuentas de usuario.

   - Para instalar el perfil de MDM para iOS usando un código QR, seleccione **Mostrar enlace a paquete de instalación** y escanee el QR usando la cámara del dispositivo móvil.

   - Si ninguno de los métodos citados es conveniente, seleccione **Mostrar enlace a paquete de instalación** → **Copiar** para copiar al portapapeles el enlace de instalación del perfil de MDM para iOS. Use cualquier método disponible para distribuir el enlace de instalación de la aplicación.

8. Finalice el Asistente de Nueva conexión de dispositivo móvil.

Después de instalar el perfil de MDM para iOS en los dispositivos móviles de los usuarios, podrá ajustar la configuración de las aplicaciones usando directivas de grupo. También podrá enviar comandos a dispositivos móviles para la protección de datos en caso de que los dispositivos se pierdan o sean robados.

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

Instalación de complementos de administración

Para administrar dispositivos móviles, los complementos de administración siguientes se deben instalar en la estación de trabajo del administrador:

- El complemento de administración Kaspersky Endpoint Security para Android incluye la interfaz para administrar los dispositivos móviles y las aplicaciones móviles instaladas en ellos mediante la Consola de administración de Kaspersky Security Center.

- El complemento de administración Kaspersky Device Management para iOS ofrece una interfaz para administrar los dispositivos móviles conectados a través del servidor de MDM de iOS y el protocolo Exchange ActiveSync mediante la Consola de administración de Kaspersky Security Center.

Para instalar los complementos de administración, puede utilizar los siguientes métodos:

- Instale un complemento de administración con el Asistente de inicio rápido de Kaspersky Security Center.

  La aplicación le solicitará automáticamente que ejecute el Asistente de inicio rápido después de la instalación del Servidor de administración, a la primera conexión. También puede iniciar manualmente el Asistente de inicio rápido en cualquier momento.

  El Asistente de inicio rápido le permite aceptar los Términos y condiciones del Contrato de licencia de usuario final (EULA) para la aplicación Kaspersky Endpoint Security para Android en la Consola de administración. Si el administrador acepta los términos de Contrato de licencia en la Consola de administración, Kaspersky Endpoint Security para Android omite el paso de aceptación durante la instalación de la aplicación. Para obtener más información sobre el Asistente de inicio rápido para Kaspersky Security Center, consulte la *Ayuda de Kaspersky Security Center*.

- Instale el complemento de administración mediante la lista de paquetes de distribución disponibles en la Consola de administración de Kaspersky Security Center.

  La lista de paquetes de distribución disponibles se actualiza automáticamente después de lanzar las nuevas versiones de las aplicaciones Kaspersky.

- Descargue el paquete de distribución desde una fuente externa e instale el complemento de administración con el archivo EXE.

  Por ejemplo, el paquete de distribución del complemento de administración puede descargarse en el sitio web de Kaspersky.

Instalando los complementos de administración desde la lista en la Consola de administración

Para instalar los complementos de administración, siga los siguientes pasos:

1. En el árbol de la consola, seleccione **Avanzado → Instalación remota → Paquetes de instalación**.
2. En el espacio de trabajo, seleccione **Acciones adicionales → Ver versiones actuales de aplicaciones Kaspersky**.

   Se abre la lista de versiones actualizadas de las aplicaciones Kaspersky.
3. En la sección **Dispositivos móviles**, seleccione el complemento **Kaspersky Endpoint Security para Android** o **Kaspersky Device Management para iOS**.
4. Haga clic en el botón **Descargar paquetes de distribución**.

   Se descargará un paquete de distribución del complemento en la memoria del equipo (archivo EXE).
5. Ejecute el archivo EXE y siga las instrucciones del Asistente de instalación.

Instalando los complementos de administración desde el paquete de distribución

Para instalar el complemento de administración Kaspersky Endpoint Security para Android, siga los siguientes pasos,

Copie el archivo de instalación del complemento `klcfinst.exe` incluido en el paquete de distribución de la solución integrada y ejecútelo en la estación de trabajo del administrador.

El Asistente se encarga de la instalación y no hace falta definir la configuración.

Instalar el complemento de administración de Kaspersky Device Management para iOS,

Copie el archivo de instalación del complemento `klmdminst.exe` incluido en el paquete de distribución de la solución integrada y ejecútelo en la estación de trabajo del administrador.

El Asistente se encarga de la instalación y no hace falta definir la configuración.

Para asegurarse de que los complementos de administración se han instalado, vea la lista de complementos de administración de aplicación instalados en la ventana de propiedades del Servidor de administración, en la sección **Avanzado → Detalles de los complementos de administración instalados de la aplicación**.

Actualización de una versión anterior de la aplicación

La actualización de la aplicación debe cumplir los siguientes requisitos:

- La versión del complemento de administración de Kaspersky Endpoint Security y la versión de la aplicación móvil de Kaspersky Endpoint Security para Android deben coincidir.

  Puede ver los números de compilación de las versiones del complemento de administración y de la aplicación móvil en las Notas de la versión para Kaspersky Security para dispositivos móviles.

- Asegúrese de que Kaspersky Security Center cumpla con los requisitos del software de Kaspersky Security para dispositivos móviles.

- Los complementos de administración de Kaspersky Endpoint Security 10.0 Service Pack 2 (compilación 10.6.0.1801) y Kaspersky Device Management para iOS 10.0 Service Pack 2 (compilación 10.6.0.1767) y de las versiones posteriores se pueden actualizar automáticamente a la versión actual. Las actualizaciones de versiones anteriores de complementos de administración no se admiten.

  Para actualizar los complementos de administración de versiones anteriores, debe eliminar los complementos de administración instalados y las directivas de grupo que se crearon con ellos. A continuación instale las nuevas versiones de los complementos de administración. Para obtener más información sobre cómo eliminar complementos de administración, visite el *sitio web del Servicio de soporte técnico de Kaspersky*.

- Use la misma versión de Kaspersky Endpoint Security para Android en todos los dispositivos móviles de la organización.

Los términos y condiciones del servicio de soporte técnico para Kaspersky Security para dispositivos móviles están disponibles en el *sitio web del Servicio de soporte técnico de Kaspersky*.

Para ver la versión y número de compilación de los complementos de administración:

1. En el árbol de la consola del menú contextual del Servidor de Administración, seleccione **Propiedades**.
2. En la ventana de propiedades del Servidor de administración, seleccione **Avanzado → Detalles de los complementos de administración instalados de la aplicación**.

El espacio de trabajo muestra información sobre complementos de administración instalados en el formato `<Plug-in name> <Version> <Build>`.

Puede ver la versión y el número de compilación de la aplicación de Kaspersky Endpoint Security para Android utilizando los métodos siguientes:

- Si Kaspersky Endpoint Security para Android se instaló con un paquete de instalación independiente, puede ver la versión y el número de compilación de la aplicación en las propiedades del paquete.
- Si Kaspersky Endpoint Security para Android se instaló mediante Google Play, puede ver el número de compilación en la configuración de la aplicación (→ **Acerca de la aplicación**).

Actualización de la versión anterior de Kaspersky Endpoint Security para Android

Kaspersky Endpoint Security para Android se puede actualizar de las siguientes maneras:

- Mediante Google Play. El usuario del dispositivo móvil descarga la nueva versión de la aplicación desde Google Play y la instala en el dispositivo.
- Mediante Kaspersky Security Center. Puede actualizar remotamente la versión de la aplicación en el dispositivo mediante el sistema de administración remota de 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 Google Play

La aplicación puede actualizarse desde Google Play siguiendo el procedimiento de actualización estándar de la plataforma Android. Para actualizar la aplicación deben cumplirse las siguientes condiciones:

- El usuario del dispositivo debe tener una cuenta de Google.
- El dispositivo debe estar asociado a su cuenta de Google.
- El dispositivo debe estar conectado a Internet.

Después de descargar la aplicación desde Google Play, Kaspersky Endpoint Security para Android comprueba los Términos y condiciones de Contrato de licencia de usuario final (EULA). Si se actualizan los términos del EULA, la aplicación envía una solicitud al Kaspersky Security Center. Si el administrador acepta el EULA en la Consola de administración, Kaspersky Endpoint Security para Android omite el paso de aceptación durante la instalación de la aplicación. Si el administrador utiliza una versión obsoleta del complemento de administración, Kaspersky Security Center le solicitará que lo actualice. Cuando lo haga, el administrador podrá aceptar los términos del EULA en la Consola de administración para la aplicación Kaspersky Endpoint Security para Android.

Si Kaspersky Endpoint Security para Android se instaló desde Google Play, puede actualizar la aplicación mediante Google Play. Si la aplicación se instaló con otro método, no puede actualizarla mediante Google Play.

Actualización de la aplicación mediante Kaspersky Security Center

Kaspersky Endpoint Security para Android se puede actualizar utilizando Kaspersky Security Center tras la aplicación de una directiva de grupo. En la configuración de la directiva de grupo, puede seleccionar el paquete de instalación independiente de Kaspersky Endpoint Security para Android de la versión que cumpla los requisitos de seguridad corporativa.

Puede actualizar a través de Kaspersky Security Center si Kaspersky Endpoint Security para Android se instaló desde Kaspersky Security Center. Si se instaló desde Google Play, no puede actualizar la aplicación a través de Kaspersky Security Center.

Para actualizar Kaspersky Endpoint Security for Android usando un paquete de instalación independiente, se debe permitir la instalación de las aplicaciones desde fuentes desconocidas en el dispositivo móvil del usuario. Para obtener información sobre la instalación de aplicaciones sin Google Play, consulte la *Guía de ayuda de Android*.

Para actualizar la versión de la aplicación:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Adicional**.
5. En la sección **Actualizando Kaspersky Endpoint Security para Android**, haga clic en el botón **Seleccionar**.

   Esto abre la ventana **Actualizando Kaspersky Endpoint Security para Android**.
6. En la lista de paquetes de instalación independientes de Kaspersky Endpoint Security, seleccione el paquete cuya versión cumpla con los requisitos de seguridad corporativos.

   Puede actualizar Kaspersky Endpoint Security solo a una versión de aplicación más reciente. No se puede actualizar Kaspersky Endpoint Security a una versión de aplicación anterior.
7. Haga clic en el botón **Seleccionar**.

   Se muestra una descripción del paquete de instalación independiente seleccionado en la sección **Actualizando Kaspersky Endpoint Security para Android**.
8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil. Se le solicita al usuario del dispositivo móvil que instale la versión nueva de la aplicación. Después de que el usuario acepta, la versión nueva de la aplicación se instala en el dispositivo móvil.

Instalación de una versión anterior de Kaspersky Endpoint Security para Android

Si desea evitar la actualización automática de la aplicación y utilizar una versión específica de Kaspersky Endpoint Security para Android, desactive la actualización automática de la aplicación en la configuración de Google Play. Para obtener más información, consulte el sitio web del Soporte Técnico de Google.

La actualización automática de Kaspersky Endpoint Security para Android solo está disponible si la aplicación se instaló desde Google Play o a través de Kaspersky Security Center mediante el enlace de Google Play. Si la aplicación se instaló a través de Kaspersky Security Center mediante un enlace a su propio servidor web (mediante el paquete de instalación independiente), la actualización automática no estará disponible. En este caso, puede usar una directiva de grupo para actualizar manualmente Kaspersky Endpoint Security para Android.

Para instalar una versión anterior de Kaspersky Endpoint Security para Android:

1. Elimine Kaspersky Endpoint Security para Android de los dispositivos móviles de los usuarios.

2. Instale Kaspersky Endpoint Security para Android a través de Kaspersky Security Center utilizando un enlace a su propio servidor web. Para hacerlo, necesitará el paquete de instalación para la versión específica. Puede descargar el paquete de distribución para versiones anteriores de Kaspersky Endpoint Security para Android en el sitio web de soporte técnico de Kaspersky.

Para obtener detalles sobre las versiones anteriores de Kaspersky Endpoint Security para Android, consulte la *Ayuda para obtener la versión adecuada de Kaspersky Security para dispositivos móviles*.

Actualización de versiones anteriores de complementos de administración

Puede actualizar los complementos de administración con los siguientes métodos:

- Instale la nueva versión del complemento de administración desde la lista de paquetes de distribución disponibles en la Consola de administración de Kaspersky Security Center.

  La lista de paquetes de distribución disponibles se actualiza automáticamente después de lanzar las nuevas versiones de las aplicaciones Kaspersky.

- Descargue el paquete de distribución desde una fuente externa e instale la nueva versión del complemento de administración con el archivo EXE.

  Para actualizar los complementos de administración de Kaspersky Endpoint Security para Android y Kaspersky Device Management para iOS, debe descargar la última versión de la aplicación de la página web de Kaspersky Security para dispositivos móviles y ejecutar el Asistente de instalación de cada uno de los complementos. Las versiones anteriores de los complementos se eliminan automáticamente durante el uso del asistente de instalación.

Los expertos de Kaspersky recomiendan utilizar la misma versión de la aplicación y los complementos de administración. Si el usuario actualiza la aplicación desde Google Play, Kaspersky Security Center muestra la notificación con una indicación para actualizar el complemento de administración.

Cuando se actualizan los complementos de administración, se guardan los grupos de administración existentes de la carpeta **Dispositivos administrados** y las reglas de asignación automática de dispositivos de la carpeta **Dispositivos no asignados** de estos grupos. También se guardan las directivas de grupo de dispositivos móviles ya existentes. Las nuevas configuraciones de directiva que implementan nuevas funciones de Kaspersky Security para dispositivos móviles se agregarán a las directivas existentes y tendrán los valores predeterminados.

Si se agregaron nuevos ajustes o se cambiaron los valores predeterminados en la nueva versión del complemento de administración, los cambios se aplicarán sólo después de que se abra una directiva de grupo. Mientras el administrador no abra una política de grupo, se aplicará a los dispositivos móviles la configuración de la versión anterior del complemento, incluso si la versión del complemento se ha actualizado.

Actualizando desde la lista en la Consola de administración

Para actualizar los complementos de administración, siga los siguientes pasos:

1. En el árbol de la consola, seleccione **Avanzado → Instalación remota → Paquetes de instalación**.
2. En el espacio de trabajo, seleccione **Acciones adicionales → Ver versiones actuales de aplicaciones Kaspersky**.

   Se abre la lista de versiones actualizadas de las aplicaciones Kaspersky.
3. En la sección **Dispositivos móviles**, seleccione el complemento **Kaspersky Endpoint Security para Android** o **Kaspersky Device Management para iOS**.
4. Haga clic en el botón **Descargar paquetes de distribución**.

   Se descargará un paquete de distribución del complemento en la memoria del equipo (archivo EXE). Ejecute el archivo EXE. Siga las instrucciones del Asistente de instalación.

Actualizando desde el paquete de distribución

Para actualizar el complemento de administración Kaspersky Endpoint Security para Android, siga los siguientes pasos,

Copie el archivo de instalación del complemento `klcfinst.exe` incluido en el paquete de distribución de la solución integrada y ejecútelo en la estación de trabajo del administrador.

El Asistente se encarga de la instalación y no hace falta definir la configuración.

Para actualizar el complemento de administración de Kaspersky Device Management para iOS, siga los siguientes pasos,

Copie el archivo de instalación del complemento `klmdminst.exe` incluido en el paquete de distribución de la solución integrada y ejecútelo en la estación de trabajo del administrador.

El Asistente se encarga de la instalación del complemento y no hace falta definir la configuración.

Para asegurarse de que los complementos de administración se han actualizado, vea la lista de complementos de administración instalados de la aplicación en la ventana de propiedades del Servidor de administración, en la sección **Avanzado → Detalles de los complementos de administración instalados de la aplicación**.

Eliminación de 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 el usuario pueda eliminar la aplicación, esta acción debe habilitarse en la directiva aplicada al dispositivo.
2. Eliminación de la aplicación por parte del administrador

   El administrador elimina la aplicación remotamente usando la Consola de administración de Kaspersky Security Center. La aplicación se puede eliminar desde un dispositivo independiente o desde varios dispositivos a la vez.

Eliminación remota de la aplicación

Puede eliminar remotamente Kaspersky Endpoint Security para Android de los dispositivos móviles de los usuarios de las formas siguientes:

- Mediante una directiva de grupo. Este método es recomendable si desea eliminar la aplicación de varios dispositivos a la vez.
- Mediante la configuración de la aplicación local. Este método recomendable si desea eliminar la aplicación desde un dispositivo independiente.

Para eliminar la aplicación con una directiva de grupo:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Adicional**.
5. En la sección **Desinstalar Kaspersky Endpoint Security para Android**, seleccione la casilla **Desinstalar Kaspersky Endpoint Security para Android del dispositivo**.
6. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Como consecuencia, Kaspersky Endpoint Security para Android se elimina de los dispositivos móviles tras la sincronización con el Servidor de Administración. Los usuarios de los dispositivos móviles reciben una notificación que indica que la aplicación se ha eliminado.

Para eliminar la aplicación mediante la configuración local:

1. En el árbol de la consola, seleccione **Administración de dispositivos móviles → Dispositivos móviles**.
2. En la lista de dispositivos, seleccione el dispositivo en el que desea eliminar la aplicación.
3. Abra la ventana de propiedades del dispositivo haciendo doble clic en ella.
4. Seleccione **Aplicaciones → Kaspersky Endpoint Security para Android**.
5. Abra la ventana de propiedades de Kaspersky Endpoint Security haciendo doble clic en ella.
6. Seleccione la sección **Adicional**.
7. En la sección **Eliminación de Kaspersky Endpoint Security para Android**, seleccione la casilla **Desinstalar Kaspersky Endpoint Security para Android del dispositivo**.
8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Como consecuencia, Kaspersky Endpoint Security para Android se elimina de los dispositivos móviles tras la sincronización con el Servidor de administración. El usuario del dispositivo móvil recibe una notificación que indica que la aplicación se ha eliminado.

Permitir que los usuarios eliminen la aplicación

Para proteger la aplicación contra la eliminación en dispositivos con Android 7.0 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. Si hace esto, la aplicación no estará protegida contra la eliminación.

Puede permitir que los usuarios eliminen Kaspersky Endpoint Security para Android de sus dispositivos móviles de los modos siguientes:

- Mediante una directiva de grupo. Este método es recomendable si desea permitir a los usuarios que eliminen la aplicación de varios dispositivos a la vez.
- Mediante la configuración de la aplicación local. Este método es recomendable si se desea permitir al usuario de un dispositivo independiente que elimine la aplicación.

Para permitir la eliminación de la aplicación en una directiva de grupo:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Adicional**.
5. En la sección **Eliminación de Kaspersky Endpoint Security para Android**, configure la casilla **Permitir la eliminación de Kaspersky Endpoint Security para Android**.
6. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Como consecuencia, se permite que los usuarios eliminen la aplicación en los dispositivos móviles tras 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 permitir la eliminación de la aplicación en la configuración de la aplicación local:

1. En el árbol de la consola, seleccione **Adicional** → **Administración de dispositivos móviles** → **Dispositivos móviles**.
2. En la lista de dispositivos, seleccione el dispositivo para el que desea permitir que el usuario elimine la aplicación.
3. Abra la ventana de propiedades del dispositivo haciendo doble clic en ella.
4. Seleccione **Aplicaciones** → **Kaspersky Endpoint Security para dispositivos móviles**.
5. Abra la ventana de propiedades de Kaspersky Endpoint Security haciendo doble clic en ella.
6. Seleccione la sección **Adicional**.

7. En la sección **Eliminación de Kaspersky Endpoint Security para Android**, configure la casilla **Permitir la eliminación de Kaspersky Endpoint Security para Android**.

8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Como consecuencia, se permite que el usuario elimine la aplicación en el dispositivo móvil tras 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.

Eliminación de la aplicación 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, pulse → **Desinstalar la aplicación**.

   Aparece una solicitud de confirmación en la pantalla.

   Si el botón **Desinstalar la 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 móvil del usuario.

Configuración y administración

Esta sección de la Ayuda está destinada a especialistas que administran Kaspersky Security para dispositivos móviles, así como a especialistas que proporcionan servicio de soporte técnico a organizaciones que usan Kaspersky Security para dispositivos móviles.

Guía de inicio rápido

Esta sección describe las acciones que se recomiendan realizar para comenzar a utilizar Kaspersky Security para dispositivos móviles.

Inicio y cierre de la aplicación

Kaspersky Security Center inicia y detiene automáticamente los complementos de administración de Kaspersky Endpoint Security y Kaspersky Device Management para iOS.

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 de grupo para 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 virus planificado o sincronizar el dispositivo con Kaspersky Security Center. Este problema se puede atribuir a las funciones específicas del software integrado de estos dispositivos.

Creación de un grupo de administración

Si desea configurar de manera centralizada la aplicación Kaspersky Endpoint Security para Android instalada en los dispositivos móviles de los usuarios, debe aplicar las directivas de grupo a los dispositivos.

Para aplicar la directiva a un grupo de dispositivos, es aconsejable crear un grupo aparte para los dispositivos en la carpeta **Dispositivos administrados** antes de instalar las aplicaciones móviles en dispositivos de los usuarios.

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. Los parámetros de configuración que son comunes para todos los dispositivos utilizando una directiva de grupo.

Para crear un grupo de administración, siga estos pasos:

1. En el árbol de la consola, seleccione la carpeta **Dispositivos administrados**.
2. En el espacio de trabajo de la carpeta o subcarpeta **Dispositivos administrados**, seleccione la pestaña **Dispositivos**.
3. Haga clic en el botón **Nuevo grupo**.

   Esto abre la ventana en la cual puede crear un nuevo grupo.
4. En la ventana **Nombre del grupo**, escriba un nombre y haga clic en **Aceptar**.

   Aparecerá una nueva carpeta de grupo de administración con el nombre especificado en el árbol de la consola. Para obtener más información sobre el uso de los grupos de administración, consulte la *ayuda de Kaspersky Security Center*.

Directivas de grupo para administrar dispositivos móviles

Una *directiva de grupo* es un paquete de configuración para administrar dispositivos móviles que pertenecen a un grupo de administración y para administrar las aplicaciones móviles instaladas en los dispositivos. Puede crear una directiva de grupo por medio del Asistente de directivas.

Puede usar una directiva para cambiar la configuración tanto de dispositivos individuales como de un grupo de dispositivos. Para un grupo de dispositivos, las opciones de administración pueden configurarse en la ventana de propiedades de la directiva de grupo. Para un dispositivo individual, se pueden configurar en la ventana de configuración de la aplicación local. La configuración de administración individual especificada para un dispositivo puede diferir de los valores de las opciones configurados en la directiva para un grupo al que pertenece este dispositivo.

Cada parámetro representado en una directiva tiene un atributo de bloqueo, que muestra si la opción se puede modificar en las directivas de los niveles jerárquicos anidados (para los grupos anidados y los Servidores de administración secundarios), en la configuración de la aplicación local.

Los valores de las opciones configurados en la directiva y en la configuración de la aplicación local 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. Si el usuario ha especificado otros valores de opciones de configuración que no han sido bloqueadas, durante la siguiente sincronización del dispositivo con el Servidor de administración, los nuevos valores de las opciones de configuración se transmiten al Servidor de administración y se guardan en la configuración local de la aplicación en lugar de los valores que el administrador había especificado previamente.

Para mantener actualizada la seguridad corporativa de los dispositivos móviles, puede supervisar el cumplimiento de los dispositivos de los usuarios con la directiva de administración del grupo.

El indicador de nivel de seguridad se muestra en la parte superior de la ventana de la directiva del grupo. El indicador de nivel de seguridad le ayudará a configurar la directiva para garantizar un alto nivel de protección del dispositivo. El estado del indicador del nivel de protección cambia según la configuración de la directiva:

- **Nivel de protección alto**: se proporciona un nivel apropiado de protección del dispositivo. Todos los componentes de protección funcionan de acuerdo con las configuraciones recomendadas por Kaspersky.
- **Nivel de protección medio**: el nivel de protección es más bajo que el recomendado. Se deshabilitan algunos componentes de protección críticos (por ejemplo, Protección web). Los problemas importantes se marcan con el icono .
- **Nivel de protección bajo**: hay problemas que pueden conducir a un daño del dispositivo o pérdida de datos. Se deshabilitan algunos componentes de protección críticos (por ejemplo, se deshabilita la protección en tiempo real de dispositivos). Los problemas Críticos se marcan con el icono .

Para obtener más información sobre la gestión de las directivas y los grupos de administración en la Consola de administración de Kaspersky Security Center, consulte la *ayuda de Kaspersky Security Center*.

Creación de directivas de grupo

Esta sección describe el proceso de creación de directivas de grupo para dispositivos que tienen instalada la aplicación móvil Kaspersky Endpoint Security para Android, y para dispositivos EAS y dispositivos iOS MDM.

Las directivas creadas para un grupo de administración se muestran en el espacio de trabajo del grupo en la Consola de administración de Kaspersky Security Center en la ficha **Directivas**. Antes del nombre de la directiva, aparece un icono que muestra su estado (activo/inactivo). En un grupo, pueden crearse diversas directivas para aplicaciones diferentes. Solo una directiva para cada aplicación puede estar activa. Cuando se crea y habilita una directiva nueva, la anterior deja de estar en efecto.

Si lo desea, podrá modificar las directivas que cree.

A una directiva de grupo para administrar dispositivos móviles:

1. En el árbol de la consola, seleccione el grupo de administración para el que desee crear la directiva.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Haga clic en el vínculo **Crear directiva** para iniciar el Asistente de directivas.

Se inicia el Asistente de directivas.

Paso 1. Elección de una aplicación para crear la directiva de grupo

En este paso, seleccione la aplicación para la cual desea crear una directiva de grupo en la lista de aplicación:

- **Kaspersky Endpoint Security para Android**: para dispositivos que utilizan la aplicación móvil Kaspersky Endpoint Security para Android.

Se recomienda crear una directiva separada para dispositivos Huawei y Honor que no posean servicios de Google Play. De esta manera, se pueden enviar enlaces a Huawei AppGallery a los usuarios de dichos dispositivos.

- **Kaspersky Device Management para iOS**: para dispositivos EAS y para dispositivos MDM de iOS.

Se puede crear una directiva para dispositivos móviles si los complementos de administración Kaspersky Endpoint Security para Android y Kaspersky Device Management para iOS están instalados en el escritorio del administrador. Si no están instalados los complementos, no aparece el nombre de la aplicación pertinente en la lista de aplicaciones.

Continúe con el paso siguiente del Asistente de directivas.

Paso 2. Elección de un nombre para la directiva de grupo

En este paso, escriba el nombre para la nueva directiva en el campo **Nombre**. Si especifica el nombre de una directiva existente, se le añadirá un (1) al final de manera automática.

Continúe con el paso siguiente del Asistente de directivas.

Paso 3. Crear una directiva de grupo para la aplicación

En este paso, el asistente le solicita que seleccione el estado de la directiva:

- **Directiva activa**. El asistente guarda la directiva creada en el Servidor de administración. En la siguiente sincronización del dispositivo móvil con el Servidor de administración, la directiva se usará como directiva activa en el dispositivo.
- **Directiva 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.

Salga del asistente.

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 del dispositivo móvil con Kaspersky Security Center se puede realizar de las siguientes formas:

- **Por programación**. La sincronización por programación se realiza mediante el protocolo HTTP. Puede configurar la programación de sincronización en la configuración de las políticas de grupo. Las modificaciones en la configuración de la política de grupo, los comandos y las tareas se realizarán cuando el dispositivo se sincronice con Kaspersky Security Center según la programación, es decir con un retraso. De forma predeterminada, los dispositivos móviles se sincronizan automáticamente con Kaspersky Security Center cada seis horas.

  En Android 12 o una versión posterior, la aplicación puede realizar esta tarea más tarde de lo especificado si el dispositivo está en modo de ahorro de batería.

- **Forzada**. La sincronización forzada se realiza mediante notificaciones push del servicio de FCM (Firebase Cloud Messaging). La sincronización forzada se realiza principalmente para enviar comandos a un dispositivo móvil en tiempo y forma. Si desea usar la sincronización forzada, asegúrese de que los ajustes de GSM estén configurados en Kaspersky Security Center. Para obtener más información, consulte la ayuda de Kaspersky Security Center.

Para definir la configuración de sincronización de dispositivos móviles con Kaspersky Security Center, siga estos pasos:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Sincronización**.
5. Seleccione la frecuencia de sincronización en la lista desplegable **Sincronizar**.
6. Para desactivar la sincronización de un dispositivo con Kaspersky Security Center en itinerancia, seleccione la casilla **No sincronizar en roaming**.

   El usuario del dispositivo puede realizar la sincronización manualmente en la configuración de la aplicación (→ **Configuración** → **Sincronización** → **Sincronizar**).
7. Para ocultar la configuración de sincronización (dirección del servidor, puerto y grupo de administración) del usuario en la configuración de la aplicación, desactive la casilla **Mostrar la configuración de sincronización en el dispositivo**. Es imposible modificar la configuración oculta.
8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil. Puede sincronizar manualmente el dispositivo móvil usando un comando especial. Para obtener más información sobre el funcionamiento de los comandos para dispositivos móviles, consulte la *ayuda de Kaspersky Security Center*.

Administración de revisiones a directivas de grupo

Kaspersky Security Center le permite seguir las modificaciones de directivas de grupo. Cada vez que se guardan los cambios hechos a una directiva de grupo, se crea una *revisión*. Cada revisión tiene un número.

Puede administrar revisiones solo para directivas Kaspersky Endpoint Security para Android. No puede administrar revisiones para la política de Kaspersky Device Management para iOS.

Puede realizar las siguientes acciones en revisiones de directivas de grupo:

- Comparar una revisión seleccionada con la actual.
- Comparar revisiones seleccionadas.
- Comparar una directiva con una revisión seleccionada de otra directiva.
- Ver una revisión seleccionada.
- Deshacer cambios de directiva en una revisión seleccionada.
- Guardar las revisiones como archivo .txt.

Para obtener más información sobre cómo administrar la revisión de políticas de grupo y otros objetos (por ejemplo, cuentas de usuarios), consulte la *ayuda de Kaspersky Security Center*.

Para ver el historial de revisiones de directivas de grupo:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Historial de revisiones**.

   Se muestra una lista de revisiones de directivas. Que contiene la siguiente información:

   - El número de revisión de la directiva.
   - La fecha y la hora de modificación de la directiva.
   - El nombre del usuario que modificó la directiva.
   - La acción que se llevó a cabo en la directiva.
   - Descripción de la revisión hecha en la configuración de la directiva.

Eliminación de una directiva de grupo

Para eliminar una directiva de grupo:

1. En el árbol de la consola, seleccione el grupo de administración para el que desee eliminar la directiva.
2. En el espacio de trabajo del grupo de administración en la ficha **Directivas**, seleccione la directiva que desea eliminar.
3. En el menú contextual de la directiva, seleccione **Eliminar**.

Como resultado, se borra la directiva de grupo. Antes de que se aplique la nueva directiva de grupo, los dispositivos móviles que pertenecen al grupo de administración no dejan de trabajar con la configuración especificada en la directiva que se ha borrado.

Restricción de permisos para configurar directivas de grupo

Los administradores de Kaspersky Security Center pueden configurar los permisos de acceso de los usuarios de la Consola de administración para funciones diferentes de la solución integrada Kaspersky Security para dispositivos móviles según las tareas del trabajo de los usuarios.

En la interfaz de la Consola de administración, puede configurar derechos de acceso en la ventana de propiedades del Servidor de administración en las fichas **Seguridad** y **Funciones de usuario**. La ficha **Funciones de usuario** le permite Añadir funciones estándar de usuario 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*.

También puede configurar permisos de usuario específicos para áreas funcionales. Información sobre la correspondencia entre las áreas funcionales y fichas de directiva en el Anexo.

Para cada área funcional, el administrador puede asignar los siguientes permisos:

- **Permitir modificación**. El usuario de la Consola de administración puede cambiar la configuración de las directivas en la ventana de propiedades.
- **Bloquear modificación**. El usuario de la Consola de administración no puede cambiar la configuración de las directivas en la ventana de propiedades. Las fichas de la directiva que pertenecen al alcance funcional para el cual se ha asignado este derecho no se muestran en la interfaz.

Para obtener más información sobre la administración de derechos y funciones de usuario en la Consola de administración de Kaspersky Security Center, consulte la *ayuda de Kaspersky Security Center*.

Protección

Esta sección contiene información sobre cómo administrar remotamente la protección de dispositivos móviles en la Consola de administración de Kaspersky Security Center.

Configuración de protección antivirus en dispositivos Android

Para la detección oportuna de amenazas, virus y otras aplicaciones maliciosas, debe ajustar la configuración de la protección en tiempo real y la ejecución automática de análisis antivirus.

Kaspersky Endpoint Security para Android detecta los siguientes tipos de objetos:

- Virus, gusanos informáticos, troyanos y herramientas maliciosas
- Adware
- Aplicaciones que pueden utilizar delincuentes para dañar su dispositivo o sus datos personales

El antivirus tiene varias limitaciones:

- Cuando el antivirus se está ejecutando, una amenaza detectada en la memoria externa del dispositivo (por ejemplo, una tarjeta SD) no se puede neutralizar automáticamente en el Perfil de trabajo (Aplicaciones con el icono de un maletín, Configuración del perfil de trabajo de Android). Kaspersky Endpoint Security para Android no tiene el acceso a la memoria externa en el Perfil de trabajo. La información sobre los objetos detectados se muestra en la sección **Estado** 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 aplicación omite esos archivos sin notificarle que se omitieron.

Para ajustar la configuración de la protección en tiempo real del dispositivo móvil:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.

2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.

4. En la ventana **Propiedades** de la directiva, seleccione la sección **Protección**.

5. En la sección **Protección**, configure las opciones de protección del sistema de archivos del dispositivo móvil:

   - Para habilitar la protección en tiempo real del dispositivo móvil contra las amenazas, active la casilla **Habilitar protección**.

     Kaspersky Endpoint Security para Android analiza únicamente aplicaciones nuevas y archivos de la carpeta Descargas.

   - Para habilitar la protección extendida del dispositivo móvil contra las amenazas, active la casilla **Modo de Protección extendida**.

     Kaspersky Endpoint Security para Android analizará todos los archivos que el usuario abra, modifique, mueva, copie, inicie o guarde en el dispositivo, así como las aplicaciones móviles recién instaladas.

     > En dispositivos Android con ejecución 8.0 o posterior, Kaspersky Endpoint Security para Android analiza archivos que el usuario modifica, mueve, instala y guarda, y realiza una copia de todos los archivos. Kaspersky Endpoint Security para Android no analiza archivos cuando se abren o archivos de origen cuando se copian.

   - Para habilitar el análisis adicional de las nuevas aplicaciones antes de su primer uso en el dispositivo del usuario con la ayuda del servicio en nube de Kaspersky Security Network, seleccione la casilla **Protección en la nube (KSN)**.

   - Para bloquear adware y aplicaciones que pueden usar delincuentes para dañar el dispositivo o los datos del usuario, seleccione la casilla de verificación **Detectar adware, marcadores automáticos y aplicaciones que los delincuentes pueden utilizar para dañar el dispositivo y los datos del usuario**.

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

   - **Eliminar**

     Los objetos detectados se eliminarán automáticamente. El usuario no deberá realizar ninguna acción avanzada. Antes de eliminar un objeto, Kaspersky Endpoint Security para Android mostrará una notificación temporal para indicar la detección del objeto.

   - **Omitir**

Si las amenazas se han omitido, Kaspersky Endpoint Security para Android le advertirá al usuario sobre problemas en la protección del dispositivo. La información sobre amenazas omitidas se muestra en la sección **Estado** de la aplicación. Para cada amenaza omitida, la aplicación proporciona acciones que el usuario puede realizar para eliminar la amenaza. La lista de amenazas omitidas puede cambiar, por ejemplo, si un archivo sospechoso se eliminara o se moviera. Para recibir una lista actualizada de amenazas, ejecute un análisis completo del dispositivo. Para garantizar la protección confiable de sus datos, elimine todas las amenazas detectadas.

- **Cuarentena**

7. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Para configurar una ejecución automática de análisis antivirus en el dispositivo móvil:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Análisis**.
5. Para bloquear adware y aplicaciones que pueden usar delincuentes para dañar el dispositivo o los datos del usuario, seleccione la casilla de verificación **Detectar adware, marcadores automáticos y aplicaciones que los delincuentes pueden utilizar para dañar el dispositivo y los datos del usuario**.
6. En la lista **Acción al detectar una amenaza**, seleccione una de las siguientes opciones:

- **Eliminar**

  Los objetos detectados se eliminarán automáticamente. El usuario no deberá realizar ninguna acción avanzada. Antes de eliminar un objeto, Kaspersky Endpoint Security para Android mostrará una notificación temporal para indicar la detección del objeto.

- **Omitir**

Si las amenazas se han omitido, Kaspersky Endpoint Security para Android le advertirá al usuario sobre problemas en la protección del dispositivo. La información sobre amenazas omitidas se muestra en la sección **Estado** de la aplicación. Para cada amenaza omitida, la aplicación proporciona acciones que el usuario puede realizar para eliminar la amenaza. La lista de amenazas omitidas puede cambiar, por ejemplo, si un archivo sospechoso se eliminara o se moviera. Para recibir una lista actualizada de amenazas, ejecute un análisis completo del dispositivo. Para garantizar la protección confiable de sus datos, elimine todas las amenazas detectadas.

- **Cuarentena**

- **Preguntar al usuario**

  La aplicación Kaspersky Endpoint Security para Android muestra una notificación que le solicita al usuario que elija la acción que debe realizarse con el objeto detectado: **Omitir** o **Eliminar**.

Cuando la aplicación detecta varias amenazas, la opción **Preguntar al usuario** permite que el usuario del dispositivo aplique una acción seleccionada a cada archivo usando la casilla **Aplicar a todas las amenazas**.

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 10.0 o posterior. Kaspersky Endpoint Security para Android solicita al usuario que configure la aplicación 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.

7. La sección **Análisis programado** le permite configurar el inicio automático del análisis completo del sistema de archivos del dispositivo. Para hacer esto, haga clic en el botón **Programación** y especifique la frecuencia y el inicio del análisis completo en la ventana **Programación**.

   En Android 12 o una versión posterior, la aplicación puede realizar esta tarea más tarde de lo especificado si el dispositivo está en modo de ahorro de batería.

8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil. 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 de antivirus.

De manera predeterminada, las actualizaciones de la base de datos antivirus se deshabilitan cuando el dispositivo está en roaming. No se realizan actualizaciones programadas de las bases de datos antivirus.

Para configurar las actualizaciones de la base de datos antivirus:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Actualización de bases de datos**.
5. 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 roaming, seleccione la casilla **Permitir actualizaciones de bases de datos en roaming** de la sección **Actualización de bases de datos en roaming**.

   Aunque la casilla esté desactivada, el usuario podrá iniciar manualmente una actualización de la base de datos antivirus cuando el dispositivo está en roaming.

6. En la sección **Origen de actualizaciones de bases de datos**, especifique el origen de las actualizaciones desde donde Kaspersky Endpoint Security para Android recibe e instala las actualizaciones de las bases de datos antivirus:

   - **Servidores de Kaspersky**

Utilización de un servidor de actualización Kaspersky como origen de actualizaciones para descargar las bases de datos de Kaspersky Endpoint Security para Android en los dispositivos móviles de los usuarios. Para actualizar las bases de datos desde los servidores de Kaspersky, Kaspersky Endpoint Security for Android transmite datos a Kaspersky (por ejemplo, el ID de la tarea de actualización misma). La lista de datos que se transmite durante las actualizaciones de la base de datos se indica en el Contrato de licencia de usuario final.

- **Servidor de administración**

  Utilización del repositorio del servidor de administración de Kaspersky Security Center como origen de actualizaciones para descargar las bases de datos de Kaspersky Endpoint Security para Android en los dispositivos móviles de los usuarios.

- **Otro origen**

  Utilización de un servidor de terceros como origen de actualizaciones para descargar las bases de datos de Kaspersky Endpoint Security para Android en los dispositivos móviles de los usuarios. Para iniciar una actualización, debe introducir la dirección de un servidor HTTP en el campo siguiente (p. ej., http://domain.com/).

7. En la sección **Actualización de la base de datos programada**, configure las opciones para actualizaciones automáticas de la base de datos antivirus en el dispositivo del usuario. Para hacer esto, haga clic en el botón **Programación** y especifique la frecuencia y el horario de inicio de las actualizaciones en la ventana **Programación**.

   En Android 12 o una versión posterior, la aplicación puede realizar esta tarea más tarde de lo especificado si el dispositivo está en modo de ahorro de batería.

8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Protección de dispositivos Android en Internet

Para proteger los datos personales de un usuario del dispositivo móvil en Internet, habilite Protección web. El componente Protección web bloquea los sitios web maliciosos que distribuyen un código malicioso y los sitios web de phishing diseñados para robar sus datos confidenciales y acceder a sus cuentas financieras. Protección web utiliza el servicio en la nube de Kaspersky Security Network para analizar sitios web antes de abrirlos. La Protección web también le permite configurar el acceso del usuario a sitios web en función de listas predefinidas de sitios web permitidos y bloqueados.

Se debe configurar Kaspersky Endpoint Security para Android como una función de accesibilidad. Kaspersky Endpoint Security para Android solicita al usuario que configure la aplicación 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.

La Protección web en los dispositivos Android solo funciona en el navegador Google Chrome (incluida la función de Pestañas personalizadas), el navegador Huawei y el navegador de Internet de Samsung. La Protección web para el Navegador de Samsung no bloquea sitios en un dispositivo móvil si se utiliza un perfil de trabajo y la Protección web está habilitada solo para el perfil de trabajo.

Habilitar Protección web en Google Chrome y en los navegadores de Huawei y Samsung:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.

2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.

4. En la ventana **Propiedades** de la directiva, seleccione **Protección web**.

5. Para usar la Protección web, usted o el usuario del dispositivo deben leer y aceptar la Declaración sobre el procesamiento de datos para usar Protección web (Declaración de Protección web):

   a. Haga clic en el vínculo **Declaración de Protección web**.

   Se abrirá la ventana **Declaración sobre el procesamiento de datos para usar Protección web**. Para aceptar la Declaración de protección web, debe leer y aceptar la Directiva de privacidad.

   b. Haga clic en el vínculo de la Directiva de privacidad. Lea y acepte la Directiva de privacidad.

   Si no acepta la Directiva de privacidad, el usuario del dispositivo móvil puede aceptar la Directiva de privacidad en el Asistente de configuración inicial o en la app (→ **Acerca de** → **Términos y condiciones** → **Política de privacidad**).

   c. Seleccione el modo de aceptación de la Declaración de protección web:

   - **He leído y acepto la Declaración de protección web**
   - **Solicitar al usuario del dispositivo que acepte la Declaración de Protección web**
   - **No acepto la Declaración de protección web**

6. Si selecciona **No acepto la Declaración de protección web**, la Protección web no bloquea los sitios en el dispositivo móvil. El usuario del dispositivo móvil no puede habilitar la Protección web en Kaspersky Endpoint Security.

7. Active la casilla **Habilitar Protección web**.

8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Protección de datos de dispositivos robados o perdidos

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.

Envío de comandos a un dispositivo móvil

Para proteger los datos de un dispositivo móvil perdido o robado, puede enviar los siguientes comandos especiales (consulte la siguiente tabla).

Comandos para proteger datos de un dispositivo perdido o robado

Método de	Comando	Resultado de la ejecución del comando

comunicación con Kaspersky Security Center		
Kaspersky Endpoint Security para Android	Bloquear	El dispositivo móvil se bloquea.
	Desbloquear	Después de desbloquear un dispositivo móvil con Android 5.0 a 6.X, la contraseña de desbloqueo de pantalla (el código PIN) se restablece en "1234". Después de desbloquear un dispositivo con Android 7.0 o posterior, la contraseña de desbloqueo de pantalla no se cambia.
	Localizar dispositivo	Se localiza el dispositivo y se muestra su ubicación en Google Maps. El proveedor de servicios móviles cobra una tarifa por enviar SMS y por el acceso a Internet. 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 no más de 30 minutos antes. De lo contrario, el comando **Localizar dispositivo** falla.
	Foto de identificación	El dispositivo móvil se bloquea. La foto de identificación se toma con la cámara frontal del dispositivo cuando alguien intenta desbloquear el dispositivo. El proveedor de servicios móviles cobra una tarifa por enviar SMS y por el acceso a Internet. Cuando el usuario intenta desbloquear el dispositivo, automáticamente consiente la foto de identificación. Si se revocó el permiso para usar la cámara, el dispositivo móvil muestra una notificación y le pide que proporcione el permiso. En un dispositivo móvil con Android 12 o posterior, si se revocó el permiso para usar la cámara a través de la Configuración rápida, la notificación no se muestra, pero la foto tomada es negra.
	Alarma	El dispositivo móvil suena como una alarma. La alarma suena durante 5 minutos o durante 1 minuto si la batería del dispositivo es baja.
	Eliminar datos corporativos	Eliminar datos transportados en contenedores, cuenta de correo electrónico corporativa, configuración para conectarse a la red Wi-Fi corporativa y VPN, nombre del punto del acceso (APN), perfil de trabajo de Android, contenedor KNOX y la clave del administrador de licencias KNOX.
	Restablecer la configuración de fábrica	Todos los datos se eliminan del dispositivo móvil y la configuración se restablece a sus valores de fábrica. Después de que este comando se ejecute, el dispositivo no podrá recibir o ejecutar comandos subsecuentes.
Perfil de MDM para	Bloquear	El dispositivo móvil se bloquea.

iOS	Desbloquear	El bloqueo del dispositivo móvil con un código PIN está deshabilitado. Se ha restablecido el código PIN anteriormente especificado.
	Eliminar datos corporativos	Todos los perfiles de configuración instalados, los perfiles de aprovisionamiento, el perfil de MDM para iOS y las aplicaciones para las que se ha seleccionado la casilla **Eliminar junto con el perfil de MDM para iOS** se eliminan del dispositivo.
	Restablecer la configuración de fábrica	Todos los datos se eliminan del dispositivo móvil y la configuración se restablece a sus valores de fábrica. Después de que este comando se ejecute, el dispositivo no podrá recibir o ejecutar comandos subsecuentes.
Buzón de correo de Exchange	Restablecer la configuración de fábrica	Todos los datos se eliminan del dispositivo móvil y la configuración se restablece a sus valores de fábrica. Después de que este comando se ejecute, el dispositivo no podrá recibir o ejecutar comandos subsecuentes.

Se requieren los permisos y derechos especiales para la ejecución de 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 desactivar estos permisos en la configuración del dispositivo más adelante. Si este es el caso, será imposible ejecutar comandos.

En dispositivos con Android 10.0 o posterior, el usuario debe otorgar el permiso "Todo el tiempo" para la acceder a la ubicación. En dispositivos con Android 11.0 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 de esta limitación y se le volverá a pedir que otorgue los permisos del nivel requerido. 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 más información sobre el envío de comandos desde la lista de dispositivos móviles de la Consola de administración, consulte la *ayuda de Kaspersky Security Center*.

Desbloqueo de un dispositivo móvil

Puede desbloquear un dispositivo móvil usando los siguientes métodos:

- Envíe el comando de desbloqueo de dispositivo móvil.
- Introduzca el código de un solo uso para desbloquear el dispositivo (solo para dispositivos de 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 desbloqueo de un solo uso. No puede usar comandos para desbloquear el dispositivo.

Para obtener más información sobre el envío de comandos desde la lista de dispositivos móviles de la Consola de administración, consulte la *ayuda de Kaspersky Security Center*.

Un *código de desbloqueo de un solo uso* es un código de aplicación secreto para desbloquear el dispositivo móvil. El código de un solo uso lo genera la aplicación y es exclusivo de cada dispositivo móvil. Puede cambiar el largo del código de un solo uso (4, 8 o 16 dígitos) en la configuración de directiva de grupo en la sección **Antirrobo**.

Para abrir el dispositivo móvil con un código de un solo uso:

1. En el árbol de la consola, seleccione **Administración de dispositivos móviles → Dispositivos móviles**.
2. Seleccione un dispositivo móvil para el cual desea recibir un código de desbloqueo de un solo uso.
3. Abra la ventana de propiedades del dispositivo móvil haciendo doble clic.
4. Seleccione **Aplicaciones → Kaspersky Endpoint Security para Android**.
5. Abra la ventana de propiedades de Kaspersky Endpoint Security haciendo doble clic en ella.
6. Seleccione la sección **Antirrobo**.
7. Se muestra un código único para el dispositivo seleccionado en el campo **Código de un solo uso** de la sección **Código de un solo uso para desbloquear el dispositivo**.
8. Use cualquier método disponible (por ejemplo, correo electrónico) para comunicar el código de un solo uso al usuario del dispositivo bloqueado.
9. El usuario ingresa el código de un solo uso en la pantalla del dispositivo bloqueado por Kaspersky Endpoint Security para Android.

El dispositivo móvil se desbloqueará. Después de desbloquear un dispositivo móvil con Android 5.0 a 6.X, la contraseña de desbloqueo de pantalla (el código PIN) se restablece en "1234". Después de desbloquear un dispositivo con Android 7.0 o posterior, la contraseña de desbloqueo de pantalla no se cambia.

Cifrado de datos

Para proteger los datos contra el acceso no autorizado, debe activar el cifrado de todos los datos del dispositivo (por ejemplo, datos de las cuentas del usuario, aplicaciones y dispositivos externos, así como mensajes de correo electrónico, mensajes de texto, contactos, fotografías y otros archivos). Para acceder a los datos cifrados, debe especificar una clave especial: la contraseña de desbloqueo del dispositivo. Si se cifran los datos, solo se puede acceder a ellos cuando se desbloquea el dispositivo.

El cifrado de datos se activa de forma predeterminada en dispositivos con iOS bloqueados por una contraseña (**Configuración → Touch ID / Face ID y contraseña → Activar contraseña)**.

Para cifrar todos los datos en un dispositivo Android:

1. Active el bloqueo de pantalla en el dispositivo Android (**Configuración → Seguridad → Bloqueo de pantalla**).
2. Configure una contraseña de desbloqueo del dispositivo que cumpla los requisitos de seguridad corporativa.

   No se recomienda usar un patrón de desbloqueo para desbloquear el dispositivo. En determinados dispositivos Android con sistema operativo Android 6.0 o posterior, después de cifrar los datos y reiniciar el dispositivo, debe escribir una contraseña numérica para desbloquear el dispositivo en lugar de un patrón de desbloqueo. Este problema está relacionado con el funcionamiento del servicio de funciones de accesibilidad. Para desbloquear la pantalla del dispositivo en este caso, convierta el patrón de desbloqueo en una contraseña numérica. Para obtener más información sobre la conversión de un patrón de desbloqueo en una contraseña numérica, consulte el sitio web del Servicio de soporte técnico del fabricante del dispositivo móvil.

3. Active el cifrado de todos los datos del dispositivo (**Configuración → Seguridad → Cifrar datos**).

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, se debe configurar una contraseña que se le solicita al usuario cuando el dispositivo sale del modo de reposo.

Puede imponer restricciones a la actividad del usuario en el dispositivo si la contraseña de desbloqueo es débil (por ejemplo, bloqueo del dispositivo). Puede imponer restricciones usando el componente Control de cumplimiento. Para hacer esto, en la configuración de regla de análisis, debe seleccionar el criterio **La contraseña de desbloqueo no cumple con los requisitos de seguridad**.

En ciertos dispositivos Samsung con Android 7.0 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.

Para configurar una contraseña de desbloqueo:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Administración del dispositivo**.
5. Si desea que la aplicación compruebe si se estableció una contraseña de desbloqueo, seleccione la casilla **Exigir que se defina una contraseña de desbloqueo de pantalla** en la sección **Bloqueo de pantalla**.

   Si la aplicación detecta que no se ha establecido 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 el mínimo de caracteres.

   Número mínimo de caracteres que tiene la contraseña del usuario. Valores posibles: entre 4 y 16 caracteres.

   De forma predeterminada, la contraseña del usuario tiene una longitud de cuatro caracteres.

   En dispositivos con Android 10.0 o posterior, Kaspersky Endpoint Security establece los requerimientos de seguridad de la contraseña en uno de los sistemas de valores: media o alta.

   Los valores para dispositivos con Android 10.0 o posterior se determinan en base a las siguientes reglas:

- 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 o numérica (PIN) con una secuencia que no tenga números repetidos u ordenados (por ejemplo, 1234), o alfabética/alfanumérica. El PIN o contraseña debe tener al menos 4 caracteres de extensión.

- 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 alfabética/alfanumérica (contraseña). La extensión del PIN debe ser de al menos 8 dígitos; la contraseña debe contar con al menos 6 caracteres.

7. Si desea que el usuario tenga la capacidad de usar huellas digitales para desbloquear la pantalla, seleccione la casilla **Permitir el uso de huellas dactilares**. Si la contraseña de desbloqueo no cumple con los requisitos de seguridad corporativa, no se puede usar un escáner de huellas digitales para desbloquear la pantalla.

   En dispositivos con Android 10.0 o posterior, el uso de la huella digital para desbloquear la pantalla solo puede configurarse para un perfil de trabajo.

   Kaspersky Endpoint Security para Android no restringe el uso de un escáner de huellas digitales para iniciar sesión en aplicaciones o confirmar compras.

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

   Después de añadir una huella digital en la configuración del dispositivo, el usuario puede desbloquear la pantalla usando los siguientes métodos:

   - Presionar el dedo en el escáner de huellas digitales (método principal).

   - Escribir la contraseña de desbloqueo (método secundario).

8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Configuración de una contraseña de desbloqueo segura para dispositivos iOS con MDM

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. Una *contraseña sencilla* es una contraseña que contiene caracteres sucesivos o repetitivos, por ejemplo: "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 para una contraseña de desbloqueo de dispositivos iOS con MDM:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.

2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.

4. En la ventana **Propiedades** de la directiva, seleccione la sección **Contraseña**.

5. En la sección **Configuración de contraseña**, active la casilla **Aplicar configuración en el dispositivo**.

6. Configure las opciones de seguridad de la contraseña de desbloqueo:

   - Para permitir al usuario utilizar una contraseña sencilla, active la casilla **Permitir contraseña sencilla**.
   - 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 el campo **Duración máxima de la contraseña**, especifique el período en días durante el cual la contraseña permanece vigente. Cando caduca este periodo, Kaspersky Device Management para iOS solicita al usuario que cambie la contraseña.
   - En la lista **Activar Bloqueo automático en**, seleccione la cantidad de tiempo después del cual el bloqueo automático del dispositivo iOS con MDM debe habilitarse.
   - En el campo **Historial de contraseñas**, especifique la cantidad de contraseñas utilizadas (incluida la actual) que Kaspersky Device Management compara con la nueva contraseña cuando el usuario cambia la contraseña. Si las contraseñas coinciden, se rechaza la nueva contraseña.
   - En la lista **Plazo máximo para desbloqueo sin contraseña**, seleccione la cantidad de tiempo durante la cual el usuario puede desbloquear el dispositivo iOS con MDM sin ingresar la contraseña.
   - En **Máximo de intentos de acceso**, seleccione la cantidad de intentos de acceso que el usuario puede realizar para escribir la contraseña de desbloqueo del dispositivo iOS con MDM.

7. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Como resultado, luego de que se implementa la directiva, Kaspersky Device Management 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 contraseña de desbloqueo segura para dispositivos EAS

Establezca una contraseña de desbloqueo segura para proteger la información de los dispositivos EAS.

De forma predeterminada, cuando se enciende un dispositivo móvil, Kaspersky Device Management para iOS no solicita al usuario que ingrese o establezca una contraseña de desbloqueo.

Para configurar las opciones de seguridad para una contraseña de desbloqueo de dispositivos EAS:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de EAS pertenecen.

2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.

4. En la ventana Propiedades de la directiva, seleccione la sección **Contraseña**.

5. En la sección **Configuración de contraseña**, active la casilla **Solicitar contraseña**.

6. Configure las opciones de seguridad de la contraseña de desbloqueo:

   - Para solicitar al usuario que utilice letras y números en la contraseña, active la casilla **Solicitar valor alfanumérico**. En el campo **Mínimo de caracteres**, especifique el nivel de seguridad de la contraseña alfanumérica. Valores posibles: de 1 a 4. El valor "1" corresponde al nivel de seguridad más bajo.

   - Para permitir al usuario utilizar la función de recuperación de contraseña, active la casilla **Permitir recuperación de contraseña**.

   - Si desea que los archivos se cifren en la memoria del dispositivo, active la casilla **Exigir cifrado de dispositivo**.

   - Si desea que los archivos se cifren en la tarjeta de memoria, active la casilla **Exigir cifrado de la tarjeta de memoria**.

   - Para permitir al usuario utilizar una contraseña sencilla que consiste solamente de números, active la casilla **Permitir contraseña sencilla**.

   - Para limitar la cantidad de intentos de ingresar la contraseña para acceder al dispositivo, active la casilla **Máximo de intentos de acceso**. En el campo ubicado a la derecha de la casilla, especifique la cantidad de intentos de ingreso de contraseña que el usuario tiene para desbloquear el dispositivo. Si el usuario no ingresa la contraseña correcta en la cantidad de intentos consecutivos especificada, Kaspersky Device Management para iOS elimina toda la información del dispositivo.

   - Para especificar la longitud mínima de la contraseña del usuario, active la casilla **Longitud mínima de la contraseña**. Especifique la cantidad mínima de caracteres de la contraseña en el campo ubicado a la derecha de la casilla. Valores posibles: entre 4 y 16 caracteres.

   - Para solicitarle al usuario que escriba la contraseña después de que el dispositivo ha estado inactivo durante algún tiempo, active la casilla **Espera hasta nuevo intento de escribir la contraseña (min)**. En el campo ubicado a la derecha de la casilla, especifique el período de inactividad en minutos. Cando este período expira, la aplicación solicita al usuario que escriba la contraseña.

   - Para limitar el período de validez de la contraseña, active la casilla **Período de validez de la contraseña (días)**. En el campo ubicado a la derecha de la casilla, especifique el período de validez de la contraseña. Cando este período expira, la aplicación solicita al usuario que cambie la contraseña.

   - En el campo **Historial de contraseñas**, puede especificar la cantidad de contraseñas anteriores más recientes que no se pueden volver a utilizar.

7. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil. Una vez que se aplica la directiva, Kaspersky Device Management para iOS verifica si una contraseña está establecida en el dispositivo móvil del usuario. Si la contraseña de desbloqueo no se ha establecido en el dispositivo, se solicita al usuario que lo haga. La contraseña debe establecerse teniendo en cuenta la configuración de la directiva. Si la contraseña de desbloqueo del dispositivo está establecida pero 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 manera segura un dispositivo Android a redes Wi-Fi y proteger la transferencia de datos, debería ajustar la configuración para VPN (Red privada virtual).

La configuración de VPN solo es posible para dispositivos Samsung.

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 red privada virtual 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 la conexión VPN, se deben configurar opciones adicionales en el primer inicio. Para configurar opciones, la conexión VPN debe estar permitida en las opciones de la aplicación.

Para configurar la VPN en un dispositivo móvil del usuario:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Administrar Samsung KNOX → Administrar dispositivos Samsung**.
5. En la sección **VPN**, haga clic en el botón **Configurar**.

   Esto abre la ventana **Red VPN**.
6. En la lista desplegable **Tipo de conexión**, seleccione el tipo de conexión VPN.
7. En el campo **Nombre de red**, escriba el nombre del túnel VPN.
8. En el campo **Dirección del servidor**, escriba el nombre de la red o la dirección IP del servidor VPN.
9. En la lista **Dominio(s) de búsqueda DNS**, escriba el dominio de búsqueda DNS que se añadirá automáticamente al nombre del servidor DNS.

   Puede especificar varios dominios DNS separándolos con espacios en blanco.
10. 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.
11. 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 de la VPN.

12. También configure las siguientes opciones para las redes de tipo **IPSec Xauth PSK** y **L2TP IPSec PSK**:

    a. En el campo **Clave compartida IPSec**, escriba la contraseña de la clave de seguridad preestablecida IPSec.

    b. En el campo **ID de IPSec**, escriba el nombre del usuario del dispositivo móvil.

13. Para una red **L2TP IPSec PSK**, además puede especificar la contraseña para la clave L2TP en el campo **Clave L2TP**.

14. Para una red **PPTP**, seleccione la casilla **Usar 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.

15. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Configuración de VPN en dispositivos iOS con MDM

Para conectar el dispositivo iOS con MDM a una red privada virtual y proteger la información durante la conexión a la VPN, configure las opciones de conexión a la VPN.

Para configurar la conexión a la VPN en el dispositivo iOS con MDM de un usuario:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.

2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.

4. En la ventana **Propiedades** de la directiva, seleccione la sección **VPN**.

5. Haga clic en el botón **Agregar** en la sección **Redes VPN**.

   Esto abre la ventana **Red VPN**.

6. En el campo **Nombre de red**, escriba el nombre del túnel VPN.

7. En la lista desplegable **Tipo de conexión**, seleccione el tipo de conexión VPN:

   - **L2TP** (Protocolo de Túnel de capa 2). La conexión admite autenticación del usuario de un dispositivo móvil iOS con MDM mediante contraseña MS-CHAP v2, autenticación de dos factores y autenticación automática utilizando una clave pública.

   - **PPTP** (Protocolo de túnel punto a punto). La conexión admite autenticación del usuario de un dispositivo móvil iOS con MDM mediante contraseña MS-CHAP v2 y autenticación de dos factores.

   - **IPSec (Cisco)**. 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. La configuración de la conexión VPN instala la aplicación Cisco AnyConnect desde App Store en el dispositivo móvil iOS con MDM.

- **Juniper SSL**. La conexión admite Juniper Networks SSL VPN gateway, 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 móvil iOS con MDM.

- **F5 SSL**. La conexión admite F5 BIG-IP Edge Gateway, Administrador de la directiva de acceso y soluciones Fire SSL para VPN. Para configurar la conexión VPN, instale la aplicación para clientes F5 BIG-IP Edge desde App Store en el dispositivo móvil iOS con MDM.

- **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, E-Class NSA con SonicOS de versión 5.8.1.0 o posterior. Para configurar la conexión VPN, instale la aplicación SonicWALL Mobile Connect desde App Store en el dispositivo móvil iOS con MDM.

- **Aruba VIA**. La conexión admite controladores de acceso al móvil Aruba. Para configurar la conexión VPN, instale la aplicación Aruba Networks VIA desde App Store en el dispositivo móvil iOS con MDM.

- **SSL personalizada**. La conexión admite autenticación del usuario de un dispositivo móvil iOS con MDM mediante contraseñas y autenticación de dos factores.

8. En el campo **Dirección del servidor**, escriba el nombre de la red o la dirección IP del servidor VPN.

9. En el campo **Nombre de la cuenta**, escriba el nombre de la cuenta para la autorización en el servidor VPN. Puede usar las macros de la lista desplegable **Macros disponibles**.

10. Configure las opciones de seguridad para la conexión VPN de acuerdo con el tipo de red privada virtual seleccionada.

11. De ser necesario, configure las opciones de la conexión VPN a través de un servidor proxy:

    a. Seleccione la ficha **Configuración de servidor proxy**.

    b. Seleccione el modo de configuración del servidor proxy y especifique las opciones de conexión.

    c. Haga clic en **Aceptar**.

    Como resultado, en el dispositivo iOS con MDM, se configuran las opciones de la conexión del dispositivo a una VPN a través de un servidor proxy.

12. Haga clic en **Aceptar**.

    La nueva VPN se muestra en la lista.

13. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Como resultado, luego de que se aplica la directiva, se configura una conexión VPN en el dispositivo iOS con MDM 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.

Para configurar el firewall en un dispositivo móvil:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Administrar Samsung KNOX → Administrar dispositivos Samsung**.
5. En la ventana **Firewall**, haga clic en **Configurar**.

   Se abre la ventana **Firewall**.
6. Seleccione el modo de firewall:
   - Para permitir todas las conexiones entrantes y salientes, mueva el cursor hacia **Permitir todas**.
   - Para que la aplicación bloquee toda la actividad de red excepto la actividad de las aplicaciones que se encuentran en la lista de exclusiones, mueva el cursor hacia **Bloquear todas, salvo las excepciones**.
7. Si ha configurado el modo del firewall en **Bloquear todas, salvo las excepciones**, cree una lista de exclusiones:
   a. Haga clic en **Agregar**.

      Esto abre la ventana **Exclusión del firewall**.
   b. En el campo **Nombre de la aplicación**, 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 **Aceptar**.
8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Protección de Kaspersky Endpoint Security para Android contra eliminación

Para protección del dispositivo móvil y cumplimiento de 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 7.0 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.

Para habilitar la protección contra la eliminación de Kaspersky Endpoint Security para Android:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Adicional**.
5. En la sección **Eliminación de Kaspersky Endpoint Security para Android**, anule la selección de la casilla **Permitir la eliminación de Kaspersky Endpoint Security para Android**.

   Para proteger la aplicación contra la eliminación en dispositivos con Android 7.0 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. Si hace esto, la aplicación no estará protegida contra la eliminación.

6. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

   Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil. Si se hace un intento de eliminar la aplicación, el dispositivo móvil se bloqueará.

Detección de ataques de hackers en el dispositivo (root)

Kaspersky Security para dispositivos móviles le permite detectar ataques de hackers al dispositivo (root). Los archivos de sistema están desprotegidos en un dispositivo atacado por hackers y, por lo tanto, pueden ser modificados. Además, las aplicaciones de otras empresas de fuentes desconocidas se podrían instalar en dispositivos atacados. Después de la detección de un intento de ataque de hackers, recomendamos que inmediatamente restaure el funcionamiento normal del dispositivo.

Para detectar cuando un usuario obtiene privilegios root, Kaspersky Endpoint Security para Android usa los siguientes servicios:

- *El servicio incorporado de Kaspersky Endpoint Security para Android* es un servicio de Kaspersky que comprueba si un usuario del dispositivo móvil ha obtenido privilegios root (Kaspersky Mobile Security SDK).
- *La Certificación de SafetyNet* es un servicio de Google que comprueba la integridad del sistema operativo, analiza el hardware del dispositivo y software, e identifica otros problemas de seguridad. Para obtener más información sobre la Certificación de SafetyNet, visite el sitio web del Soporte Técnico de Android.

Si el dispositivo se corta, recibe una notificación. Puede ver notificaciones de ataques de hackers en el espacio de trabajo del Servidor de administración en la ficha **Supervisión**. 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 en el dispositivo si el dispositivo es atacado (por ejemplo, bloquee el dispositivo). Puede imponer restricciones con el componente Control de cumplimiento (consulte la siguiente figura). Para hacer esto, en la configuración de regla de análisis, seleccione el criterio **El dispositivo ha sido rooteado**.

Configuración de un proxy HTTP global en dispositivos iOS con MDM

Para proteger el tráfico de Internet del usuario, configure la conexión del dispositivo iOS con MDM a Internet a través del servidor proxy.

La conexión automática a Internet a través de un servidor proxy está disponible solo para dispositivos controlados.

Para configurar las opciones del proxy HTTP global en el dispositivo iOS con MDM del usuario:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Proxy HTTP global**.
5. En la sección **Configuración de proxy HTTP global**, active la casilla **Aplicar configuración en el dispositivo**.
6. Seleccione el tipo de configuración de proxy HTTP global.

   De forma predeterminada, el tipo manual de proxy HTTP global está seleccionado y el usuario no puede conectarse a redes cautivas sin conectarse a un servidor proxy. Las *redes cautivas* son redes inalámbricas que requieren autenticación preliminar del dispositivo móvil sin conectarse a un servidor proxy.

   - Para especificar la configuración de conexión al servidor proxy manualmente:
     a. En la lista desplegable **Tipo de configuración de proxy**, seleccione **Manual**.
     b. En el campo **Dirección y puerto del servidor proxy**, 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**, establezca el nombre de la cuenta de usuario para la autorización del servidor proxy. Puede usar las macros de la lista desplegable **Macros disponibles**.
     d. En el campo **Contraseña**, establezca la contraseña de la cuenta de usuario para la autorización del servidor proxy.
     e. Para permitir al usuario acceder a redes cautivas, active 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 lista desplegable **Tipo de configuración de proxy**, seleccione **Automático**.
     b. En el campo **URL del archivo PAC**, escriba la dirección web del archivo PAC (por ejemplo: http://www.ejemplo.com/nombredearchivo.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, active la casilla **Permitir conexión directa si no se puede acceder al archivo PAC**.

d. Para permitir al usuario acceder a redes cautivas, active la casilla **Permitir acceso a redes cautivas sin conectarse al servidor proxy**.

7. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Como resultado, luego de que se aplica la directiva, el usuario del dispositivo móvil se conecta a Internet a través de un servidor proxy.

Adición de certificados de seguridad a dispositivos iOS con MDM

Para simplificar la autenticación del usuario y garantizar la protección de información, agregue certificados en el dispositivo iOS con MDM del usuario. La información firmada con un certificado se protege contra modificaciones durante el intercambio de red. El cifrado de información mediante un certificado brinda un nivel adicional de protección de información. El certificado también se puede utilizar para verificar la identidad del usuario.

Device Management del Kaspersky para iOS admite los siguientes estándares de certificación:

- **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 añadir un certificado de seguridad en el dispositivo iOS con MDM de un usuario:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Certificados**.
5. Haga clic en el botón **Agregar** en la sección **Certificados**.

   Se abre la ventana **Certificado**.
6. En el campo **Nombre del archivo**, especifique la ruta al certificado:

   Los archivos de los certificados PKCS#1 tienen la extensión cer, crt o der. Los archivos de los certificados PKCS#12 tienen la extensión p12 o pfx.
7. Haga clic en **Abierta**.

   Si el certificado está protegido con contraseña, especifique la contraseña. El nuevo certificado aparece en la lista.
8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Como resultado, luego de que se aplica la directiva, se le solicitará al usuario que instale certificados de la lista que se ha creado.

Adición de perfiles SCEP a dispositivos iOS con MDM

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 separados por 10 segundos para sondear el servidor SCEP. Si todos los intentos para firmar el certificado fallaron, debe generar una nueva solicitud de firma de certificado.
- El certificado que se ha recibido no se puede usar para firmar o cifrar información.

Puede editar la configuración especificada cuando agrega el perfil SCEP.

Para añadir un perfil SCEP:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **SCEP**.
5. Haga clic en el botón **Agregar** en la sección **Perfiles de SCEP**.

   Se abre la ventana **Perfil de SCEP**.
6. En el campo **Dirección web 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.
7. En el campo **Nombre**, escriba el nombre del Centro de certificación implementado en el servidor SCEP.
8. En el campo **Asunto**, escriba una cadena con los atributos del usuario del dispositivo iOS con MDM que se incluyen en el certificado X.500.

   Los atributos pueden contener detalles del país (C), organización (O) y nombre común del usuario (CN). Por ejemplo: /C=ES/O=MiEmpresa/CN=Usuario/. También puede usar otros atributos especificados en el RFC 5280.
9. En la lista desplegable **Tipo de nombre alternativo del titular**, seleccione el tipo de nombre alternativo del titular del servidor SCEP:

   - **No** – no se utiliza un nombre alternativo para identificación.
   - **Nombre RFC 822** – identificación utilizando la dirección de correo electrónico. La dirección de correo electrónico debe ser especificada de acuerdo al RFC 822.
   - **Nombre DNS** – identificación utilizando el nombre de dominio.

- **URI** – identificación utilizando la dirección IP o la dirección en formato FQDN.

Puede usar un nombre alternativo del titular para identificar al usuario del dispositivo móvil iOS con MDM.

10. En el campo **Nombre alternativo del titular**, 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.

11. En el campo **Nombre del titular NT**, escriba el nombre DNS del usuario del dispositivo móvil iOS con MDM en la red Windows NT.

    El nombre del titular NT está contenido en la solicitud de certificado enviada al servidor SCEP.

12. En el campo **Número de intentos de sondear el servidor de SCEP**, especifique la cantidad máxima de intentos de sondear el servidor SCEP para obtener el certificado firmado.

13. En el campo **Frecuencia de intentos (seg.)**, especifique el período en segundos entre un intento y otro de sondear el servidor SCEP para obtener la firma del certificado.

14. En el campo **Solicitud de registro**, escriba la clave de registro pre publicada.

    Antes de firmar un certificado, el servidor SCEP solicita al usuario del dispositivo móvil que proporcione una clave. Si este campo se deja en blanco, el SCEP no solicita la clave.

15. En la lista desplegable **Tamaño de clave**, seleccione el tamaño de la clave de registro en bits: 1024 o 2048.

16. Si desea permitir al usuario utilizar un certificado recibido del servidor SCEP como certificado para firmas, active la casilla **Usar para firmar**.

17. Si desea permitir al usuario utilizar un certificado recibido del servidor SCEP para el cifrado de información, active la casilla **Usar para cifrar**.

    Está prohibido utilizar el certificado del servidor SCEP como un certificado para firmar información al mismo tiempo que un certificado de cifrado de información.

18. En el campo **Huella digital del certificado**, indique una huella digital única del certificado para verificar la autenticidad de la respuesta del Centro de certificación. Puede utilizar el certificado de huella digital con el algoritmo hash SHA-1 o MD5. Puede copiar el certificado de huella digital de forma manual o seleccionar un certificado utilizando el botón **Crear a partir del certificado**. Cuando se crea la huella digital utilizando el botón **Crear a partir del certificado** se agrega al campo la huella digital de manera automática.

    Debe especificarse el certificado de huella digital si el intercambio de información entre el dispositivo móvil y el Centro de certificación ocurre mediante el protocolo HTTP.

19. Haga clic en **Aceptar**.

    El nuevo perfil SCEP aparece en la lista.

20. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

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.

Control

Esta sección contiene información sobre cómo controlar remotamente dispositivos móviles en la Consola de administración de Kaspersky Security Center.

Configuración de restricciones

Esta sección proporciona instrucciones sobre cómo configurar el acceso del usuario a las funciones de dispositivos móviles.

Consideraciones especiales para dispositivos con Android versión 10 o posterior

Android 10 introdujo varios cambios y restricciones destinados a API 29 o superior. Algunos de estos cambios afectan la disponibilidad o funcionalidad de ciertas funciones de la aplicación. Estas consideraciones afectan solo a dispositivos con Android 10 o posterior.

Capacidad para activar, desactivar y configurar Wi-Fi

- Se pueden agregar, eliminar y configurar redes de Wi-Fi en la Consola de administración de Kaspersky Security Center. Cuando se agrega una red Wi-Fi a una directiva, Kaspersky Endpoint Security recibe la configuración de esta red al conectarse por primera vez a Kaspersky Security Center.

- Cuando un dispositivo detecta una red configurada a través de Kaspersky Security Center, Kaspersky Endpoint Security solicita que el usuario se conecte a esa red. Si el usuario elige conectarse a la red, todos los ajustes configurados a través de Kaspersky Security Center se aplican de manera automática. Luego, el dispositivo se conecta de manera automática a esa red cada vez que entra en su rango, sin enviar notificaciones adicionales al usuario.

- Si el dispositivo de un usuario ya se encuentra conectado a otra red Wi-Fi, puede que el usuario no reciba una solicitud para aprobar la incorporación de una nueva red. En estos casos, el usuario debe desactivar y volver a activar la conexión Wi-Fi para recibir la sugerencia.

- Si Kaspersky Endpoint Security sugiere que el usuario se conecte a una red Wi-Fi y el usuario se rehúsa, se revoca el permiso de la aplicación para cambiar el estado de Wi-Fi. En este caso, Kaspersky Endpoint Security no puede volver a sugerir la conexión a redes Wi-Fi hasta que el usuario vuelva a conceder el permiso a través de **Configuración**→ **Apps & notificaciones**→ **Acceso especial de Apps** → **Control Wi-Fi** → **Kaspersky Endpoint Security**.

- Solo se admiten redes abiertas y redes cifradas con WPA2-PSK. No se admiten los cifrados WEP y WPA.

- Si la contraseña de una red sugerida anteriormente por la aplicación cambió, el usuario debe eliminar esa red de manera manual de la lista de redes conocidas. El dispositivo entonces podrá recibir una sugerencia de red de Kaspersky Endpoint Security y realizar la conexión.

- Cuando el SO un dispositivo se actualiza de Android versión 9 o anterior a Android versión 10 o posterior, o cuando se actualiza Kaspersky Endpoint Security en un dispositivo con Android 10 o posterior, las redes que se habían agregado anteriormente a través de Kaspersky Security Center no pueden modificarse o eliminarse a través de las directivas de Kaspersky Security Center. Sin embargo, el usuario puede modificar o eliminar estas redes de manera manual en la configuración del dispositivo.

- En los dispositivos con Android 10, el usuario debe ingresar la contraseña al intentar conectarse de manera manual a una red protegida sugerida. La conexión automática no requiere el ingreso de la contraseña. Si el dispositivo de un usuario se conecta a otra red Wi-Fi, el usuario debe primero desconectarse de esa red para permitir la conexión automática a una de las redes sugeridas.

- En los dispositivos con Android 11, el usuario puede conectarse manualmente a una red protegida sugerida por la aplicación, sin la necesidad de ingresar la contraseña.
- Al eliminar Kaspersky Endpoint Security de un dispositivo, las redes sugeridas previamente por la aplicación se ignoran.
- No se admite prohibir el uso de redes Wi-Fi.

Acceso a la cámara

- En dispositivos con Android 10, el uso de la cámara no se puede prohibir completamente. Aún se admite prohibir el uso de la cámara para perfiles de trabajo.
- Si una aplicación de otra empresa intenta acceder a la cámara del dispositivo, la aplicación se bloqueará y el usuario recibirá una notificación acerca del problema. Sin embargo, las aplicaciones que utilizan la cámara mientras se ejecutan en segundo plano no pueden bloquearse.
- En ocasiones, cuando se desconecta una cámara externa del dispositivo, se muestra una notificación para avisar que la cámara no se encuentra disponible.

Administración de métodos de desbloqueo de pantalla

- Ahora, 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 o numérica (PIN) con una secuencia que no tenga números repetidos u ordenados (por ejemplo, 1234), o alfanumérica. El PIN o contraseña debe tener al menos 4 caracteres de extensión.
  - 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). La extensión del PIN debe ser de al menos 8 dígitos; la contraseña debe contar con al menos 6 caracteres.
- El uso de la huella digital para desbloquear la pantalla puede configurarse solo en perfiles de trabajo.

Configuración de restricciones para dispositivos Android

Para mantener el dispositivo Android protegido, configure las opciones de utilización de Wi-Fi, de la cámara y de Bluetooth en el dispositivo.

De forma predeterminada, el usuario puede usar el Wi-Fi, la cámara y el Bluetooth en el dispositivo sin restricciones.

Para configurar las restricciones de utilización de Wi-Fi, de la cámara y de Bluetooth en el dispositivo:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.

4. En la ventana **Propiedades** de la directiva, seleccione la sección **Administración del dispositivo**.

5. En la sección **Restricciones**, configure el uso de Wi-Fi, de la cámara y de Bluetooth:

   - Para deshabilitar el módulo Wi-Fi en el dispositivo móvil del usuario, active la casilla **Prohibir el uso de Wi-Fi**.

     En dispositivos con Android 10.0 o una versión posterior, no se admite prohibir el uso de redes Wi-Fi.

   - Para deshabilitar la cámara en el dispositivo móvil del usuario, active la casilla **Prohibir el uso de la cámara**.

     En dispositivos con Android 10.0 o una versión posterior, el uso de la cámara no se puede prohibir completamente.

     En los dispositivos con Android 11 o posterior, Kaspersky Endpoint Security para Android debe estar configurado como una función de accesibilidad. Kaspersky Endpoint Security para Android solicita al usuario que configure la aplicación 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. Si este es el caso, no podrá restringir el uso de la cámara.

   - Para deshabilitar el Bluetooth en el dispositivo móvil del usuario, active la casilla **Prohibir el uso de Bluetooth**.

     En Android 12 o versiones posteriores, el uso de Bluetooth puede deshabilitarse solo si el usuario del dispositivo otorgó el permiso **Dispositivos Bluetooth cercanos**. El usuario puede otorgar este permiso durante el Asistente de configuración inicial o posteriormente.

6. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Configuración de restricciones de funciones de dispositivos iOS con MDM

Para garantizar conformidad con los requisitos de seguridad corporativa, configure restricciones al funcionamiento del dispositivo iOS con MDM.

Para configurar restricciones de funciones de dispositivos iOS con MDM:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.

2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.

4. En la ventana **Propiedades** de la directiva, seleccione la sección **Restricciones para las Funciones**.

5. En la sección **Configuración de restricciones de funciones**, active la casilla **Aplicar configuración en el dispositivo**.

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

7. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

8. Seleccione la sección **Restricciones para las aplicaciones**.

9. En la sección **Configuración de restricciones de aplicaciones**, active la casilla **Aplicar configuración en el dispositivo**.

10. Configure restricciones de las aplicaciones en el dispositivo iOS con MDM.

11. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

12. Seleccione la sección **Restricciones para contenido multimedia**.

13. En la sección **Configuración de restricciones de contenido multimedia**, active la casilla **Aplicar configuración en el dispositivo**.

14. Configure restricciones del contenido multimedia en el dispositivo iOS con MDM.

15. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Como resultado, luego de que se aplica la directiva, las restricciones de las funciones, de las aplicaciones y del contenido multimedia se configuran en el dispositivo móvil del usuario.

Configuración de restricciones de funciones del dispositivo EAS

Configure restricciones de las funciones del dispositivo para proteger los dispositivos EAS.

De forma predeterminada, el usuario puede utilizar las funciones de un dispositivo EAS sin restricciones.

Para configurar restricciones de las funciones del dispositivo EAS:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de EAS pertenecen.

2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.

4. En la ventana Propiedades de la directiva, seleccione la sección **Restricción de la Función**.

5. En la sección **Configuración de restricciones de funciones**, permita o bloquee la utilización de las funciones del dispositivo EAS:

   - Para permitir la conexión de tarjetas de memoria y otras unidades extraíbles a un dispositivo, seleccione la casilla **Permitir discos extraíbles**.

   - Para permitir el uso de la cámara, seleccione la casilla **Permitir uso de la cámara**.

   - Para permitir conexiones Wi-Fi, seleccione la casilla **Permitir uso de Wi-Fi**.

- Para permitir el uso del puerto de conexión infrarroja, seleccione **Permitir conexión infrarroja**.
- Para permitir el uso del dispositivo como punto de acceso Wi-Fi para crear una red inalámbrica, active la casilla **Permitir uso del dispositivo como punto de acceso Wi-Fi**.
- Para permitir que el dispositivo se conecte a un escritorio remoto, seleccione la casilla **Permitir conexión a escritorio remoto**.
- Para permitirle al usuario utilizar el cliente del escritorio ActiveSync en el dispositivo, active la casilla **Permitir sincronización de escritorio**.
- En la lista desplegable **Uso de Bluetooth**, permita o bloquee el uso de Bluetooth en el dispositivo EAS:
  - **Permitir**. Se permite el uso de Bluetooth en el dispositivo móvil.
  - **Al usar el manos libres**. Se permite el uso de Bluetooth cuando se conectan auriculares inalámbricos al dispositivo móvil.
  - **Denegar**. Se bloquea el uso de Bluetooth en el dispositivo móvil.

6. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Configuración de acceso de usuarios 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 la Protección web para configurar el acceso de usuarios de dispositivos Android a sitios web. La Protección web también puede filtrar los sitios web según las categorías definidas en el servicio en la nube de Kaspersky Security Network. El filtrado permite restringir el acceso de los usuarios a determinados sitios web o categorías de sitios web (por ejemplo, los de las categorías "Juegos de azar, loterías, sorteos" o "Comunicación por Internet"). Protección web también protege los datos personales de los usuarios en Internet.

Se debe configurar Kaspersky Endpoint Security para Android como una función de accesibilidad. Kaspersky Endpoint Security para Android solicita al usuario que configure la aplicación 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. Si hace esto, no se ejecutará la Protección Web.

La Protección web en los dispositivos Android solo funciona en el navegador Google Chrome (incluida la función de Pestañas personalizadas), el navegador Huawei y el navegador de Internet de Samsung. La Protección web para el Navegador de Samsung no bloquea sitios en un dispositivo móvil si se utiliza un perfil de trabajo y la Protección web está habilitada solo para el perfil de trabajo.

La Protección web está activada de forma predeterminada: el acceso del usuario a los sitios web de las categorías **Phishing** y **Software malicioso** está bloqueado.

Para configurar las opciones de acceso del usuario del dispositivo a sitios web:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.

2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.

4. En la ventana **Propiedades** de la directiva, seleccione **Protección web**.

5. Active la casilla **Habilitar Protección web**.

6. Para usar la Protección web, usted o el usuario del dispositivo deben leer y aceptar la Declaración sobre el procesamiento de datos para usar Protección web (Declaración de Protección web):

   a. Haga clic en el vínculo **Declaración de Protección web**.

      Se abrirá la ventana **Declaración sobre el procesamiento de datos para usar Protección web**. Para aceptar la Declaración de protección web, debe leer y aceptar la Directiva de privacidad.

   b. Haga clic en el vínculo de la Directiva de privacidad. Lea y acepte la Directiva de privacidad.

      Si no acepta la Directiva de privacidad, el usuario del dispositivo móvil puede aceptar la Directiva de privacidad en el Asistente de configuración inicial o en la app (→ **Acerca de** → **Términos y condiciones** → **Política de privacidad**).

   c. Seleccione el modo de aceptación de la Declaración de protección web:

      - **He leído y acepto la Declaración de protección web**
      - **Solicitar al usuario del dispositivo que acepte la Declaración de Protección web**
      - **No acepto la Declaración de protección web**

   Si selecciona **No acepto la Declaración de protección web**, la Protección web no bloquea los sitios en el dispositivo móvil. El usuario del dispositivo móvil no puede habilitar la Protección web en Kaspersky Endpoint Security.

7. Si desea que la aplicación restrinja el acceso del usuario a sitios web en función de su contenido, haga lo siguiente:

   a. En la sección **Protección web**, en la lista desplegable, seleccione **Los sitios web de las categorías seleccionadas están prohibidos**.

   b. Cree una lista de categorías bloqueadas seleccionando las casillas junto a las categorías de los sitios web a los que la app bloqueará el acceso.

8. Si desea que la aplicación permita que el usuario acceda solo a sitios web especificados por el administrador, haga lo siguiente:

   a. En la sección **Protección web**, en la lista desplegable, seleccione **Solo se permiten los sitios web de la lista**.

   b. Cree una lista de sitios web agregando direcciones de sitios web a los que la app no bloqueará el acceso. Kaspersky Endpoint Security para Android solo admite expresiones regulares. Al escribir la dirección de un sitio web permitido, utilice las siguientes plantillas:

- `http:\/\/www\.example\.com.*`: Todas las páginas secundarias del sitio web están permitidas (por ejemplo, `http://www.example.com/about`).

- `https:\/\/.*example\.com`—Todas las páginas del subdominio del sitio web están permitidas (por ejemplo, `https://pictures.example.com`).

También puede usar la expresión `https?` para seleccionar protocolos HTTP y HTTPS. Para obtener más información sobre las expresiones regulares, consulte el sitio web de soporte técnico de Oracle.

9. Si desea que la app bloquee el acceso del usuario a todos los sitios web, en la sección **Protección web**, en la lista desplegable, seleccione **Todos los sitios web están bloqueados**.

10. Para quitar las restricciones basadas en contenido que afectan el acceso del usuario a los sitios web, desactive la casilla **Habilitar Protección web**.

11. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Configuración de acceso a sitios web en dispositivos iOS con MDM

Configure los ajustes de Protección web para controlar el acceso a sitios web para usuarios de dispositivos iOS con MDM. La Protección web controla el acceso del usuario a sitios web en función de listas de sitios web permitidos y bloqueados. La Protección web también le permite añadir sitios web favoritos al panel de favoritos de Safari.

De forma predeterminada, el acceso a sitios web no está restringido.

Las opciones de Protección web solamente se pueden configurar en dispositivos supervisados.

Para configurar el acceso a sitios web en el dispositivo iOS con MDM del usuario:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.

2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.

4. En la ventana **Propiedades** de la directiva, seleccione la sección **Protección web**.

5. En la sección **Configuración de Protección web**, active la casilla **Aplicar configuración en el dispositivo**.

6. Para bloquear el acceso a los sitios web bloqueados y permitir el acceso a los sitios web permitidos:

   a. En la lista desplegable del **Modo de filtro web**, seleccione el modo **Limitar el contenido para adultos**.

   b. En la sección **Sitios web permitidos**, cree una lista de sitios web permitidos.

La dirección del sitio web debe comenzar con `"http://"` o `"https://"`. Kaspersky Device Management para iOS permite el acceso a todos los sitios web en el dominio. Por ejemplo, si se ha agregado http://www.ejemplo.com a la lista de sitios web permitidos, se permite el acceso a http://imágenes.ejemplo.com y http://ejemplo.com/peliculas. Si la lista de sitios web permitidos está vacía, la aplicación permite el acceso a todos los sitios web que no están incluidos en la lista de sitios web bloqueados.

c. En la sección **Sitios web prohibidos**, cree una lista de sitios web bloqueados.

La dirección del sitio web debe comenzar con `"http://"` o `"https://"`. Kaspersky Device Management para iOS bloquea el acceso a todos los sitios web en el dominio.

7. Para bloquear el acceso a todos los sitios web que no sean sitios web permitidos en la lista de la ficha:

a. En la lista desplegable del **Modo de filtro web**, seleccione el modo **Permitir los sitios web favoritos solamente**.

b. En la sección **Favoritos**, cree una lista de favoritos de sitios web permitidos.

La dirección del sitio web debe comenzar con `"http://"` o `"https://"`. Kaspersky Device Management para iOS permite el acceso a todos los sitios web en el dominio. Si la lista de favoritos está vacía, la aplicación permite el acceso a todos los sitios web. Kaspersky Device Management para iOS agrega sitios web de la lista de favoritos en la ficha de favoritos en Safari al dispositivo móvil del usuario.

8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Como resultado, luego de que se aplica la directiva, Protección web se configura en el dispositivo móvil del usuario de acuerdo con el modo seleccionado y las listas creadas.

Control de cumplimiento de dispositivos Android con requisitos de seguridad corporativa

Puede controlar dispositivos Android para el cumplimiento con los requisitos de seguridad corporativa. Los requisitos de seguridad corporativa regulan cómo el usuario puede operar con el dispositivo. Por ejemplo, la protección en tiempo real se debe habilitar en el dispositivo, las bases de datos antivirus se deben actualizar y la contraseña del dispositivo debe ser suficientemente segura. El control de cumplimiento se basa en una lista de reglas. Una regla de cumplimiento incluye los siguientes componentes:

- Criterio de control del dispositivo (por ejemplo, ausencia de aplicaciones bloqueadas en el dispositivo).
- Período asignado para que el usuario solucione instancias de incumplimiento (por ejemplo, 24 horas).
- La acción que se tomará en el dispositivo si el usuario no soluciona el incumplimiento dentro del período establecido (por ejemplo, bloquear el dispositivo).

> En Android 12 o una versión posterior, la aplicación puede realizar esta tarea más tarde de lo especificado si el dispositivo está en modo de ahorro de batería.

Si el usuario no soluciona el incumplimiento durante el período especificado, las siguientes opciones están disponibles:

- **Bloquear todas las aplicaciones, excepto las del sistema**. Se bloquea el inicio de todas las aplicaciones del dispositivo móvil del usuario, excepto las aplicaciones del sistema.

- **Bloquear dispositivo**. El dispositivo móvil se bloquea. Para obtener acceso a los datos, debe desbloquear el dispositivo. Si no se rectifica el motivo de bloqueo del dispositivo después de que se desbloquea, el dispositivo se bloqueará de nuevo después del período especificado.

- **Eliminar datos corporativos**. Eliminar datos transportados en contenedores, cuenta de correo electrónico corporativa, configuración para conectarse a la red Wi-Fi corporativa y VPN, nombre del punto del acceso (APN), perfil de trabajo de Android, contenedor KNOX y la clave del administrador de licencias KNOX.

- **Restablecimiento completo**. Todos los datos se eliminan del dispositivo móvil y la configuración se restablece a sus valores de fábrica. Cuando se completa esta acción, el dispositivo ya no será un dispositivo administrado. Para conectar el dispositivo a Kaspersky Security Center, debe reinstalar Kaspersky Endpoint Security para Android.

Para crear una regla de análisis para verificar que los dispositivos cumplan con una directiva de grupo:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.

2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.

4. En la ventana **Propiedades** de la directiva, seleccione la sección **Control de cumplimiento**.

5. Para recibir notificaciones los dispositivos que no cumplen con la directiva, en la sección **Notificaciones de incumplimiento**, active la casilla **Notificar al administrador**.

   Si el dispositivo no cumple con una política, durante la sincronización del dispositivo con el Servidor de Administración, Kaspersky Endpoint Security para Android escribe una entrada de **Violación detectada: <name of the criterion checked>** en el registro de eventos. Puede ver el registro de eventos en la ficha **Eventos** en las propiedades del Servidor de administración o en las propiedades locales de la aplicación.

6. Para notificar al usuario que el dispositivo móvil no cumple con la directiva, en la sección **Notificaciones de incumplimiento**, active la casilla **Notificar al usuario**.

   Si el dispositivo viola una directiva, durante la sincronización del dispositivo con el Servidor de administración, Kaspersky Endpoint Security para Android notifica al usuario en la sección **Estado**.

7. En la sección **Reglas de cumplimiento**, elabore una lista de reglas para verificar que el dispositivo cumpla con la directiva. Siga los pasos detallados a continuación:

   a. Haga clic en **Agregar**.

      Se inicia el Asistente de reglas de análisis.

   b. Siga las instrucciones del Asistente de reglas de análisis.

      Cuando el asistente termina, la regla nueva se muestra en la sección **Reglas de cumplimiento** en la lista de reglas de análisis.

8. Para deshabilitar temporalmente una regla de análisis que ha creado, utilice el conmutador ubicado junto a la regla seleccionada.

9. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil. Si el dispositivo del usuario no cumple con las reglas, las restricciones que ha especificado en la lista de reglas de análisis se aplican al dispositivo.

Control de inicio de aplicaciones

Esta sección contiene instrucciones sobre cómo configurar el acceso del usuario a aplicaciones en un dispositivo móvil.

Control de inicio de aplicaciones en dispositivos Android

Para mantener el dispositivo móvil del usuario protegido, debe configurar las opciones para el inicio de aplicaciones en el dispositivo.

Puede imponer restricciones a la actividad del usuario en un dispositivo en el cual se instalan aplicaciones bloqueadas o no se instalan aplicaciones requeridas (por ejemplo, bloqueo del dispositivo). Puede imponer restricciones usando el componente Control de cumplimiento. Para hacer esto, en la configuración de regla de análisis, debe seleccionar los criterios **Se instalaron aplicaciones prohibidas**, **Se instalaron aplicaciones de categorías prohibidas** o **No se instalaron todas las aplicaciones 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 aplicación 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. Si hace esto, no se ejecutará Control de apps.

Para configurar las opciones del inicio de aplicaciones en el dispositivo móvil:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Control de apps**.
5. En la sección **Modo de operación**, seleccione el modo de inicio de aplicaciones en el dispositivo móvil del usuario:
   - Para permitir que el usuario pueda iniciar todas las aplicaciones salvo aquellas especificadas en la lista de categorías y de aplicaciones bloqueadas, seleccione el modo **Aplicaciones bloqueadas**.
   - Para permitir que el usuario pueda iniciar solo las aplicaciones especificadas en la lista de categorías y de aplicaciones permitidas, recomendadas o requeridas, seleccione el modo **Aplicaciones permitidas**.
6. Si desea que Kaspersky Endpoint Security para Android envíe datos sobre aplicaciones prohibidas al registro de eventos sin bloquearlas, seleccione la casilla de verificación **No bloquear aplicaciones prohibidas, escribir solo en el registro de eventos**.

   Durante la siguiente sincronización del dispositivo móvil del usuario con el Servidor de administración, Kaspersky Endpoint Security para Android escribe una entrada de **Se ha instalado una aplicación prohibida** en el registro de eventos. Puede ver el registro de eventos en la ficha **Eventos** en las propiedades del Servidor de administración o en las propiedades locales de la aplicación.

7. Si desea que Kaspersky Endpoint Security para Android bloquee el inicio de aplicaciones del sistema en el dispositivo móvil del usuario (como Calendario, Cámara y Configuración) en el modo **Aplicaciones permitidas**, seleccione la casilla **Bloquear aplicaciones del sistema**.

   Los expertos de Kaspersky recomiendan no usar aplicaciones de sistema de bloqueo porque esto podría causar fallos en el funcionamiento del dispositivo.

8. Crear una lista de categorías y aplicaciones para configurar el inicio de las aplicaciones.

   Para obtener más información acerca de las categorías de aplicaciones, consulte los Apéndices.

   Para conocer una lista de las aplicaciones que pertenecen a cada categoría, visite el sitio web de Kaspersky.

9. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Configuración de restricciones para las aplicaciones del dispositivo EAS

Para proteger el dispositivo EAS, configure las restricciones a la actividad de las aplicaciones (navegador, aplicaciones no firmadas).

De forma predeterminada, el usuario puede utilizar las aplicaciones de un dispositivo EAS sin restricciones.

Para configurar las restricciones a la actividad de las aplicaciones del dispositivo EAS:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de EAS pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.
4. En la ventana Propiedades de la directiva, seleccione la sección **Restricciones para las aplicaciones**.
5. En la sección **Configuración de restricciones de aplicaciones**, configure las restricciones a la actividad de las aplicaciones:
   - Para permitir al usuario utilizar el navegador, active la casilla **Permitir uso del navegador**.
   - Para permitir al usuario crear cuentas de correo electrónico personales (POP3 o IMAP4), seleccione la casilla **Permitir correo personal**.
   - Para permitir al usuario iniciar aplicaciones que no se firmaron con un certificado de autenticación, active la casilla **Permitir aplicaciones sin firma**.
   - Para permitir al usuario instalar aplicaciones que no se firmaron con un certificado de autenticación, active la casilla **Permitir paquetes de instalación sin firma**.
6. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Inventario de software en dispositivos Android

Puede inventariar las aplicaciones que hay en los dispositivos Android conectados a Kaspersky Security Center. Kaspersky Endpoint Security para Android recibe información sobre todas las aplicaciones instaladas en los dispositivos móviles. La información adquirida durante el inventario se muestra en las propiedades del dispositivo en la sección **Eventos**. Puede consultar información detallada sobre cada aplicación instalada, incluida la versión y el editor.

Para habilitar el inventario de software:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Control de apps**.
5. En la sección **Inventario de software**, seleccione la casilla de verificación **Enviar datos de aplicaciones instaladas**.
6. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil. Kaspersky Endpoint Security para Android envía datos al registro de eventos cada vez que se instala o elimina una aplicación del dispositivo.

Configuración de visualización de dispositivos Android en Kaspersky Security Center

Para operaciones convenientes con la lista de dispositivos móviles, debería ajustar la configuración para mostrar dispositivos en Kaspersky Security Center. De forma predeterminada, la lista de dispositivos móviles se muestra en el árbol de la consola **Adicional → Administración de dispositivos móviles → Dispositivos móviles**. La información del dispositivo se actualiza automáticamente. También puede actualizar manualmente la lista de dispositivos móviles haciendo clic en el botón **Actualizar** en la esquina derecha superior.

Después de conectar el dispositivo a Kaspersky Security Center, los demás se agregan automáticamente a la lista de dispositivos móviles. La lista de dispositivos móviles puede contener información detallada sobre ese dispositivo: modelo, sistema operativo, dirección IP, etc.

Puede configurar el formato del nombre del dispositivo y seleccionar el estado del dispositivo. El estado del dispositivo le informa sobre cómo los componentes de Kaspersky Endpoint Security for Android están funcionando en el dispositivo móvil del usuario.

Los componentes de Kaspersky Endpoint Security para Android podrían no estar en funcionamiento por las siguientes razones:

- El usuario deshabilitó el componente en la configuración del dispositivo.
- El usuario no concedió a la aplicación los permisos necesarios para el funcionamiento del componente (por ejemplo, no hay permiso para determinar la ubicación del dispositivo para el comando Antirrobo

correspondiente).

Para que se muestre el estado del dispositivo, debe habilitar la condición **Determinado por la aplicación** en las propiedades del grupo de administración (**Propiedades** → **Estado del dispositivo** → **Establecer estado del dispositivo como Crítico si** y **Establecer estado del dispositivo como Advertencia si**). En las propiedades del grupo de administración, también puede seleccionar otros criterios para determinar el estado del dispositivo móvil.

Para configurar la visualización de dispositivos Android en Kaspersky Security Center:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Información del dispositivo**.
5. En la sección **Nombre del dispositivo en Kaspersky Security Center**, seleccione el formato para el nombre del dispositivo móvil en la Consola de administración:
   - Modelo del dispositivo [correo electrónico, ID de dispositivo]
   - Modelo del dispositivo [correo electrónico (si hay uno disponible) o ID de dispositivo]

   Un *ID De dispositivo* es un Id. exclusivo que genera Kaspersky Endpoint Security para Android a partir de los datos que recibe de un dispositivo. Para los dispositivos móviles que ejecutan Android 10 o posterior, Kaspersky Endpoint Security para Android usa el SSAID (ID de Android) o la suma de comprobación de otros datos recibidos del dispositivo. Para las versiones anteriores de Android, la aplicación usa el IMEI.
6. Establezca el atributo "lock" en la posición de bloqueo ( ).
7. En la sección **Estado del dispositivo en Kaspersky Security Center**, seleccione el estado del dispositivo apropiado si un componente de Kaspersky Endpoint Security para Android no está funcionando: (**Aceptar**), (**Advertencia**) o (**Aceptar**).

   En la lista de dispositivos móviles, el estado del dispositivo cambiará según el estado seleccionado.
8. Establezca el atributo "lock" en la posición de bloqueo.
9. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Administración

Esta sección contiene información sobre cómo administrar remotamente los ajustes de dispositivos móviles en la Consola de administración de Kaspersky Security Center.

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 conectar el dispositivo móvil a una red Wi-Fi:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Wi-Fi**.
5. En la sección **Redes Wi-Fi**, haga clic en **Agregar**.

   Esto abre la ventana **Red Wi-Fi**.
6. En el campo **Identificador de red (SSID)**, escriba el nombre de la red Wi-Fi que incluye el punto de acceso (SSID).
7. En la sección **Protección de la red**, seleccione el tipo de seguridad de red Wi-Fi (red pública o segura protegida con protocolos WEP o WPA/WPA2 PSK).
8. En el campo **Contraseña**, establezca una contraseña de acceso a la red si seleccionó una red segura en el paso anterior.
9. En el campo **Dirección y puerto del servidor proxy**, escriba la dirección IP o nombre DNS del servidor proxy y el número de puerto, si corresponde.

   En dispositivos la versión 8.0 de Android en ejecución o posterior, la configuración del servidor proxy para Wi-Fi no se puede redefinir con la directiva. Sin embargo, puede configurar manualmente la configuración del servidor proxy para una red Wi-Fi en el dispositivo móvil.

   Si está utilizando un servidor proxy para conectarse a una red Wi-Fi, puede usar una política para configurar los ajustes para conectarse a la red. En los dispositivos que ejecutan Android 8.0 o posterior, debe configurar manualmente la configuración del servidor proxy. En los dispositivos que ejecutan Android 8.0 o posterior, no puede usar una política para cambiar la configuración de la conexión de red Wi-Fi, excepto la contraseña de acceso a la red.

   Si no está utilizando un servidor proxy para conectarse a una red Wi-Fi, no hay limitaciones en el uso de políticas para administrar una conexión de red Wi-Fi.
10. En el campo **No utilizar el servidor proxy para las siguientes direcciones**, genere una lista de 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 que operan con Android 8.0 o posterior, la exclusión del servidor proxy para direcciones web no funciona.

11. Haga clic en **Aceptar**.

    La red Wi-Fi agregada se muestra en la lista **Redes Wi-Fi**.

    Puede modificar o eliminar redes Wi-Fi en la lista de redes Wi-Fi con los botones **Editar** y **Eliminar** que se encuentran en la parte superior de la lista.

12. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil. Luego de aplicar la directiva en el dispositivo móvil, el usuario puede conectarse a la red Wi-Fi que se ha agregado, sin especificar la configuración de red.

En dispositivos con Android versión 10.0 o posterior, si un usuario se rehúsa a conectarse a la red de 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 dispositivo iOS con MDM a una red Wi-Fi

Para que un dispositivo iOS con MDM se conecte automáticamente a una red Wi-Fi disponible y para proteger los datos durante la conexión, configure las opciones de conexión.

Para configurar la conexión de un dispositivo iOS con MDM a una red Wi-Fi:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Wi-Fi**.
5. Haga clic en el botón **Agregar** en la sección **Redes Wi-Fi**.

   Esto abre la ventana **Red Wi-Fi**.
6. En el campo **Identificador de red (SSID)**, escriba el nombre de la red Wi-Fi que incluye el punto de acceso (SSID).
7. Si desea que el dispositivo iOS con MDM se conecte a la red Wi-Fi automáticamente, seleccione la casilla **Conexión automática**.
8. Para hacer que sea imposible conectar dispositivos iOS con MDM a una red Wi-Fi que requiere autenticación preliminar (red cautiva), seleccione la casilla **Desactivar 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.
9. Si desea que la red Wi-Fi esté oculta en la lista de redes disponibles en el dispositivo iOS con MDM, 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 router Wi-Fi en el dispositivo móvil.

10. En la lista desplegable **Protección de la red**, seleccione el tipo de protección de la conexión a la red Wi-Fi:

    - **Deshabilitado**. No se requiere la autenticación del usuario.
    - **WEP**. La red está protegida con el protocolo de cifrado inalámbrico WEP.
    - **WPA / WPA2 (Personal)**. La red está protegida con el protocolo WPA/WPA2 (Acceso Wi-Fi protegido).
    - **WPA2 (Personal)**. La red está protegida con el protocolo WPA2 (Acceso Wi-Fi protegido 2.0). La protección WPA2 está disponible para los dispositivos que funcionan con la versión de iOS 8 o posteriores. WPA2 no está disponible en dispositivos de Apple TV.
    - **Cualquiera (Personal)**. La red está protegida mediante protocolos de cifrado WEP, WPA o WPA2 dependiendo del tipo de router Wi-Fi. Para autenticación se utiliza una clave única de cifrado para cada usuario.
    - **WEP (Dinámica)**. Se protege la red utilizando el protocolo WEP y con una clave dinámica.
    - **WPA/WPA2 (Empresas)**. La red está protegida mediante el protocolo de cifrado WPA/WPA2 con el uso del protocolo 802.1X.
    - **WPA2 (Empresas)**. La red está protegida mediante el protocolo de cifrado WPA2 y con una clave única para todos los usuarios (802.1X). La protección WPA2 está disponible para los dispositivos que funcionan con la versión de iOS 8 o posteriores. WPA2 no está disponible en dispositivos de Apple TV.
    - **Cualquiera (Empresas)**. La red está protegida utilizando protocolos WEP o WPA/WPA2 dependiendo del tipo de router Wi-Fi. Para autenticación se utiliza una clave de cifrado compartida por todos los usuarios.

    Si ha seleccionado **WEP (Dinámica)**, **WPA/WPA2 (Empresas)**, **WPA2 (Empresas)** o **Cualquiera (Empresas)** en la lista de **Protección de la red** en la sección **Protocolos**, podrá seleccionar los tipos de protocolos de EAP (Protocolo de la Autentificación Extensible) para la identificación del usuario 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 iOS con MDM en servidores de confianza.

11. Configure las opciones de la cuenta para la autenticación del usuario luego de que el dispositivo iOS con MDM se conecte a la red Wi-Fi:

    a. En la sección **Autenticación**, haga clic en el botón **Configurar**.

    Se abre la ventana **Autenticación**.

    b. En el campo **Nombre de usuario**, escriba el nombre de la cuenta para la autenticación del usuario al conectarse a la red Wi-Fi.

    c. Para solicitarle al usuario que escriba la contraseña manualmente cada vez que se conecta a una red Wi-Fi, active la casilla **Solicitar contraseña con cada conexión**.

    d. En el campo **Contraseña**, escriba la contraseña de la cuenta para la autenticación en la red Wi-Fi.

    e. En la lista desplegable **Certificado de autenticación**, seleccione un certificado para la autenticación del usuario en la red Wi-Fi. Si la lista no contiene ningún certificado, **puede agregarlos en la sección** Certificados.

    f. 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 se diseña para hacer más seguro el proceso de autenticación, ya que no se muestra abiertamente el nombre del usuario pero se transmite a través del túnel cifrado TLS.

g. Haga clic en **Aceptar**.

Como resultado, las opciones de la cuenta para la autenticación del usuario en la conexión a una red Wi-Fi se configuran en el dispositivo iOS con MDM.

12. De ser necesario, configure las opciones de la conexión a la red Wi-Fi a través de un servidor proxy:

    a. En la sección **Servidor proxy**, haga clic en el botón **Configurar**.

    b. En la ventana **Servidor proxy** que se abre, seleccione el modo de configuración de servidor proxy y especifique la configuración de conexión.

    c. Haga clic en **Aceptar**.

    Como resultado, en el dispositivo iOS con MDM, se configuran las opciones de la conexión del dispositivo a la red Wi-Fi a través de un servidor proxy.

13. Haga clic en **Aceptar**.

    La nueva red Wi-Fi se muestra en la lista.

14. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

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. La tecnología de autenticación asegura la protección de información durante una conexión a 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

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 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.

Para añadir una cuenta de correo electrónico del usuario del dispositivo iOS con MDM:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.

2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.

4. En la ventana **Propiedades** de la directiva, seleccione **Correo electrónico**.

5. Haga clic en el botón **Agregar** en la sección **Cuenta de correo electrónico**.

   Se abre la ventana **Cuenta de correo electrónico**.

6. En el campo **Descripción**, escriba una descripción de la cuenta de correo electrónico del usuario.

7. Seleccione el protocolo de correo electrónico:

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

8. De ser necesario, especifique el prefijo de ruta IMAP en el campo **Prefijo de ruta IMAP**.

   El prefijo de ruta IMAP debe ingresarse con letras mayúscula (por ejemplo: GMAIL para Google Mail). Este campo está disponible si el protocolo para cuenta IMAP está seleccionado.

9. En el campo **Nombre de usuario como se muestra en los mensajes**, escriba el nombre de usuario a mostrar en el campo **De:** para todos los mensajes salientes.

10. En el campo **Correo electrónico**, especifique la dirección de correo electrónico del usuario del dispositivo iOS con MDM.

11. Configure las opciones adicionales de la cuenta de correo electrónico:

    - Para permitir al usuario mover mensajes de correo electrónico entre las cuentas de usuario, active la casilla **Permitir movimiento de mensajes entre cuentas**.
    - Para permitir que las direcciones de correo electrónico utilizadas se sincronicen entre las cuentas de usuario, active la casilla **Permitir sincronización de direcciones recientes**.
    - Para permitir que el usuario utilice el servicio Mail Drop para reenviar adjuntos de gran tamaño, seleccione la casilla **Permitir Mail Drop**.
    - Para permitir que el usuario utilice únicamente el cliente de correo electrónico estándar de iOS, seleccione la casilla **Permitir uso de la aplicación Mail**.

12. Ajuste la configuración para usar el protocolo S/MIME en la aplicación del Correo. *S/MIME* es un protocolo para transmitir mensajes cifrados digitalmente firmados.

    - Para usar el protocolo S/MIME para firmar los mensajes de correo electrónico que envíe, seleccione la casilla de verificación **Firmar mensajes** y seleccione un certificado para la firma. Una firma digital confirma la autenticidad del remitente e indica que los contenidos del mensaje no se han modificado durante la transmisión al destinatario. La firma para mensajes está disponible en dispositivos que funcionan con la versión iOS 10.3 o posterior.
    - Para usar el protocolo S/MIME para cifrar los mensajes de correo electrónico que envía, seleccione la casilla de verificación **Cifrar mensajes de manera predeterminada** y seleccione un certificado de cifrado (clave pública). El cifrado de mensajes está disponible para los dispositivos que funcionan con la versión de iOS 10.3 o posterior.

- Para permitir que un usuario pueda cifrar sus mensajes particulares, seleccione la casilla de verificación **Mostrar botón de alternancia para cifrar mensajes**. Para enviar mensajes cifrados, el usuario debe hacer clic en el icono de la aplicación del Correo en el campo **Para**.

13. En las secciones **Servidor de correo entrante** y **Servidor de correo saliente**, haga clic en el botón **Configuración** para configurar las opciones de conexión del servidor:

    - **Dirección y puerto del servidor**: nombres de host o direcciones IP de los servidores de correo entrante y de los servidores de correo saliente, y números de puerto del servidor.
    - **Nombre de la cuenta**: nombre de la cuenta del usuario para la autorización del servidor de correo entrante y saliente.
    - **Tipo de autenticación**: tipo de autenticación de la cuenta de correo electrónico del usuario en los servidores de correo entrante y en los servidores de correo saliente.
    - **Contraseña**: contraseña de la cuenta para autenticación en el servidor de correo entrante y saliente protegido mediante el método de autenticación seleccionado.
    - **Usar una contraseña para servidores de correo entrante y saliente**: use una contraseña para la autenticación del usuario en servidores de correo entrante y saliente.
    - **Usar conexión SSL**: uso del protocolo SSL (Secure Sockets Layer) de transporte de datos que utiliza cifrado y autenticación basada en certificados para proteger la transmisión de información.

14. Haga clic en **Aceptar**.

    La nueva cuenta de correo electrónico aparece en la lista.

15. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Como resultado, luego de que se aplica la directiva, las cuentas de correo electrónico de la lista compilada se agregan al dispositivo móvil del usuario.

Configuración de un buzón de correo de Exchange en dispositivos iOS con MDM

Para permitir al usuario del dispositivo iOS con MDM 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 añadir una cuenta Exchange ActiveSync del usuario del dispositivo iOS con MDM:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.

2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.

4. En la ventana **Propiedades** de la directiva, seleccione la sección **Exchange ActiveSync**.

5. Haga clic en el botón **Agregar** en la sección **Cuentas de Exchange ActiveSync**.

   Se abre la ventana **Cuenta de Exchange ActiveSync** en la ficha **General**.

6. En el campo **Nombre de la cuenta**, escriba el nombre de la cuenta para la autorización en el servidor Microsoft Exchange. Puede usar las macros de la lista desplegable **Macros disponibles**.

7. En el campo **Dirección del servidor**, escriba el nombre de la red o la dirección IP del servidor Microsoft Exchange.

8. Para usar el protocolo SSL (Secure Sockets Layer) de transporte de datos para proteger la transmisión de información, active la casilla **Usar conexión SSL**.

9. En el campo **Dominio**, escriba el nombre de dominio del usuario del dispositivo iOS con MDM. Puede usar las macros de la lista desplegable **Macros disponibles**.

10. En el campo **Nombre de usuario de la cuenta**, escriba el nombre del usuario del dispositivo iOS con MDM.

    Si deja este campo en blanco, Kaspersky Device Management para iOS solicita al usuario que ingrese el nombre de usuario cuando aplica la directiva en el dispositivo iOS con MDM. Puede usar las macros de la lista desplegable **Macros disponibles**.

11. En el campo **Correo electrónico**, especifique la dirección de correo electrónico del usuario del dispositivo iOS con MDM. Puede usar las macros de la lista desplegable **Macros disponibles**.

12. En el campo **Contraseña**, escriba la contraseña de la cuenta Exchange ActiveSync para la autorización en el servidor Microsoft Exchange.

13. Seleccione la ficha **Adicional** y configure las opciones adicionales de la cuenta de Exchange ActiveSync:

    - **Número de días para sincronizar el correo para <time period>**.
    - **Tipo de autenticación**.
    - **Permitir movimiento de mensajes entre cuentas**.
    - **Permitir sincronización de direcciones recientes**.
    - **Permitir uso de la aplicación Mail**.

14. Ajuste la configuración para usar el protocolo S/MIME en la aplicación del Correo. *S/MIME* es un protocolo para transmitir mensajes cifrados digitalmente firmados.

    - Para usar el protocolo S/MIME para firmar los mensajes de correo electrónico que envíe, seleccione la casilla de verificación **Firmar mensajes** y seleccione un certificado para la firma. Una firma digital confirma la autenticidad del remitente e indica que los contenidos del mensaje no se han modificado durante la transmisión al destinatario. La firma para mensajes está disponible en dispositivos que funcionan con la versión iOS 10.3 o posterior.
    - Para usar el protocolo S/MIME para cifrar los mensajes de correo electrónico que envía, seleccione la casilla de verificación **Cifrar mensajes de manera predeterminada** y seleccione un certificado de cifrado (clave

pública). El cifrado de mensajes está disponible para los dispositivos que funcionan con la versión de iOS 10.3 o posterior.

- Para permitir que un usuario pueda cifrar sus mensajes particulares, seleccione la casilla de verificación **Mostrar botón de alternancia para cifrar mensajes**. Para enviar mensajes cifrados, el usuario debe hacer clic en el icono de la aplicación del Correo en el campo **Para**.

15. Haga clic en **Aceptar**.

    La nueva cuenta de Exchange ActiveSync aparece en la lista.

16. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

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.

Configuración de un buzón de correo de Exchange en dispositivos Android (solo Samsung)

Para trabajar con el calendario, el correo y los contactos corporativos en el dispositivo móvil, debería ajustar la configuración del buzón de correo de Exchange.

La configuración de un buzón de correo de Exchange solo es posible para dispositivos Samsung.

Para configurar un buzón de correo de Exchange en un dispositivo móvil:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Administrar Samsung KNOX → Administrar dispositivos Samsung**.
5. En la ventana **Exchange ActiveSync**, haga clic en el botón **Configurar**.

   Se abre la ventana **Configuración del servidor de correo Exchange**.
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 **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 **Usar conexión SSL**.
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**.
11. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Administración de aplicaciones móviles de terceros

Puede usar contenedores para supervisar la actividad de las aplicaciones iniciadas en el dispositivo móvil del usuario. *Un contenedor* es un armazón especial para aplicaciones móviles que permite controlar la actividad de la aplicación con armazón, por lo que protege los datos personales y corporativos del usuario en el dispositivo.

En Kaspersky Security para dispositivos móviles Service Pack 3 Maintenance Release 2, ya no se admite la creación de contenedores para aplicaciones móviles. Sin embargo, los contenedores que se crearon en versiones anteriores de la aplicación se pueden añadir a dispositivos Android.

Puede instalar una aplicación contenida en el dispositivo del usuario de una de las maneras siguientes:

- Enviando al usuario un correo electrónico con el vínculo del paquete de instalación de la aplicación contenida.
- Especificando una aplicación contenida como aplicación requerida o permitida en la sección **Control de apps** de la ventana de propiedades de la directiva. Después de que se sincroniza el dispositivo móvil con Kaspersky Security Center, el paquete de distribución de la aplicación que se encuentra en el contenedor se copia automáticamente al dispositivo del usuario.

Para instalar aplicaciones en contenedores, debe permitir la instalación de aplicaciones de orígenes desconocidos en el dispositivo móvil del usuario. Para proteger el dispositivo y los datos después de instalar aplicaciones contenidas, se recomienda prohibir la instalación de aplicaciones desde orígenes desconocidos. Para obtener información sobre la instalación de aplicaciones sin Google Play, consulte la *Guía de ayuda de Android*.

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 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 tocar el estado de protección del dispositivo y ver la lista de problemas en la app.
- **Notificaciones de la app**. Estas notificaciones informan al usuario del dispositivo sobre la aplicación (por ejemplo, detección de amenazas).
- **Mensajes emergentes**. Los mensajes emergentes requieren una acción del usuario del dispositivo (por ejemplo, qué hacer cuando se detecta una amenaza).

Todas las notificaciones de Kaspersky Endpoint Security para Android están activadas de forma predeterminada.

Un usuario del dispositivo Android puede desactivar todas las notificaciones de Kaspersky Endpoint Security para Android en la configuración de la barra de notificaciones. Si las notificaciones están desactivadas, el usuario no podrá controlar el funcionamiento la aplicación y se perderá de 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:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Adicional**.
5. En la sección **Notificaciones de la app**, haga clic en el botón **Configurar**.

   Se abrirá la ventana **Configuración de notificaciones del dispositivo**.
6. Seleccione los problemas de Kaspersky Endpoint Security for Android que desea mostrar en el dispositivo móvil del usuario y haga clic en el botón **Aceptar**.

   Kaspersky Endpoint Security para Android no mostrará problemas en la notificación de estado de protección ni en la sección **Estado** de la app. Kaspersky Endpoint Security para Android continuará mostrando las notificaciones de estado de protección y las notificaciones de la app.

   Algunos problemas de Kaspersky Endpoint Security para Android son obligatorios e imposibles de desactivar (por ejemplo, los problemas sobre la caducidad de la licencia).
7. Para ocultar todas las notificaciones y los mensajes emergentes, seleccione **Desactivar notificaciones y mensajes emergentes cuando la app se ejecuta 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 el número de problemas. Además, la aplicación muestra notificaciones cuando el usuario está trabajando con la aplicación (por ejemplo, si el usuario está actualizando las bases de datos antivirus de forma manual).

   Los expertos de Kaspersky recomiendan activar las notificaciones y los mensajes emergentes. Si desactiva 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. Los usuarios de dispositivos móviles pueden conocer el estado de protección del dispositivo únicamente cuando abren la aplicación.
8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil. Las notificaciones de Kaspersky Endpoint Security for Android que desactive no se mostrarán en el dispositivo móvil del usuario.

Conexión de dispositivos iOS con MDM a AirPlay

Configure la conexión a dispositivos AirPlay para habilitar la transmisión de música, fotos y videos de dispositivos iOS con MDM 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 los dispositivos Apple TV (segunda y tercera generación), dispositivos AirPort Express, altavoces o radios con AirPlay.

La conexión automática a dispositivos AirPlay está disponible solo para dispositivos controlados.

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

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **AirPlay**.
5. En la sección **Dispositivos AirPlay**, seleccione la casilla **Aplicar configuración en el dispositivo**.
6. Haga clic en el botón **Agregar** en la sección **Contraseñas**.

   Se agrega una fila vacía a la tabla de contraseñas.
7. En la columna **Nombre de dispositivo**, escriba el nombre del dispositivo AirPlay en la red inalámbrica.
8. En la columna **Contraseña**, escriba la contraseña al dispositivo AirPlay.
9. Para restringir el acceso de los dispositivos iOS con MDM a los dispositivos AirPlay, cree una lista de dispositivos permitidos en la sección **Dispositivos permitidos**. Para ello, agregue las direcciones MAC de los dispositivos AirPlay a la lista de dispositivos permitidos.

   Se bloquea el acceso a los dispositivos AirPlay que no están en la lista de dispositivos permitidos. Si la lista de dispositivos permitidos está en blanco, Kaspersky Device Management para iOS permite el acceso a todos los dispositivos AirPlay.
10. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

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 en forma inalámbrica desde el dispositivo iOS con MDM con la tecnología 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 AirPrint.

Para configurar la conexión de un dispositivo iOS con MDM a una impresora AirPrint:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **AirPrint**.
5. Haga clic en el botón **Agregar** en la sección **Impresoras AirPrint**.
   Se abre la ventana **Impresora**.
6. En el campo **Dirección IP**, escriba la dirección IP de la impresora AirPrint.
7. 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:
   - impresora/Canon_MG5300_series
   - ipp/impresora
   - Epson_IPP_impresora
8. Haga clic en **Aceptar**.
   La impresora AirPrint recién agregada aparece en la lista.
9. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

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)

Para conectar un dispositivo móvil a servicios de transferencia de datos en una red móvil, debería configurar los ajustes de APN (Nombre de punto de acceso).

Configuración de APN en dispositivos Android (solo Samsung)

La configuración de APN solo es posible 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. Una configuración de punto de acceso incorrecta puede conllevar cargos de telefonía móvil adicionales.

Configuración del Nombre de punto de acceso (APN):

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.

4. En la ventana **Propiedades** de la directiva, seleccione la sección **Administrar Samsung KNOX → APN**.

5. En la sección **APN**, haga clic en el botón **Configurar**.

   Se abre la ventana **Configuración de APN**.

6. En la ficha **General**, especifique las siguientes opciones del punto de acceso:

   a. En la lista desplegable **Tipo de APN**, seleccione el tipo de punto de acceso.

   b. En el campo **Nombre de APN**, especifique el nombre del punto de acceso.

   c. En el campo **MCC**, ingrese el código de país de móvil (MCC).

   d. En el campo **MNC**, ingrese el código de operador de móvil (MNC).

   e. Si ha seleccionado **MMS** o **Internet y MMS** como el tipo de punto de acceso, especifique las siguientes opciones adicionales de MMS:

   - En el campo **Servidor de MMS**, especifique el nombre de dominio completo del servidor de la empresa de telefonía móvil que se utiliza para intercambiar MMS.

   - En el campo **Servidor proxy de MMS**, especifique el nombre de la red o la dirección IP del servidor proxy y el número de puerto del servidor de la empresa de telefonía móvil que se utiliza para intercambiar MMS.

7. En la ficha **Adicional**, configure las opciones adicionales del nombre de punto de acceso (APN):

   a. En la lista desplegable **Tipo de autenticación**, seleccione el tipo de autenticación del usuario del dispositivo móvil en el servidor de la empresa de telefonía móvil que se utiliza para acceder a la red.

   b. 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.

   c. En el campo **Dirección de servidor proxy**, especifique el nombre de la red o la dirección IP y el número de puerto del servidor proxy de la empresa de telefonía móvil que se utiliza para acceder a la red.

   d. En el campo **Nombre de usuario**, escriba el nombre usuario para la autorización en la red móvil.

   e. En el campo **Contraseña**, escriba la contraseña para la autorización del usuario en la red móvil.

8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

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.

La sección **APN** está desactualizada. Se recomienda ajustar la configuración de APN en la sección **Comunicaciones móviles**. Antes de hacer modificaciones en la configuración de comunicaciones móviles, asegúrese de que no se haya aplicado la configuración de la sección **APN** en el dispositivo (la casilla **Aplicar configuración en el dispositivo** no está seleccionada). La configuración en las secciones **APN** y **Comunicaciones móviles** no se puede utilizar de manera concurrente.

Para configurar el punto de acceso en el dispositivo iOS con MDM de un usuario:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Comunicaciones móviles**.
5. En la sección **Configuración de comunicaciones móviles**, seleccione la casilla **Aplicar configuración en el dispositivo**.
6. En la lista de **tipo de APN**, seleccione el tipo de punto de acceso para la transferencia de datos en una red móvil GPRS/3G/4G:
   - **APN integrado**: configuración de comunicaciones móviles para la transferencia de datos mediante un operador de la red móvil que admite la operación con SIM de Apple integrada. Para obtener más información sobre dispositivos con SIM de Apple integrada, visite el sitio web del Soporte Técnico de Apple.
   - **APN**: configuración de comunicaciones móviles para la transferencia de datos mediante el operador de red móvil de la tarjeta SIM insertada.
   - **APN y APN integrado**: configuración de comunicaciones móviles para transferencia de datos mediante los operadores 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 del Soporte Técnico de Apple.
7. En el campo **Nombre de APN**, especifique el nombre del punto de acceso.
8. En la lista desplegable **Tipo de autenticación**, seleccione el tipo de autenticación del usuario del dispositivo móvil en el servidor de la empresa de telefonía móvil que se utiliza para acceder a la red (Internet y MMS):
9. En el campo **Nombre de usuario**, escriba el nombre usuario para la autorización en la red móvil.
10. En el campo **Contraseña**, escriba la contraseña para la autorización del usuario en la red móvil.
11. En el campo **Dirección y puerto del servidor proxy**, escriba el nombre del host o la dirección IP del servidor proxy y el número de puerto del servidor proxy.
12. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Como resultado, el nombre de punto de acceso (APN) se configura en el dispositivo móvil del usuario después de que se aplica la directiva.

Configuración del perfil de trabajo de Android

Esta sección contiene información sobre cómo trabajar con un perfil de trabajo de Android.

Sobre el perfil de trabajo de Android

Android Enterprise es una plataforma para administrar la infraestructura móvil corporativa que proporciona a los empleados de empresas un entorno de trabajo 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 el perfil de trabajo de Android (de aquí en adelante, también "perfil de trabajo") en el dispositivo móvil del usuario. El *perfil de trabajo de Android* es un entorno seguro en el dispositivo del usuario en el que el administrador puede gestionar aplicaciones y cuentas de usuario sin restringir el uso de sus datos personales por parte del usuario. Cuando se crea un perfil de trabajo 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 corporativas instaladas en el perfil de trabajo y las notificaciones de estas aplicaciones se marcan con el icono. Debe crear una cuenta corporativa de Google separada para la aplicación Google Play Market. Las aplicaciones instaladas en el perfil de trabajo aparecen en la lista común de aplicaciones.

Configuración del perfil de trabajo

Configuración del perfil de trabajo Android:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione **Perfil de trabajo de Android**.
5. En el espacio de trabajo **Perfil de trabajo de Android**, seleccione la casilla **Crear perfil de trabajo**.
6. Configure el perfil de trabajo:

   - Para habilitar Control de apps en el perfil de trabajo de Android y deshabilitarlo en el perfil personal, seleccione la casilla **Habilitar el Control de apps solo en el perfil de trabajo**.

     En la sección **Usuarios**, puede seleccionar **Control de apps** y usar el espacio de trabajo para crear listas de aplicaciones permitidas, bloqueadas, recomendadas y requeridas, así como categorías de aplicaciones permitidas y bloqueadas en la sección.

   - Para habilitar la Protección web para Google Chrome en el perfil de trabajo y deshabilitarla en el perfil personal, en el espacio de trabajo de la sección **Perfil de trabajo de Android**, seleccione la casilla **Habilitar protección web en el perfil de trabajo solamente**.

     La Protección web para el Navegador de Samsung bloquea sitios en los perfiles de trabajo y personales. No puede activar la Protección web para el Navegador de Samsung solo en el perfil de trabajo. Para usar la Protección web para el Navegador de Samsung en el perfil de trabajo, deshabilite la opción **Habilitar protección web en el perfil de trabajo solamente**. Si esta opción está activada, no se ejecuta la Protección web para el Navegador de Samsung. La Protección web en el perfil de trabajo está deshabilitada de forma predeterminada.

     La Protección web en dispositivos Android solo funciona en el navegador Google Chrome y en el Navegador de Samsung.

     Puede configurar el acceso a sitios web (crear una lista de categorías de sitios web bloqueados o una lista de sitios web permitidos) en la sección **Protección web**.

- Para impedir que el usuario copie datos mediante el portapapeles de aplicaciones del perfil de trabajo en aplicaciones personales, seleccione la casilla **Prohibir la transferencia de datos desde el perfil de trabajo al perfil personal**.

- Para evitar que el usuario utilice el modo de depuración de USB en el dispositivo móvil en el perfil de trabajo, seleccione la casilla **Prohibir la activación del modo de depuración USB**.

  En el modo de depuración de USB, el usuario puede descargar una app mediante una estación de trabajo, por ejemplo.

- Para prohibir al usuario instalar aplicaciones en el perfil de trabajo de Android desde todas las fuentes excepto Google Play, seleccione la casilla **Prohibir la instalación de aplicaciones en el perfil de trabajo desde orígenes desconocidos**.

- Para prohibir al usuario eliminar aplicaciones desde el perfil de trabajo de Android, seleccione la casilla **Prohibir la eliminación de aplicaciones del perfil de trabajo**.

7. Para configurar el perfil de trabajo en el dispositivo móvil del usuario, bloquee los cambios a la configuración.

8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil. El espacio del dispositivo móvil del usuario se divide en un perfil de trabajo y un perfil personal.

Agregar una cuenta LDAP

Para permitir al usuario del dispositivo iOS con MDM acceder a contactos corporativos en el servidor LDAP, agregue la cuenta LDAP.

Para añadir una cuenta LDAP del usuario del dispositivo iOS con MDM:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.

2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.

4. En la ventana **Propiedades** de la directiva, seleccione la sección **LDAP**.

5. Haga clic en el botón **Agregar** en la sección **Cuentas LDAP**.

   Se abre la ventana **Cuenta LDAP**.

6. En el campo **Descripción**, escriba una descripción de la cuenta LDAP del usuario. Puede usar las macros de la lista desplegable **Macros disponibles**.

7. En el campo **Nombre de la cuenta**, escriba el nombre de la cuenta para la autorización en el servidor LDAP. Puede usar las macros de la lista desplegable **Macros disponibles**.

8. En el campo **Contraseña**, escriba la contraseña de la cuenta LDAP para la autorización en el servidor LDAP.

9. En el campo **Dirección del servidor**, escriba el nombre de dominio del servidor LDAP. Puede usar las macros de la lista desplegable **Macros disponibles**.

10. Para usar el protocolo SSL (Secure Sockets Layer) de transporte de datos para proteger la transmisión de mensajes, active la casilla **Usar conexión SSL**.

11. Compile una lista de búsquedas del acceso del usuario del dispositivo móvil iOS con MDM a los datos corporativos del servidor LDAP:

    a. Haga clic en el botón **Agregar** en la sección **Configuración de búsqueda**.

    Aparece una fila vacía en la tabla con búsquedas.

    b. En la columna **Nombre**, escriba el nombre de una búsqueda.

    c. En la columna **Ámbito de búsqueda**, seleccione el nivel de anidamiento de la carpeta para la búsqueda de datos corporativos en el servidor LDAP:

    - **Base** – búsqueda en la carpeta base del servidor LDAP.
    - **Un nivel** – búsqueda en las carpetas del primer nivel de anidamiento contando desde la carpeta base.
    - **Subárbol** – búsqueda en las carpetas en todos los niveles de anidamiento contando desde la carpeta base.

    d. En la columna **Base de búsqueda**, 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.

12. Haga clic en **Aceptar**.

    La nueva cuenta LDAP aparece en la lista.

13. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

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 calendario

Para permitir al usuario del dispositivo iOS con MDM acceder a los eventos del calendario del usuario en el servidor CalDAV, agregue la cuenta CalDAV. La sincronización con el servidor CalDAV permite al usuario crear y recibir invitaciones, recibir actualizaciones de eventos y sincronizar tareas con la aplicación de recordatorios.

Para añadir una cuenta CalDAV del usuario del dispositivo iOS con MDM:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.

2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.

4. En la ventana **Propiedades** de la directiva, seleccione la sección **Calendario**.

5. Haga clic en el botón **Agregar** en la sección **Cuentas de CalDAV**.

   Se abre la ventana **Cuenta de CalDAV**.

6. En el campo **Descripción**, escriba una descripción de la cuenta de CalDAV del usuario.

7. En el campo **Dirección y puerto del servidor**, escriba el nombre del host o la dirección IP del servidor CalDAV y el número de puerto del servidor CalDAV.

8. En el campo **URL principal**, especifique la URL de la cuenta CalDAV del usuario del dispositivo iOS con MDM en el servidor CalDAV (por ejemplo: http://ejemplo.com/caldav/usuarios/miempresa/usuario).

   La URL del sitio web debe comenzar con `"http://"` o `"https://"`.

9. En el campo **Nombre de la cuenta**, escriba el nombre de la cuenta para la autorización en el servidor CalDAV.

10. En el campo **Contraseña**, establezca la contraseña de la cuenta de CalDAV para la autorización en el servidor CalDAV.

11. Para usar el protocolo SSL (Secure Sockets Layer) de transporte de datos para proteger la transmisión de información de eventos entre el servidor CalDAV y el dispositivo móvil, active la casilla **Usar conexión SSL**.

12. Haga clic en **Aceptar**.

    La nueva cuenta CalDAV aparece en la lista.

13. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Como resultado, luego de que se aplica la directiva, las cuentas CalDAV de la lista compilada se agregan al dispositivo móvil del usuario.

Agregar una cuenta de contactos

Para permitir al usuario del dispositivo iOS con MDM sincronizar información con el servidor CardDAV, agregue la cuenta CardDAV. La sincronización con el servidor CardDAV permite al usuario acceder a los detalles de contacto desde cualquier dispositivo.

Para Añadir una cuenta CardDAV del usuario del dispositivo iOS con MDM:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.

2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.

4. En la ventana **Propiedades** de la directiva, seleccione la sección **Contactos**.

5. Haga clic en el botón **Agregar** en la sección **Cuentas de CardDAV**.

   Se abre la ventana **Cuenta de CardDAV**.

6. En el campo **Descripción**, escriba una descripción de la cuenta de CardDAV del usuario. Puede usar las macros de la lista desplegable **Macros disponibles**.

7. En el campo **Dirección y puerto del servidor**, escriba el nombre del host o la dirección IP del servidor CardDAV y el número de puerto del servidor CardDAV.

8. En el campo **URL principal**, especifique la URL de la cuenta CardDAV del usuario del dispositivo iOS con MDM en el servidor CardDAV (por ejemplo: http://example.com/carddav/users/mycompany/user).

   La URL del sitio web debe comenzar con `"http://"` o `"https://"`.

9. En el campo **Nombre de la cuenta**, escriba el nombre de la cuenta para la autorización en el servidor CardDAV. Puede usar las macros de la lista desplegable **Macros disponibles**.

10. En el campo **Contraseña**, establezca la contraseña de la cuenta de CardDAV para la autorización en el servidor CardDAV.

11. Para usar el protocolo SSL (Secure Sockets Layer) de transporte de datos para proteger la transmisión de contactos entre el servidor CardDAV y el dispositivo móvil, active la casilla **Usar conexión SSL**.

12. Haga clic en **Aceptar**.

    La nueva cuenta CardDAV aparece en la lista.

13. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Como resultado, luego de que se aplica la directiva, las cuentas CardDAV de la lista compilada se agregan al dispositivo móvil del usuario.

Configuración de la suscripción al calendario

Para permitir al usuario del dispositivo iOS con MDM añadir eventos de calendarios compartidos (como el calendario corporativo) al calendario del usuario, agregue la suscripción a este calendario. Los *calendarios compartidos* son calendarios de otros usuarios que poseen una cuenta de CalDAV, un calendario iCal y otros calendarios publicados abiertamente.

Para añadir la suscripción al calendario:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.

2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.

4. En la ventana **Propiedades** de la directiva, seleccione la sección **Calendario suscrito**.

5. Haga clic en el botón **Agregar** en la sección **Calendarios suscritos**.

   Se abre la ventana **Calendario suscrito**.

6. En el campo **Descripción**, escriba una descripción de la suscripción al calendario.

7. En el campo **Dirección de servidor web**, especifique la dirección web del calendario de otras empresas.

   En este campo, puede ingresar la dirección de correo URL de la cuenta CalDAV del usuario a cuya cuenta se está suscribiendo. También puede especificar la URL de un calendario iCal o un calendario diferente abiertamente publicado.

8. En el campo **Nombre de usuario**, escriba el nombre de la cuenta de usuario para la autenticación en el servidor del calendario de terceros.

9. En el campo **Contraseña**, escriba la contraseña de la suscripción al calendario para la autenticación en el servidor del calendario de terceros.

10. Para usar el protocolo SSL (Secure Sockets Layer) de transporte de datos para proteger la transmisión de información de eventos entre el servidor CalDAV y el dispositivo móvil, active la casilla **Usar conexión SSL**.

11. Haga clic en **Aceptar**.

12. La nueva suscripción al calendario aparece en la lista.

13. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

    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.

Agregar clips web

Un *clip web* es una aplicación que abre un sitio web desde la pantalla de inicio del dispositivo. Cuando hace clic en los iconos de los clips web en la pantalla de inicio del dispositivo, el usuario puede abrir sitios web rápidamente (como el sitio web corporativo). Puede añadir clips web a dispositivos de usuarios y configurar el aspecto del icono del clip web que se muestra en la pantalla.

De forma predeterminada, se aplican las siguientes restricciones a la utilización de clips web:

- El usuario no puede quitar manualmente los clips web del dispositivo móvil.
- Los sitios web que se abren cuando el usuario hace clic en el icono de un clip web no se abren en el modo pantalla completa.
- Los efectos visuales de redondeo de bordes, sombra y brillo se aplican al icono del clip web en la pantalla.

Para añadir un clip web al dispositivo iOS con MDM de un usuario:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.

2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.

4. En la ventana **Propiedades** de la directiva, seleccione la sección **Clip web**.

5. Haga clic en el botón **Agregar** en la sección **Clip web**.

   Se abre la ventana **Clip web**.

6. En el campo **Nombre**, escriba el nombre del clip web a mostrar en la pantalla de inicio del dispositivo iOS con MDM.

7. En el campo **URL**, escriba la dirección web del sitio web que se abrirá cuando se haga clic en el icono del clip web. La dirección debe comenzar con `"http://"` o `"https://"`.

8. Para permitir al usuario eliminar un clip web del dispositivo iOS con MDM, active la casilla **Permitir eliminación**.

9. Haga clic en el botón **Seleccionar** y especifique el archivo con la imagen para el icono del clip web.

   El icono se muestra en la pantalla de inicio en el dispositivo iOS con MDM. La imagen debe cumplir con los siguientes requisitos:

   - Tamaño de la imagen de 400 x 400 píxeles como máximo.
   - Formato de archivo: GIF, JPEG o PNG.

- Tamaño del archivo no mayor a 1 MB.

Puede encontrar una vista previa del icono del clip web en el campo **Icono**. Si no selecciona una imagen para el clip web, se muestra un cuadrado en blanco como icono.

Si desea que el icono del clip web se muestre sin efectos visuales especiales (efecto de redondeo de bordes y brillo del icono), active la casilla **Icono precompuesto**.

10. Si desea que el sitio web se abra en modo pantalla completa en el dispositivo iOS con MDM cuando hace clic en el icono, active la casilla **Web clip de pantalla completa**.

11. Haga clic en **Aceptar**.

    El nuevo clip web aparece en la lista.

12. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Como resultado, luego de que se aplica la directiva, los iconos de los clips web de la lista que ha creado se agregan a la pantalla de inicio del dispositivo móvil del usuario.

Agregar fuentes

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

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de iOS con MDM pertenecen.

2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Abra la ventana de propiedades de la directiva haciendo doble clic en ella.

4. En la ventana **Propiedades** de la directiva, seleccione la sección **Fuentes**.

5. Haga clic en el botón **Agregar** en la sección **Fuentes**.

   Se abre la ventana **Fuente**.

6. En el campo **Nombre del archivo**, especifique la ruta al archivo de fuente (un archivo con extensión .ttf u .otf).

   No se admiten las fuentes con extensión .ttc u .otc.

   Las fuentes son identificadas utilizando nombres PostScript. No instale fuentes con el mismo nombre PostScript aunque su contenido sea distinto. Resulta en un error indefinido instalar las fuentes con el mismo nombre PostScript.

7. Haga clic en **Abierta**.

   La nueva fuente aparece en la lista.

8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Como resultado, luego de que se aplica la directiva, se le solicitará al usuario que instale fuentes de la lista que se ha creado.

Administrar la aplicación a través de sistemas EMM de otras empresas (solo para Android)

Puede usar la aplicación Kaspersky Endpoint Security para Android sin los sistemas de administración de Kaspersky. Utilice las soluciones de otros proveedores de servicios EMM (Enterprise Mobility Management) para instalar y administrar la aplicación Kaspersky Endpoint Security para Android. Kaspersky participa en la Comunidad AppConfig para garantizar que la aplicación opere con las soluciones EMM de otras empresas.

Puede administrar la aplicación Kaspersky Endpoint Security para Android a través de soluciones EMM de otras empresas solo en dispositivos con Android.

Puede usar las soluciones de terceros EMM para instalar solo la aplicación Kaspersky Endpoint Security para Android. Conecte el dispositivo a Kaspersky Security Center y administre la aplicación en la Consola de administración. En tal caso, la administración de la aplicación Kaspersky Endpoint Security para Android en la consola EMM no estará disponible.

Si instaló la aplicación Kaspersky Endpoint Security para Android con el sistema de terceros EMM, es imposible administrar la aplicación en Kaspersky Endpoint Security Cloud. Puede administrar la aplicación Kaspersky Endpoint Security para Android en la Consola EMM.

Las siguientes soluciones EMM admiten el uso de la aplicación Kaspersky Endpoint Security para Android:

- VMware AirWatch
- MobileIron
- IBM Maas360
- Microsoft Intune
- SOTI MobiControl

Puede realizar las siguientes acciones en la Consola EMM:

- Instale la aplicación a un perfil de trabajo de Android en los dispositivos de los usuarios.
- Activar la aplicación.
- Establecer la configuración de la aplicación:
  - Habilitar la protección contra sitios web maliciosos y de phishing en Internet.
  - Configure los ajustes para conectar el dispositivo a Kaspersky Security Center.
  - Establecer la configuración de Antirrobo.
  - Configure la programación para ejecutar un análisis de virus en el dispositivo.
  - Permita la detección de adware y aplicaciones que pueden ser utilizados para dañar su dispositivo o sus datos personales.

- Configure la programación para actualizaciones de la base de datos de la aplicación.

Guía de inicio rápido

Para instalar la aplicación en los dispositivos móviles de los usuarios, debe Añadir Kaspersky Endpoint Security para Android a la tienda de la aplicación EMM. Puede agregar Kaspersky Endpoint Security para Android a la tienda de la aplicación EMM usando un vínculo de Google Play. Para obtener más información sobre el funcionamiento con aplicaciones en Consola EMM, visite el *sitio web del Soporte Técnico del proveedor de servicios EMM*.

La aplicación Kaspersky Endpoint Security para Android se instala en un perfil de trabajo de Android. La aplicación se aísla de los datos personales del usuario y protege solo datos corporativos en el perfil de trabajo. Se recomienda asegurarse de que Kaspersky Endpoint Security para Android cuente con protección contra la eliminación por herramientas de Consola EMM.

Cómo instalar la aplicación

Según Console EMM, seleccione el método para instalar la aplicación en dispositivos: instalación silenciosa, enviar un correo electrónico que contenga un vínculo a la aplicación en Google Play u otro método disponible.

Para que la aplicación funcione, se requieren los siguientes permisos:

- Permiso de almacenamiento para acceder a los archivos cuando se ejecuta el antivirus (solo para Android 6.0 o versiones posteriores).
- Permiso telefónico para identificar el dispositivo, por ejemplo, al activar la aplicación.
- Solicitud para Añadir Kaspersky Endpoint Security para Android a la lista de aplicaciones que se abren al iniciarse el sistema operativo en ciertos dispositivos Huawei, Meizu y Xiaomi. Si la solicitud Añadir no se muestra, manualmente agregue Kaspersky Endpoint Security para Android a la lista de aplicaciones de inicio. La solicitud no se puede mostrar si la aplicación de seguridad no se instala en el perfil de trabajo.

Puede conceder los permisos requeridos en la Consola EMM antes de instalar la aplicación Kaspersky Endpoint Security para Android. Para obtener más información sobre la concesión de permisos en la Consola EMM, visite el *sitio web del soporte técnico del proveedor de servicios EMM*. También puede conceder los permisos mientras completa el Asistente de configuración inicial de Kaspersky Endpoint Security para Android en el dispositivo.

Se instalará la aplicación Kaspersky Endpoint Security para Android en el perfil de trabajo de Android.

Para la operación de la Protección web, también debe configurar un servidor proxy en la configuración Google Chrome:

- Modo de la configuración del servidor proxy: manual.
- Dirección y puerto del servidor proxy: 127.0.0.1:3128.
- Protocolo SPDY: desactivado.
- Compresión de datos a través de servidor proxy: desactivado.

Cómo activar la aplicación

Se transmite la información sobre la licencia al dispositivo móvil junto con la otra configuración en el archivo de configuración.

Si la aplicación no se activa en un plazo de 30 días después de su instalación en el dispositivo móvil, la licencia de prueba vence. Cuando caduca la licencia de evaluación, se desactivan todas las funciones de la aplicación móvil Kaspersky Endpoint Security para Android.

Cuando caduca la licencia comercial, la aplicación móvil sigue funcionando de manera limitada (por ejemplo, las actualizaciones de la base de datos de Kaspersky Endpoint Security para Android no están disponibles). Para seguir utilizando todas las funciones de la aplicación, es preciso renovar la licencia comercial.

Para activar Kaspersky Endpoint Security para Android:

1. En Console EMM, abra la configuración de la aplicación Kaspersky Endpoint Security para Android.
2. En el campo `LicenseActivationCode`, escriba el código de activación de la aplicación.

   Para activar la aplicación en un dispositivo, debe tener acceso a servidores de activación de Kaspersky.

Cómo conectar un dispositivo a Kaspersky Security Center

Después de instalar Kaspersky Endpoint Security para Android en un dispositivo móvil, puede conectar el dispositivo a Kaspersky Security Center. Los datos necesarios para conectar el dispositivo a Kaspersky Security Center se transmiten al dispositivo móvil junto con los demás ajustes que figuran en el archivo de configuración. Después de conectar el dispositivo a Kaspersky Security Center, puede utilizar directivas de grupo para establecer de forma centralizada la configuración de la aplicación. También puede recibir informes y estadísticas sobre el rendimiento de Kaspersky Endpoint Security para Android.

Antes de conectar dispositivos a Kaspersky Security Center, asegúrese de que se cumplan las siguientes condiciones:

- El complemento de administración Kaspersky Endpoint Security para Android esté instalado en la estación de trabajo del administrador.
- El puerto para conectar dispositivos móviles esté abierto en las propiedades del Servidor de administración.
- La visualización de la carpeta **Administración de dispositivos móviles** esté habilitada en la Consola de administración.
- Se haya creado un certificado general para identificar al usuario del dispositivo móvil en el almacenamiento de certificados de Kaspersky Security Center.

Antes de conectar los dispositivos a Kaspersky Security Center, se recomienda hacer lo siguiente:

- Si desea crear tareas y políticas para dispositivos móviles, cree un grupo de administración diferente para dispositivos móviles.
- Si desea mover dispositivos móviles de manera automática a un grupo de administración diferente, cree una regla para mover dispositivos automáticamente desde la carpeta **Dispositivos no asignados**.
- Si desea configurar Kaspersky Endpoint Security para Android de manera centralizada, cree una política de grupo.

Para conectar un dispositivo a Kaspersky Security Center:

1. En Console EMM, abra la configuración de la aplicación Kaspersky Endpoint Security para Android.
2. En el campo `KscServer`, escriba el nombre DNS o la dirección IP del Servidor de administración de Kaspersky Security Center. El puerto predeterminado es 13292.
3. Si no desea que las notificaciones de Kaspersky Endpoint Security para Android distraigan al usuario, deshabilite las notificaciones de la aplicación. Para ello, establezca la configuración `DisableNotification = True`.

   Después de conectarse, la aplicación muestra todas las notificaciones. Puede deshabilitar ciertas notificaciones de la aplicación en la configuración de la directiva.

   No deshabilite las notificaciones de la aplicación si no utiliza Kaspersky Security Center. Esto podría hacer que un usuario no reciba notificaciones sobre la expiración de la licencia. Como resultado, la aplicación dejará de cumplir su función.

Una vez configurada la conexión, Kaspersky Endpoint Security para Android muestra una notificación que le solicita que conceda los siguientes derechos y permisos adicionales:

- Permiso para usar la cámara para la operación antirrobo (comando **Foto de identificación**).
- Permiso para usar la ubicación para la operación antirrobo (comando **Localizar dispositivo**).
- Derechos de administrador del dispositivo (propietario del perfil de trabajo de Android) para el funcionamiento de las siguientes funciones de la aplicación:
  - Instalación de certificado de seguridad.
  - Configuración de Wi-Fi.
  - Configuración de Exchange ActiveSync.
  - Restricción del uso de la cámara, Bluetooth y Wi-Fi.

  Debido a las características específicas de un perfil de trabajo de Android (ausencia del servicio de accesibilidad), las funciones de Control de apps y Antirrobo no están disponibles en la aplicación.

Cuando el usuario otorga los derechos y permisos necesarios, el dispositivo se conecta a Kaspersky Security Center. Si no se creó una regla para mover dispositivos automáticamente a un grupo de administración, el dispositivo se agregará automáticamente a la carpeta **Dispositivos no asignados**. Si se creó una regla para mover dispositivos automáticamente a un grupo de administración, el dispositivo se agregará automáticamente al grupo definido.

Kaspersky Endpoint Security ofrece el siguiente formato de nombre de dispositivos:

- Modelo del dispositivo [correo electrónico, ID de dispositivo]
- Modelo del dispositivo [correo electrónico (si hay uno disponible) o ID de dispositivo]

Un ID de dispositivo es un ID exclusivo que genera Kaspersky Endpoint Security para Android a partir de los datos que recibe de un dispositivo. Para los dispositivos móviles que ejecutan Android 10 o posterior, Kaspersky Endpoint Security para Android usa el SSAID (ID de Android) o la suma de comprobación de otros datos recibidos del dispositivo. Para las versiones anteriores de Android, la aplicación usa el IMEI. Puede configurar el formato de nombre de dispositivo en la directiva de grupo. También puede agregar una etiqueta al nombre de dispositivo. Esto hace que sea más fácil encontrar y ordenar dispositivos en Kaspersky Security Center. La etiqueta solo está disponible para VMware AirWatch.

Para agregar la etiqueta al nombre del dispositivo:

1. En Console EMM, abra la configuración de la aplicación Kaspersky Endpoint Security para Android.
2. En el campo `KscDeviceNameTag`, seleccione los siguientes valores:
   - `{DeviceSerialNumber}`: Número de serie del dispositivo.
   - `{DeviceUid}`: Identificador único del dispositivo (UDID).
   - `{DeviceAssetNumber}`: Número de activo del dispositivo. Este número se crea internamente desde dentro de su organización.

   Recomendamos utilizar únicamente estos valores. VMware AirWatch admite otros valores, pero Kaspersky Endpoint Security no puede garantizar que vayan a funcionar.

Puede agregar algunos valores (por ejemplo, `{DeviceSerialNumber} {DeviceUid}`). La etiqueta se agregará al nombre del dispositivo en Kaspersky Security Center. Un espacio separa la etiqueta y el nombre del dispositivo. Por ejemplo, si el nombre del dispositivo es `Google Pixel 2 a10c6b75f7b31de9 22:7D:78:9E:C5:1E`, `22:7D:78:9E:C5:1E` es la etiqueta de UDID. Si utiliza Kaspersky Security Center y VMwareAirWatch, la etiqueta le permite identificar dispositivos en ambas consolas. Para emparejar el dispositivo, seleccione los mismos valores para el nombre del dispositivo (por ejemplo, el número de serie del dispositivo).

Una vez que el dispositivo está conectado a Kaspersky Security Center, la configuración de la aplicación se modifica de acuerdo con la directiva de grupo. Kaspersky Endpoint Security para Android ignora la configuración de la aplicación del archivo de configuración que se configuró en la Consola EMM. Puede configurar todas las secciones de la directiva excepto las siguientes:

- **Antirrobo** (Bloqueo del dispositivo)
- **Contenedores**
- **Administración del dispositivo** (Bloqueo de pantalla)
- **Control de apps** (Bloqueo de aplicaciones bloqueadas)
- **Perfil de trabajo de Android**
- **Administrar Samsung KNOX**

Debido al método utilizado para implementar un perfil de trabajo, no puede aplicar la configuración de directiva de grupo desde la sección **Perfil de trabajo de Android**. Esta configuración solo se puede aplicar si el perfil de trabajo se creó utilizando Kaspersky Security Center.

Archivo AppConfig

Se genera un archivo de configuración para configurar la aplicación en una consola EMM. Los ajustes de la aplicación en el archivo de configuración se presentan en la siguiente tabla.

Configuración de archivos

Clave de la configuración	Descripción	Tipo	Valor
`LicenseActivationCode`	Código de activación de la aplicación	String	Código de activación de la app que consiste en 20 letras y números latinos. Para activar la aplicación con un código de activación, se necesita acceder a Internet para conectarse a los servidores de activación de Kaspersky. Si deja el campo en blanco, la aplicación se activará con una licencia de prueba. La licencia de evaluación es válida durante 30 días. Cuando caduca la licencia de evaluación, se desactivan todas las funciones de la aplicación móv Kaspersky Endpoint Security para Android. Para continuar usando la aplicación, debe adquirir la versión comercial.
`EulaAcceptanceConfirmationV1`	<License Agreement link>	Choice	Esta configuración solo está disponible para VMware AirWatch. `Accepted`: Confirmo que he leído completamente, comprendo y acepto los términos y las condiciones de este Contrato de licencia de usuario final. `Declined`: No acepto los términos y las condiciones de este Contrato de licencia de usuario final (EULA). Para aceptar los términos y las condiciones del EULA para todos los dispositivos móviles, necesita acceder a Internet a fin de conectarse a los servidores de Kaspersky. Si elige `Declined`, la aplicación le pedirá al usuario que acepte los términos y las condiciones del EULA. Los usuarios del dispositivo móvil pueden aceptar las condiciones en el Asistente de configuración inicial.
`EulaAcceptanceCodeV1`	Código de Contrato de licencia	String	Esta configuración solo está disponible para VMware AirWatch.
`EulaAcceptanceCodesV2`	Códigos de	String	

	Contrato de licencia		Utilice `EulaAcceptanceCodeV1` si desea aceptar un único Contrato de licencia de usuario final (EULA). Utilice `EulaAcceptanceCodesV2` si desea aceptar varios EULA al mismo tiempo. E campo `EulaAcceptanceCodesV2` debe contener una lista de códigos EULA separados por punto y coma: `"<EULAid1>;<EULAid2>;<EULAid3>;..."`. El código del Contrato de licencia está incluido en el Contrato de licencia de usuario final. *Para conocer el código del Contrato de licencia:* 1. Copie el vínculo del Contrato de licencia (`EulaAcceptanceConfirmationV1` de la Consola EMM. 2. Pegue el vínculo en el navegador. Se abrirá el Contrato de licencia de usuario final (EULA). 3. Lea los términos y las condiciones de este EULA y busque el código del Contrato de licencia. Para aceptar los términos y las condiciones de los EULA para todos los dispositivos móviles, debe acceder a Internet a fin de conectarse a los servidores de Kaspersky. Si deja los campos en blanco, la aplicación le pedirá al usuario que acept los términos y las condiciones de los EULA. El usuario del dispositivo móvil puede aceptar las condiciones en el Asistente de configuración inicial. Si especifica los valores de ambos campos, se aceptarán los términos y las condiciones de todos los EULA especificados en ellos.
`KscServer`	Dirección y puerto del servidor de administración de Kaspersky Security Center	String	Nombre DNS o dirección IP del servidor de administración de Kaspersky Securit Center y número de puerto. Ingrese la dirección como se indica a continuación `<server address>:<port>`. Si ingres la dirección del servidor sin especificar e puerto, la aplicación utilizará el puerto predeterminado 13292.
`DisableNotification`	Deshabilite las notificaciones	Boolean	`True`: Kaspersky Endpoint Security para Android oculta todas las notificaciones

	de la aplicación antes de conectarse a Kaspersky Security Center		de la aplicación. Kaspersky Endpoint Security para Android oculta las notificaciones hasta que el dispositivo s conecta con Kaspersky Security Cente Después de conectarse, la aplicación muestra todas las notificaciones. Puede deshabilitar ciertas notificaciones de la aplicación en la configuración de la directiva. No deshabilite las notificaciones de la aplicación si no utiliza Kaspersky Security Center. Esto podría hacer que un usuario no vea las notificaciones sobre la expiración de la licencia. En este caso, la aplicación dejaría de funcionar. `False` – Kaspersky Endpoint Security para Android muestra todas las notificaciones de la aplicación.
`ScanScheduleType`	Modo de ejecución de análisis	Choice	`AfterUpdate` – Inicia un análisis antivirus después de una actualización de la base de datos. La aplicación actualiza las bases de datos antivirus según la programación definida `(UpdateScheduleType)`. `Daily` – Inicia un análisis antivirus una vez al día. Configure el tiempo de inicio de análisis `(ScanScheduleTime)`. `Weekly` – Inicia un análisis antivirus una vez por semana. Seleccione el día de la semana para iniciar un análisis de virus `(ScanScheduleDay)` y configurar el tiempo `(ScanScheduleTime)`. `Off` – Se deshabilita el inicio automátic un análisis antivirus. Independientemente del valor configurado, el usuario del dispositivo puede iniciar manualmente un análisis de virus.
`ScanScheduleDay`	Día del análisis	Choice	`Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday` Puede seleccionar solo un valor para este parámetro.
`ScanScheduleTime`	Hora del análisis	String	El tiempo se puede indicar en formato de 24 horas (por ejemplo, 13:00) o en formato de 12 horas (por ejemplo, 10:30 p. m.).
`ScanScheduleLock`	Bloquee la configuración del modo de	Boolean	`True` – El usuario no puede acceder a la configuración del modo de ejecución de

	ejecución de análisis		análisis antivirus en la configuración de l aplicación. `False` – El usuario puede configurar el modo de ejecución del análisis de virus y por ejemplo, deshabilitar el inicio automático de un análisis antivirus.
`ScanOnlyExecutableFiles`	Tipos de archivos para analizar (Análisis de virus)	Choice	`AllFiles` – Analiza todos los archivos. `OnlyExecutables` – Solo analiza archivos ejecutables. Los archivos ejecutables son archivos con extensiones .apk (.zip), .dex o .so. En Kaspersky Endpoint Security para Android Service Pack 4 Maintenance Release 1, no puede habilitar el análisis d archivos ejecutables únicamente.
`ScanArchives`	Desempaquetar y analizar archivos de almacenamiento	Boolean	`True` – La aplicación descomprime archivos y analiza su contenido. `False` – La aplicación solo analiza los archivos. La aplicación solo analiza archivos con extensión .zip (.apk). En Kaspersky Endpoint Security para Android Service Pack 4 Maintenance Release 1, no puede deshabilitar el análisis del contenido de los archivos.
`ScanActionOnThreatFound`	Acción al detectar una amenaza (Análisis de virus)	Choice	`Quarantine` – La aplicación pone objetos detectados en cuarentena. La cuarentena almacena los archivos como archivos comprimidos para que no puedan causar daños al dispositivo. El filtro de llamadas y mensajes de texto le permite eliminar o restaurar los archivos que se movieron a la cuarentena. `Delete` – La aplicación elimina el archiv detectado. `Skip` – La aplicación deja los objetos detectados sin alterar. Si las amenazas se han omitido, Kaspersky Endpoint Security para Android le advertirá al usuario sobre problemas en la protección del dispositivo. Cuando hay un intento de acceder a un objeto en el dispositivo (por ejemplo un intento de copiar o abrirlo), la aplicación bloquea el acceso al objeto. `AskUser` – La aplicación solicita al usuario seleccionar una acción para cad objeto detectado: omitir, poner en cuarentena o eliminar. Cuando se detectan varios objetos, el usuario puede aplicar una acción seleccionada a todos los objetos.

			Se registra la información sobre amenazas detectadas y las acciones tomadas sobre ellas en informes de la aplicación.
`ScanLock`	Bloquee la configuración de análisis	Boolean	`True` – El usuario no puede acceder a la siguiente configuración de análisis en la configuración de la aplicación: el tipo de archivos para analizar, análisis de archivos y la acción que se tomará cuando se detecta una amenaza. `False` – El usuario puede establecer la configuración de análisis y, por ejemplo, seleccionar la acción `Skip` para amenazas detectadas.
`ScanAndProtectionAdwareRiskware`	Bloquear adware, marcadores automáticos y aplicaciones que los delincuentes pueden utilizar para dañar el dispositivo y los datos del usuario	Boolean	`True`: La aplicación detecta el adware y otras aplicaciones que los delincuentes pueden utilizar para dañar el dispositivo los datos del usuario. `False`: La aplicación omite el adware y otras aplicaciones que los delincuentes pueden utilizar para dañar el dispositivo los datos del usuario.
`ProtectionMode`	Presione Modo de protección en tiempo real.	Choice	`Recommended` – La aplicación analiza solo nuevas aplicaciones una vez inmediatamente después de que se han instalado, así como archivos desde la carpeta Descargas. `Extended` – La aplicación analiza todos los archivos que el usuario abre, modifica, copia, ejecuta y guarda en el dispositivo. La aplicación también analiz aplicaciones y archivos nuevos desde la carpeta Descargas. `Disabled` – La protección en tiempo real está deshabilitada.
`UseKsnMode`	Modo Kaspersky Security Network	Choice	`Recommended` – La aplicación cambia datos con Kaspersky Security Network (KSN). Kaspersky Endpoint Security para Android usa KSN para la protección en tiempo real del dispositivo contra amenazas (Protección en la nube) y el funcionamiento de Protección web en Internet.

			`Extended` – La aplicación cambia datos con Kaspersky Security Network y también envía al Virus Laboratory (Laboratorio de virus) ciertas estadísticas de rendimiento de Kaspersky Endpoint Security para Android. Esta información permite hace un seguimiento de las amenazas en tiempo real. Los servicios de KSN no obtienen, procesan o almacenan datos personales. `Disabled` – La aplicación no usa datos desde Kaspersky Security Network. No puede habilitar la Protección web (`EnableWebFilter`). El componente Protección en la nube no está disponible para el Antivirus.
`ProtectScanOnlyExecutableFiles`	Tipos de archivos para analizar (Protección en tiempo real)	Boolean	`AllFiles` – Analiza todos los archivos. `OnlyExecutables` – Solo analiza archivos ejecutables. Los archivos ejecutables son archivos con extensiones .apk (.zip), .dex o .so. En Kaspersky Endpoint Security para Android Service Pack 4 Maintenance Release 1, no puede habilitar el análisis d archivos ejecutables únicamente.
`ProtectionActionOnThreatFound`	Acción al detectar una amenaza (Protección en tiempo real)	Choice	`Quarantine` – La aplicación pone objetos detectados en cuarentena. La cuarentena almacena los archivos como archivos comprimidos para que no puedan causar daños al dispositivo. La cuarentena le permite eliminar o restaurar los archivos que se movieron a almacenamiento aislado. `Delete` – La aplicación elimina el archiv detectado. `Skip` – La aplicación deja los objetos detectados sin alterar. Si las amenazas se han omitido, Kaspersky Endpoint Security para Android le advertirá al usuario sobre problemas en la protección del dispositivo. Cuando se produce un intento de acceder a un objeto en el dispositivo (por ejemplo, un intento de copiar o abrirlo), la aplicación bloquea el acceso al objeto. Se registra la información sobre amenazas detectadas y las acciones tomadas sobre ellas en informes de la aplicación.
`ProtectionLock`	Bloquee el ajuste de la configuración	Boolean	`True` – El usuario no puede acceder a la siguiente configuración de la protección en tiempo real en la configuración de la aplicación: modo de protección en

	de la protección en tiempo real		tiempo real, tipos de archivos para analizar, y la acción que se tomará cuando se detecta una amenaza. `False` – El usuario puede ajustar la configuración de la protección en tiempo real y, por ejemplo, seleccionar la acción `Skip` para amenazas detectadas
`UpdateScheduleType`	Modo de ejecución de actualización de Bases de datos	Choice	`Daily` – Examina nuevas bases de datos antivirus y las descarga a los dispositivos una vez al día. Configure el tiempo del inicio de actualización de la base de datos `(UpdateScheduleTime)`. `Weekly` – Examina nuevas bases de datos antivirus y las descarga a dispositivos una vez por semana. Seleccione el día de la semana para iniciar una actualización de la base de datos `(UpdateScheduleDay)` y configurar el tiempo `(UpdateScheduleTime)`. `Off` – Se deshabilita la actualización automática de bases de datos antivirus Independientemente del valor establecido, el usuario puede actualizar manualmente una base de datos antivirus.
`UpdateScheduleDay`	Día para iniciar una actualización de la base de datos	Choice	`Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday` Puede seleccionar solo un valor para este parámetro.
`UpdateScheduleTime`	Tiempo para iniciar la actualización de la base de datos	String	El tiempo se puede indicar en formato de 24 horas (por ejemplo, 13:00) o en formato de 12 horas (por ejemplo, 10:30 p. m.).
`UpdateScheduleLock`	Bloquee la configuración del modo de ejecución de actualización de la base de datos	Boolean	`True` – El usuario no puede acceder a la configuración del modo de ejecución de actualización de la base de datos en la configuración de la aplicación. `False` – El usuario puede configurar el modo de ejecución de actualización de base de datos y, por ejemplo, deshabilitar el inicio automático de las actualizaciones de la base de datos de antivirus.
`AllowUpdateInRoaming`	Actualización de bases de datos en roaming	Boolean	`True` – La aplicación descarga bases de datos antivirus si el dispositivo está en modo roaming. La aplicación descarga bases de datos antivirus según la programación definida `(UpdateScheduleType)`.

			`False` – La aplicación descarga bases de datos antivirus solo si el dispositivo está conectado a la red doméstica.
`EnableWebFilter`	Protección web	Boolean	`True`: La aplicación usa el componente Protección web para bloquear sitios wel maliciosos y de phishing en Internet. La Protección web solo admite Google Chrome. Se permite que los sitios web phishing y maliciosos que utilizan el protocolo HTTPS permanezcan desbloqueados si el dominio es de confianza. Si el dominio no es de confianza, la Protección web bloquea los sitios web maliciosos y de phishing. `False` – Se deshabilita la protección contra sitios web phishing y maliciosos. Para que el componente Protección we funcione, se deben cumplir las siguiente condiciones: • Los usuarios del dispositivo aceptan la Política de privacidad y la Declaración de protección web en el Asistente de configuración inicial o e la configuración de la aplicación. • Se configura un servidor proxy en la configuración del navegador: `ProxyMode = "fixed_servers"` `ProxyServer = "127.0.0.1:3128"` `DisableSpdy = true` `DataCompressionProxyEnabled false` La configuración del servidor proxy puede variar según la versión de Google Chrome. Para obtener más información sobre la configuración d Google Chrome, visite el sitio web de proyecto de Chromium. Después de que la aplicación Kaspersky Endpoint Security para Android se elimina del l dispositivo móvil, reinicie la configuración del servidor proxy. • El uso de KSN está activado en la configuración de la aplicación: `UseKsnMode = Recommended` o `UseKsnMode = Extended`. • Se recomienda seleccionar Google Chrome como el navegador

			predeterminado en la configuración del sistema operativo.
`EnableWebFilterLock`	Bloquee la configuración de Protección web	Boolean	`True` – El usuario no puede acceder a la configuración de la Protección web en la configuración de la aplicación. `False`: El usuario puede ajustar la configuración de Protección web y, por ejemplo, deshabilitar la protección contra sitios web maliciosos y de phishing en Internet.
`UpdateServer`	Dirección del servidor fuente de actualizaciones de la base de datos	String	Dirección del servidor que aloja las actualizaciones de la base de datos, por ejemplo, `http://update.server.com` Si deja el campo en blanco, Kaspersky Endpoint Security para Android usa los servidores de actualización de la base de datos de Kaspersky.
`AllowGoogleAnalytics`	Enviar datos a los servicios de Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics	Boolean	`True`: la aplicación envía automáticamente los datos de funcionamiento de Kaspersky Endpoint Security para Android a los servicios de Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics. Estos datos son necesarios para mejorar el funcionamiento de la aplicación y analizar la satisfacción del usuario. Los datos se transfieren a los servicios de Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics a través de una conexión segura. El acceso a los datos y su protección están regulados por los correspondientes términos de uso de los servicios de Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics. `False`: se deshabilita el envío de datos los servicios de Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics.
`KscDeviceNameTag`	Etiqueta de nombre de dispositivo para Kaspersky Security Center	String	Esta configuración solo está disponible para VMware AirWatch.

			La etiqueta se agregará al nombre del dispositivo en Kaspersky Security Center. Un espacio separa la etiqueta y el nombre del dispositivo. Esto hace que sea más fácil encontrar y ordenar dispositivos en Kaspersky Security Center. • `{DeviceSerialNumber}`: Número de serie del dispositivo. • `{DeviceUid}`: Identificador único d dispositivo (UDID). • `{DeviceAssetNumber}`: Número de activo del dispositivo. Este número s crea internamente dentro de su organización. Puede agregar algunos valores (por ejemplo, `{DeviceSerialNumber}` `{DeviceUid}`). Recomendamos utilizar únicamente estos valores. VMware AirWatch admite otros valores, pero Kaspersky Endpoint Security no puede garantizar que funcionen.
`KscGroup`	Nombre del grupo de dispositivos	String	Puede especificar grupos de dispositivos en una consola EMM. Cuando un dispositivo se conecta a Kaspersky Security Center, se añadirá automáticamente a una subcarpeta de carpeta de dispositivos No asignados. E nombre de la subcarpeta coincidirá con el nombre del grupo especificado en este parámetro. Después, puede crear reglas para el traslado automático de dispositivos, desde las subcarpetas de l carpeta Dispositivos no asignados a grupos de administración en la carpeta Dispositivos administrados. Si deja el campo en blanco, el dispositivo se añadirá automáticamente a la raíz de la carpeta Dispositivos no asignados.
`KscCorporateEmail`	Correo electrónico corporativo del usuario	String	Puede especificar las direcciones de correo electrónico corporativo de los usuarios en una consola EMM. Estos correos electrónicos se visualizarán en Kaspersky Security Center. La cadena debe ser una dirección de correo electrónico válida. Otros valores no se tienen en cuenta.

Carga de red

Esta sección contiene información sobre el volumen de tráfico de red que se intercambia entre dispositivos móviles y Kaspersky Security Center.

Volumen de tráfico

Tarea	Tráfico saliente	Tráfico entrante	Tráfico Total
Uso inicial de la aplicación, Mb	0,08	17,76	17,84
Actualización inicial de las bases de datos antivirus (el volumen de tráfico se puede diferenciar debido al tamaño de las bases de datos antivirus), MB	0,04	2,21	2,25
Sincronización del dispositivo móvil con Kaspersky Security Center, MB	0,03	0,02	0,05
Actualización habitual de las bases de datos antivirus (el volumen de tráfico se puede diferenciar debido al tamaño de las bases de datos antivirus), MB	0,08	3,06	3,14
Ejecución de comandos Antirrobo. Localice el dispositivo (el volumen de tráfico se puede diferenciar debido a las especificaciones de la cámara incorporada y la calidad de imágenes), MB	0,09	0,8	0,17
Ejecución de comandos Antirrobo. Foto de identificación, MB	1,0	0,02	1,02
Ejecución de comandos Antirrobo. Bloqueo del dispositivo, MB	0,06	0,05	0,11
Volumen promedio diario, MB	0,22	6,96	7,18

Participación en Kaspersky Security Network

Para proteger los dispositivos móviles con más eficacia, Kaspersky Endpoint Security para Android usa datos recopilados 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 en línea 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 recopilar información en tiempo real sobre tipos y fuentes de amenazas nuevas, a desarrollar métodos para neutralizarlas y a reducir las falsas alarmas de Kaspersky Endpoint Security para Android. Participar en Kaspersky Security Network también le permite acceder a estadísticas de reputación de aplicaciones y sitios web.

Cuando participa en Kaspersky Security Network, ciertas estadísticas se obtienen mientras Kaspersky Endpoint Security for Android se está 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 puedan 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 la operación de Kaspersky Endpoint Security para Android. KSN se utiliza en los componentes principales de la aplicación: Antivirus, Protección web y Control de apps. 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. Al leer el Contrato de licencia de usuario final, podrá saber cuáles son los datos que Kaspersky Endpoint Security para Android transmitirá 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 transmite a Kaspersky Security Network.

Intercambio de información con Kaspersky Security Network

Para mejorar la protección en tiempo real, Kaspersky Security para dispositivos móviles utiliza Kaspersky Security Network para el funcionamiento de los siguientes componentes:

- **Antivirus.** La aplicación obtiene acceso a la base de conocimientos de Kaspersky para consultar por la reputación de los archivos y aplicaciones. El análisis se realiza para amenazas cuya información aún no se ha añadido a las bases de datos antivirus, pero que ya está disponible en KSN. El servicio en la nube de Kaspersky Security Network permite el funcionamiento completo del antivirus y reduce la posibilidad de falsas alarmas.

- **Protección web.** La aplicación usa datos recibidos de KSN para ejecutar un análisis de los 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 aplicaciones 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 Antivirus y Control de apps 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.

Con el objetivo de identificar las amenazas de seguridad de la información emergentes, las amenazas de intrusión y las amenazas que son difíciles de detectar (junto con sus respectivas fuentes), y para mejorar la protección de la información almacenada y procesada con su dispositivo, podrá extender 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.

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 Security for Mobile (Devices) también cambiará a *Advertencia*.

- 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. 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.

Para obtener más información sobre la provisión de datos a KSN, consulte la sección "Provisión de datos".

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 que utilizan Kaspersky Security Network, la aplicación envía solicitudes a los servicios en la nube. Las solicitudes contienen los datos descritos en la sección "Provisión de datos".

Si se deshabilita el uso de Kaspersky Security Network en el dispositivo, los componentes Protección en la nube, Protección web y Control de apps se deshabilitan automáticamente.

Para habilitar o deshabilitar el uso de Kaspersky Security Network:

1. Abra la ventana con la configuración de la directiva de administración para dispositivos móviles en los que está instalado Kaspersky Endpoint Security para Android.
2. En la ventana **Propiedades** de la directiva, seleccione la sección **Adicional**.
3. En la sección de **Configuración de Kaspersky Security Network (KSN)**, ajuste la configuración para usar Kaspersky Security Network:
   - Seleccione la casilla **Usar Kaspersky Security Network** para la operación de los siguientes componentes: Antivirus (Protección en la nube), Protección web y Control de apps (Categorías de la aplicación).
   - Seleccione la casilla **Permitir el envío de estadísticas a KSN** 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.
4. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil. Una vez aplicada la directiva, los componentes que utilizan Kaspersky Security Network se deshabilitan y la configuración de los componentes deja de estar disponible.

Uso de Kaspersky Private Security Network

Kaspersky Private Security Network (en lo sucesivo, también denominado *KSN privada* o *KPSN)* es una solución que otorga acceso a las bases de datos de reputación de Kaspersky Security Network, sin enviar datos a Kaspersky Security Network desde los dispositivos de los usuarios.

Una base de datos de reputación de objetos (archivos o URL) se almacena en el servidor de Kaspersky Private Security Network, pero no en los servidores de Kaspersky Security Network. Las bases de datos de reputación de KPSN se almacenan dentro de la red corporativa y son administradas por el administrador de la empresa.

Cuando KPSN está habilitado, Kaspersky Endpoint Security no envía ningún dato estadístico a KSN desde los dispositivos de los usuarios.

Para habilitar el uso de KSN privada a través de Kaspersky Security Center:

1. En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, haga clic en **Configuración** ( ).

   Se abrirá la ventana de propiedades del Servidor de administración.

2. En la pestaña **General**, seleccione la sección **Configuración de Proxy KSN.**

3. Cambie el botón de alternancia **Usar Kaspersky Private Security Network a la posición ACTIVADO**.

4. Haga clic en el **botón Seleccionar archivo con configuración de Proxy KSN** y luego busque un archivo de configuración que tenga la extensión pkcs7 o pem (proporcionado por Kaspersky).

5. Haga clic en **Abierta**.

6. Si definió la configuración del servidor proxy en las propiedades del Servidor de administración, pero la arquitectura de su red requiere que use una KSN privada directamente, habilite la opción **Ignorar la configuración del servidor proxy KSC al conectarse a KSN privada**. De lo contrario, las solicitudes de las aplicaciones administradas no pueden alcanzar la KSN privada.

7. Haga clic en el botón **Guardar**.

Después de descargar la configuración, la interfaz muestra el nombre y los contactos del proveedor, así como la fecha de creación del archivo con la configuración de la KSN privada. La configuración de KPSN se aplica a los dispositivos móviles.

Cuando cambia a KSN privada, Control de apps no es compatible con las categorías de aplicaciones disponibles cuando usa Global KSN. La categorización de aplicaciones estará disponible si elige volver a KSN.

Provisión de datos a servicios de terceros

Kaspersky Endpoint Security para Android utiliza los servicios de Google™ conocidos como Firebase Cloud Messaging, Google Analytics para Firebase™, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics. Kaspersky Endpoint Security para Android usa el servicio Firebase Cloud Messaging (FCM) para asegurar la entrega oportuna de los comandos a los dispositivos móviles y la sincronización forzada cuando se cambia la configuración de la directiva. Kaspersky Endpoint Security para Android utiliza los servicios de Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics para mejorar el rendimiento de la aplicación y ayudar a Kaspersky a crear materiales de marketing más efectivos.

Intercambio de información con Firebase Cloud Messaging

Kaspersky Endpoint Security para Android usa el servicio Firebase Cloud Messaging (FCM) para asegurar la entrega oportuna de los comandos a los dispositivos móviles y la sincronización forzada cuando se cambia la configuración de la directiva. La aplicación también usa notificaciones push.

Para usar el servicio de Firebase Cloud Messaging, debe configurar el servicio en Kaspersky Security Center. Para obtener más información sobre cómo configurar Firebase Cloud Messaging en Kaspersky Security Center, consulte la *ayuda de Kaspersky Security Center*. Si no se configura Firebase Cloud Messaging, los comandos en el dispositivo móvil y la configuración de las directivas se enviarán cuando el dispositivo se sincronice con Kaspersky Security Center según el cronograma establecido en la directiva (por ejemplo, cada 24 horas). En otras palabras, los comandos y la configuración de las directivas se enviarán con un retraso.

Con el fin de contribuir al funcionamiento principal del producto, se compromete a proporcionar automáticamente al servicio Firebase Cloud Messaging el ID único de la instalación de la aplicación (ID del caso), y los siguientes datos:

- Información sobre el software instalado: versión de la aplicación, ID de la aplicación, versión de la aplicación, nombre del paquete de la aplicación.
- Información sobre el equipo en el cual el software se instala: versión del SO, ID del dispositivo, versión de los servicios de Google.
- Información sobre FCM: ID de la aplicación en FCM, ID del usuario de FCM, versión del protocolo.

Los datos se transmiten a los servicios Firebase mediante una conexión segura. El acceso y la protección de la información se rigen conforme a las condiciones de uso del servicio de Firebase pertinentes: https://firebase.google.com/terms/data-processing-terms/, https://firebase.google.com/support/privacy/.

Para evitar el intercambio de información con el servicio de Firebase Cloud Messaging:

1. En el árbol de la consola, seleccione **Administración de dispositivos móviles → Dispositivos móviles**.
2. En el menú contextual de la carpeta **Dispositivos móviles**, seleccione **Propiedades**.
3. En la ventana de propiedades de la carpeta **Dispositivos móviles**, seleccione la sección de **configuración de Google Firebase Cloud Messaging**.
4. Haga clic en el botón **Restablecer configuración**.

Intercambio de información con Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics

Si utiliza el complemento de administración de una versión anterior y ha habilitado el intercambio de datos con el servicio de Google Analytics, Kaspersky Endpoint Security para Android Service Pack 4 Maintenance Release 3 realizará el intercambio de datos con el servicio de Google Analytics para Firebase. El soporte de Google Analytics ha sido discontinuado.

Kaspersky Security para dispositivos móviles intercambia datos con los servicios de Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics con los siguientes objetivos:

- Para mejorar el rendimiento de la aplicación.

  Para intercambiar datos con los servicios de Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics con el fin de mejorar el rendimiento de la aplicación, se deben cumplir las siguientes condiciones:

  - El administrador 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.

    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 Security for Mobile (Devices) también cambiará a *Advertencia*.

  - El administrador debe configurar la directiva de grupo para permitir que se envíen estadísticas a KSN (véase abajo).

- Para ayudar a Kaspersky a crear materiales de marketing más efectivos.

  Para intercambiar datos con los servicios de Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics con el fin de ayudar a Kaspersky a crear materiales de marketing efectivos, se deben cumplir las siguientes condiciones:

  - El administrador o el usuario del dispositivo deben leer y aceptar los términos de la Declaración en cuanto al procesamiento de la información con propósitos de marketing. Si elige que los usuarios acepten la Declaración, podrán aceptar los términos de la Declaración cuando instalen la aplicación o en la sección **Acerca de la aplicación** en la configuración de Kaspersky Endpoint Security para Android.

  - El administrador debe ajustar la configuración de la directiva de grupo para permitir el envío de datos a Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics (véase abajo).

[Provisión de datos a Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics según la declaración sobre el procesamiento de datos con 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 de diagnóstico sobre el dispositivo del servicio de SafetyNet Attestation
- información sobre la configuración de Kaspersky Endpoint Security para Android como una función de accesibilidad
- información sobre transiciones entre pantallas de aplicaciones, duración de la sesión, inicio y final de una sesión de pantalla, nombre de 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 la bases de datos antivirus y sincronización con el Servidor Administrativo
- 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: el grupo etario y el género, el identificador de país de residencia y la lista de intereses
- información sobre la computadora del Usuario en la que se instaló el Software: el nombre del fabricante del equipo, el tipo de equipo, el modelo, la 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 que 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.

Certificación de SafetyNet

Durante el uso del Software, se enviarán los siguientes datos a SafetyNet Attestation automáticamente y de manera periódica a fin de alcanzar el propósito declarado:

- hora de verificación del dispositivo
- información sobre el software, nombre y datos de los certificados del software
- resultados de verificación del dispositivo
- verificaciones de identidad aleatorias para verificar los resultados de la verificación del dispositivo

  La transmisión de datos a SafetyNet Attestation se realiza a través de un canal seguro. La información sobre cómo se procesan los datos en SafetyNet Attestation se publica en: https://policies.google.com/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 app
- 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 destrabado o tiene acceso a los permisos de administración (root)
- fuerza de la señal
- duración de los rastros automatizados
- red y la información correspondiente a continuación: código de respuesta, tamaño de la 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 se encuentra 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 del dispositivo
- espacio total del disco y cantidad usada actualmente
- nombre y versión del SO
- RAM total y cantidad usada actualmente
- mensaje que indica si el dispositivo tiene acceso a los permisos de administración (root)
- orientación de la pantalla al momento del evento
- fabricante del producto/hardware
- ID de instalación único
- versión de las estadísticas enviadas
- tipo de excepción de Software
- texto del mensaje de error
- marca que indica que la excepción de Software fue provocada por una excepción anidada
- ID de subproceso
- marca que indica si el marco fue el motivo del error de Software
- marca que indica que el subproceso provocó el cierre inesperado del Software
- información sobre la señal que provocó el cierre inesperado del Software: nombre de la señal, código de la señal, dirección de la señal
- para cada marco asociado con un subproceso, una excepción o un error: el 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 eventos ion que se produjeron antes del cierre inesperado del Software: identificador de 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 está publicada en: https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

Proporcionar la información anterior para procesamiento con fines de marketing es voluntario.

Para deshabilitar el intercambio de datos con los servicios de Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics:

1. Abra la ventana de configuración de la directiva de administración de los dispositivos móviles en los que está instalada la aplicación Kaspersky Endpoint Security para Android.
2. En la ventana **Propiedades** de la directiva, seleccione la sección **Adicional**.
3. En la sección **Transferencia de datos**, desmarque la casilla de verificación **Permitir la transferencia de datos para mejorar la calidad, la apariencia y el rendimiento de la aplicación**.
4. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Aceptación global de declaraciones adicionales

Para habilitar la protección proporcionada por Kaspersky Endpoint Security para Android, se deben aceptar los términos del Contrato de licencia de usuario final, así como las declaraciones adicionales (ver abajo). Usted puede configurar una política para aceptar las declaraciones que se enumeran a continuación de forma global, para todos los usuarios. No se les pedirá a los usuarios que lean y acepten los términos de los siguientes contratos y declaraciones que ya se aceptaron globalmente:

- Declaración de Kaspersky Security Network
- Declaración sobre el procesamiento 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 Security for Mobile (Devices) también cambiará a *Advertencia*.

Para elegir si los términos se deben aceptar globalmente o si deben hacerlo los usuarios mediante la aplicación de una política de grupo:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Adicional**.
5. En la sección **Transferencia de datos**, elija si la declaración sobre el procesamiento de datos con propósitos de marketing se aceptará globalmente o la aceptarán los usuarios.
6. En la sección **Configuración de Kaspersky Security Network (KSN)**, elija si la declaración de Kaspersky Security Network se aceptará globalmente o la aceptarán los usuarios.
7. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

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.

Samsung KNOX

Samsung KNOX es una solución móvil para configurar y proteger dispositivos móviles Samsung que utilizan el sistema operativo Android. Para obtener más información sobre Samsung KNOX, visite el *sitio web del soporte técnico de Samsung*.

Instalación de la aplicación Kaspersky Endpoint Security para Android a través de KNOX Mobile Enrollment

KNOX Mobile Enrollment (KME) es parte de la solución móvil de Samsung KNOX. Se utiliza para la instalación de lotes y la configuración inicial de aplicaciones en dispositivos Samsung nuevos comprados a proveedores oficiales.

La instalación de la aplicación Kaspersky Endpoint Security para Android mediante KNOX Mobile Enrollment consiste en los siguientes pasos:

1. La creación de un perfil de MDM KNOX con la aplicación Kaspersky Endpoint Security para Android.
2. Agregar dispositivos a KNOX Mobile Enrollment.
3. Instalar la aplicación Kaspersky Endpoint Security para Android en el dispositivo móvil del usuario.

Para obtener más información sobre el funcionamiento con KNOX Mobile Enrollment, consulte la *Guía del usuario de KNOX Mobile Enrollment*.

La instalación a través de KNOX Mobile Enrollment solo es posible para dispositivos Samsung. Para la lista de dispositivos admitidos, visite el *sitio web del Soporte Técnico de Samsung*.

Crear un perfil de MDM KNOX

Un perfil *MDM KNOX* es un perfil que contiene vínculos a aplicaciones para una rápida instalación y configuración inicial en dispositivos móviles.

Crear un perfil MDM KNOX:

1. Inicie sesión en la consola Samsung KNOX → **KNOX Mobile Enrollment**.
2. Seleccione la sección **Perfiles de MDM**.
3. Haga clic en **Agregar**.

   Se inicia el Nuevo Asistente de Perfil de MDM KNOX.
4. En el paso **Conexión del servidor MDM**, seleccione **No se requiere URI del servidor para mi servicio de MDM** y haga clic en **Siguiente**.
5. En el paso **Información del perfil MDM**:
   a. Introduzca información general sobre el perfil MDM de KNOX: **Nombre de perfil** y **Descripción**.
   b. Haga clic en el botón **Añadir aplicaciones de MDM** e ingrese la ruta al archivo de instalación APK.

      Se incluye el archivo de instalación para Kaspersky Endpoint Security para Android en el Kit de distribución móvil Kaspersky Security. De antemano, coloque el archivo de instalación APK en el Servidor web de Kaspersky Security Center o en otro servidor que sea accesible para descargar desde el dispositivo.
   c. Ingrese la configuración para conectar el dispositivo a Kaspersky Security Center en el campo **Datos del usuario JSON** en el siguiente formato:
      `{"serverAddress":"ksc.server.com","serverPort":"12345","groupName":"MOBILE GROUP"}`.

      El dispositivo se debe conectar a Kaspersky Security Center para activar la aplicación, configurar el dispositivo y enviar comandos.
   d. Seleccione la casilla de verificación **Añadir acuerdos de Knox**.

      Para instalar la Kaspersky Endpoint Security para Android mediante la inscripción móvil de KNOX, el usuario del dispositivo móvil debe aceptar las condiciones del contrato de licencia de Samsung. Puede ver las condiciones del Contrato de licencia de Samsung en la sección titulada **Acuerdos de licencia de usuario final, Términos de servicio y Contratos de usuario**. También puede añadir otros documentos oficiales de su empresa que sean necesarios para desplegar un perfil MDM de KNOX haciendo clic en el botón **Añadir contrato de usuario**.
   e. Retire la selección de la casilla de verificación **Vincular licencia de Knox con este perfil**.

      La información de la licencia de KNOX de Samsung se enviará al dispositivo móvil junto con la política al sincronizar el dispositivo con Kaspersky Security Center.
6. Haga clic en el botón **Guardar**.

Por lo tanto, se agregará el nuevo perfil MDM KNOX con la aplicación Kaspersky Endpoint Security para Android a la lista en la consola KME.

Agregar dispositivos a KNOX Mobile Enrollment

Los dispositivos se pueden agregar en la consola KNOX Mobile Enrollment (KME) de los siguientes modos:

- El proveedor automáticamente agrega dispositivos a la consola KME después de que los dispositivos se compran.

  Seleccione este método si su organización está funcionando con un proveedor oficial de dispositivos de Samsung.

- El administrador instala la aplicación de Instalación KNOX desde Google Play a su dispositivo móvil y emigra el perfil MDM KNOX a los dispositivos de los usuarios a través de Bluetooth o NFC (Near Field Communication). Después de la instalación del perfil MDM KNOX, el dispositivo automáticamente se agregará a la consola KME.

  Seleccione este método si los dispositivos de Samsung no se compraron desde un proveedor oficial.

Agregar un dispositivo a través del proveedor

Se registra un proveedor oficial de dispositivos de Samsung en Samsung KNOX. Para la lista de proveedores oficiales, visite el *sitio web del Soporte Técnico de Samsung*. El proveedor automáticamente agrega los dispositivos en la consola de KME para su cuenta de Samsung inmediatamente después de que los dispositivos se compran. Para agregar los dispositivos por el proveedor, debe registrar al proveedor en la consola KME para su cuenta de Samsung. Necesitará un ID del revendedor para agregar al proveedor de dispositivos Samsung en la consola KME. Para recibir el ID del revendedor, debe enviar una solicitud al proveedor. En la solicitud, especifique su ID del cliente KNOX.

Ver su ID de cliente KNOX:

1. Inicie sesión en la consola Samsung KNOX → **KNOX Mobile Enrollment**.
2. Seleccione la sección **Revendedores**.
3. Su ID se muestra en el campo de **ID del cliente KNOX**.

Después de que reciba una respuesta del proveedor con el ID del revendedor, registre al proveedor en la consola KME. Antes del registro del proveedor, puede crear un perfil MDM KNOX de modo que el perfil se pueda implementar automáticamente al agregar dispositivos nuevos.

Registrar a un proveedor oficial en la consola KME:

1. Inicie sesión en la consola Samsung KNOX → **KNOX Mobile Enrollment**.
2. Seleccione la sección **Revendedores**.
3. Haga clic en el botón **Registrar revendedor**.

   Esto abre una ventana para registrar al proveedor del dispositivo.
4. En el campo **ID del Revendedor**, escriba el ID recibido del proveedor oficial de dispositivos de Samsung.
5. Si creó un perfil MDM KNOX, seleccione el perfil MDM KNOX en la ventana de registro del proveedor.

   Cuando agrega dispositivos nuevos, el perfil MDM KNOX se instala en forma automática.

6. En la lista **Método de confirmación de descarga preferido**, seleccione un método para confirmar la adición de un dispositivo para un proveedor.

   - **Todas las descargas se deben confirmar**. Cuando el proveedor agregue un dispositivo, tendrá que confirmar la operación.

   - **Automáticamente confirme todas las descargas de este revendedor**. Los dispositivos del proveedor automáticamente se agregarán a la consola KME.

7. Haga clic en **Aceptar**.

El proveedor de dispositivos de Samsung se agregará a la lista de proveedores en la consola KME.

Luego de comprar los dispositivos desde el proveedor oficial, la aplicación Kaspersky Endpoint Security para Android se instalará automáticamente en los dispositivos después de que estos se conecten a Internet. Para obtener más información sobre el funcionamiento con KNOX Mobile Enrollment, consulte la *Guía del usuario de KNOX Mobile Enrollment*. Si ya tiene una lista de dispositivos en la consola KME, agregue el perfil MDM KNOX con la aplicación de MDM KNOX al dispositivo.

Entregar un perfil MDM KNOX a dispositivos:

1. Inicie sesión en la consola Samsung KNOX → **KNOX Mobile Enrollment**.

2. Seleccione **Dispositivos** → **Todos los dispositivos**.

3. Seleccione los dispositivos en los cuales desea instalar el perfil MDM KNOX.

4. Haga clic en el botón **Configurar**.

   Se abre la ventana **Información del dispositivo**.

5. En la lista **Perfil MDM**, seleccione el perfil MDM KNOX con la aplicación Kaspersky Endpoint Security para Android.

6. En el campo **Etiquetas**, escriba etiquetas para agrupar y poner etiqueta a dispositivos, y para la optimización de búsqueda en la consola KME.

7. Ingrese las credenciales de la cuenta de usuario del dispositivo en los campos **Contraseña** e **ID de usuario**.

   Se requieren credenciales de cuenta para recibir un certificado general. El ID de usuario y la contraseña deben coincidir con las credenciales de la cuenta de usuario en Kaspersky Security Center (Nombre completo y Contraseña en propiedades de la cuenta de usuario).

8. Seleccione el perfil MDM KNOX para los dispositivos restantes.

9. Haga clic en el botón **Guardar**.

Después de que el dispositivo se conecte a Internet, se le solicitará al usuario instalar el perfil MDM KNOX.

Agregar un dispositivo a través de la aplicación de Implementación KNOX

Si no compró su dispositivo de Samsung desde un proveedor oficial, puede agregar el dispositivo a KNOX Mobile Enrollment a través de Bluetooth o NFC. Esto requerirá el dispositivo móvil del administrador que será usado para entregar perfiles de MDM KNOX a los dispositivos móviles de los usuarios.

Para agregar dispositivos usando la aplicación de Implementación KNOX, se deben cumplir las siguientes condiciones:

- Según el modo de entrega seleccionado, se debe habilitar Bluetooth o los módulos NFC en los dispositivos móviles.
- Los dispositivos móviles deben estar conectados a Internet.

Entregar un perfil MDM KNOX usando la aplicación de Implementación KNOX:

1. Instalar la aplicación KNOX Deployment desde Google Play en el dispositivo móvil del administrador.
2. Inicie la aplicación KNOX Deployment.
3. Ingrese sus credenciales de la cuenta de Samsung.
4. En la ventana **KNOX Deployment**, ajuste la configuración para instalar un perfil MDM KNOX:
   - Seleccione el perfil MDM KNOX.
   - Seleccione el modo de instalar: **Bluetooth** o **NFC**.

     Al usar Bluetooth, puede agregar un perfil MDM KNOX a varios dispositivos al mismo tiempo.
5. Haga clic en **Iniciar instalación**:
   - **Bluetooth**. En el dispositivo móvil del usuario, abra el sitio web https://configure.samsungknox.com.

     Esto inicia el Asistente de Registro del Dispositivo de Samsung KNOX. Siga las instrucciones en la pantalla.

     Después de que se instale el perfil MDM KNOX, se agregará el dispositivo nuevo con la etiqueta **Bluetooth** a la consola KME.
   - **NFC**. Acerque el dispositivo móvil del administrador al dispositivo móvil del usuario y transfiera el perfil MDM de KNOX.

     En el dispositivo móvil del usuario se solicitará la instalación del perfil MDM de KNOX. El dispositivo nuevo con la etiqueta **NFC** se agregará a la consola KME.

Instalar la aplicación

Antes de la instalación de la aplicación Kaspersky Endpoint Security para Android, emita un certificado general para usuarios del dispositivo móvil en la Consola de administración de Kaspersky Security Center. Se requiere un certificado general para identificar al usuario del dispositivo móvil en la Consola de administración de Kaspersky Security Center.

Después de iniciar la instalación del perfil MDM KNOX, el archivo de instalación APK se descargará en forma automática en el dispositivo móvil. Se inicia la instalación de la aplicación Kaspersky Endpoint Security para Android automáticamente. El usuario debe aceptar el Contrato de licencia de Samsung KNOX y el Contrato de licencia de Kaspersky Endpoint Security para Android. No se requiere ninguna configuración adicional de la aplicación. Después de que la aplicación se instale, la sincronización con Kaspersky Security Center se realizará automáticamente. El dispositivo móvil se añadirá a la Consola de administración de Kaspersky Security Center al grupo de administración especificado en la configuración del Perfil MDM KNOX (`groupName`).

Configurar contenedores KNOX

Esta sección contiene información sobre cómo trabajar con contenedores KNOX en dispositivos Samsung con sistema operativo Android.

El uso de contenedores KNOX solo está disponible en dispositivos Samsung que ejecutan la versión 6.0 de Android o posterior.

Acerca de contenedores KNOX

Un *contenedor KNOX* es un entorno seguro en el dispositivo de un usuario que tiene su propio escritorio, panel de inicio rápido, aplicaciones y widgets. Un contenedor KNOX le permite aislar aplicaciones y datos corporativos de aplicaciones y datos personales. Un contenedor KNOX es un componente de la solución móvil Samsung KNOX.

Samsung KNOX es una solución móvil para configurar y proteger dispositivos móviles Samsung que utilizan el sistema operativo Android. Para obtener más información sobre Samsung KNOX, visite el *sitio web del soporte técnico de Samsung*.

Los contenedores KNOX le permiten separar datos personales y corporativos en un dispositivo móvil. Por ejemplo, es imposible usar un buzón de correo personal para enviar un archivo que se encuentra en un contenedor KNOX. Se recomienda implementar un contenedor KNOX si los dispositivos móviles personales de empleados se utilizan para que funcionen con datos corporativos.

Para usar contenedores KNOX, debe activar Samsung KNOX. Después de sincronizar un dispositivo con Kaspersky Security Center, al usuario del dispositivo móvil se le solicitará instalar el contenedor KNOX. Antes de instalar el contenedor KNOX, el usuario debe aceptar los términos del Contrato de licencia para usuario final de Samsung.

Después de instalar el contenedor KNOX, el icono de KNOX  se añadirá al escritorio del dispositivo móvil. O el espacio de trabajo se agregará a la lista de aplicaciones en el dispositivo móvil. Para trabajar con datos corporativos, el usuario tiene que iniciar la aplicación desde el contenedor KNOX.

La aplicación Kaspersky Endpoint Security para Android no está instalada en el contenedor KNOX y no protege los datos corporativos. La aplicación Kaspersky Endpoint Security para Android no detecta la descarga de archivos maliciosos y bloquea los sitios maliciosos en el contenedor KNOX. No puede controlar el inicio de la aplicación ni prohibir el uso de la cámara en el contenedor KNOX. La aplicación Kaspersky Endpoint Security para Android solo protege los datos privados. Puede proteger los datos corporativos con las herramientas de Samsung KNOX. Para obtener más información sobre Samsung KNOX, visite el *sitio web del soporte técnico de Samsung*.

Activación de Samsung KNOX

Para usar un contenedor KNOX en el dispositivo móvil del usuario, debe activar Samsung KNOX. El procedimiento para activar Samsung KNOX depende de la versión de Kaspersky Endpoint Security para Android instalada en los dispositivos de sus usuarios:

- Si la versión actual de Kaspersky Endpoint Security para Android está instalada en los dispositivos, no necesita ninguna clave para activar Samsung KNOX.
- Si hay una versión anterior de Kaspersky Endpoint Security para Android (10.8.3.174 o anterior) instalada en los dispositivos, debe obtener una clave del administrador de licencias KNOX (en lo sucesivo, clave KLM) de Samsung. Una *clave del administrador de licencias KNOX* es un código único utilizado por el sistema de licencias de Samsung KNOX. Si desea obtener más información acerca de las claves KLM, visite el sitio web del soporte técnico de Samsung KNOX.

El uso de contenedores KNOX solo es posible en dispositivos Samsung.

Para activar Samsung KNOX:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Administrar Samsung KNOX → Contenedores KNOX**.
5. En el campo **Clave del administrador de licencias KNOX**, especifique lo siguiente:
   - Si hay una versión actual de Kaspersky Endpoint Security para Android instalada en los dispositivos, escriba cualquier carácter.
   - Si hay una versión anterior de Kaspersky Endpoint Security para Android (10.8.3.174 o anterior) instalada en los dispositivos, ingrese la clave KLM de Samsung.
6. Establezca el atributo "lock" en la posición de bloqueo .
7. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Samsung KNOX se activará después de la siguiente sincronización del dispositivo con Kaspersky Security Center. Al usuario se le solicitará que acepte los términos del Contrato de licencia de usuario final de Samsung e instalar el contenedor KNOX.

Para desactivar Samsung KNOX:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Administrar Samsung KNOX → Contenedores KNOX**.
5. Elimine el valor del campo **Clave del administrador de licencias KNOX**.
6. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Samsung KNOX se desactivará después de la siguiente sincronización del dispositivo con Kaspersky Security Center. El acceso al contenedor KNOX se bloqueará.

Limitaciones de Samsung KNOX

- El uso de contenedores KNOX solo está disponible en dispositivos Samsung.
- En los dispositivos Samsung compatibles con KNOX 2.6, 2.7 y 2.7.1, Protección web y Control de apps no funcionan en un contenedor KNOX. Este problema se debe a la carencia de permisos relevantes en el contenedor KNOX (Servicio de accesibilidad). En dispositivos compatibles con KNOX 2.8 y superiores, todos los componentes de la aplicación se ejecutan sin limitaciones.
- Las versiones de Kaspersky Endpoint Security para Android anteriores a Service Pack 4 Maintenance Release 3 Update 2 pueden ser inestables en dispositivos Samsung con Android 10 debido a las actualizaciones de Samsung KNOX. Se recomienda actualizar Kaspersky Endpoint Security para Android a la versión Service Pack 4 Maintenance Release 3 Update 2.

Configuración de firewall en KNOX

Debería configurar las opciones del firewall para supervisar conexiones de red en un contenedor KNOX.

Para configurar el firewall en un contenedor KNOX:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Administrar Samsung KNOX → Contenedores KNOX**.
5. En la ventana **Firewall**, haga clic en **Configurar**.

   Se abre la ventana **Firewall**.
6. Seleccione el modo de firewall:
   - Para permitir todas las conexiones entrantes y salientes, mueva el cursor hacia **Permitir todas**.
   - Para que la aplicación bloquee toda la actividad de red excepto la actividad de las aplicaciones que se encuentran en la lista de exclusiones, mueva el cursor hacia **Bloquear todas, salvo las excepciones**.
7. Si ha configurado el modo del firewall en **Bloquear todas, salvo las excepciones**, cree una lista de exclusiones:
   a. Haga clic en **Agregar**.

      Esto abre la ventana **Exclusión del firewall**.

   b. En el campo **Nombre de la aplicación**, 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 **Aceptar**.

8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Configuración de un buzón de correo de Exchange en KNOX

Para trabajar con el calendario, el correo y los contactos corporativos en un contenedor KNOX, debería ajustar la configuración del buzón de correo de Exchange.

Para configurar un buzón de correo de Exchange en un contenedor KNOX:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al cual los dispositivos de Android pertenecen.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Para abrir la ventana de propiedades de la directiva, haga doble clic en cualquier columna.
4. En la ventana **Propiedades de la directiva**, seleccione la sección **Administrar Samsung KNOX → Contenedores KNOX**.
5. En la ventana **Exchange ActiveSync**, haga clic en el botón **Configurar**.

   Se abre la ventana **Configuración del servidor de correo Exchange**.
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 **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 **Usar conexión SSL**.
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**.
11. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Después de la siguiente sincronización del dispositivo con Kaspersky Security Center, se establece la configuración del dispositivo móvil.

Apéndices

Esta sección proporciona información que complementa el texto del documento.

Permisos para configurar directivas de grupo

Los administradores de Kaspersky Security Center pueden configurar los derechos de acceso de los usuarios de la Consola de administración relativos a diversas funciones de aplicaciones, en función de las tareas de los usuarios.

Para cada área funcional, el administrador puede asignar los siguientes permisos:

- **Permitir modificación**. El usuario de la Consola de administración puede cambiar la configuración de las directivas en la ventana de propiedades.
- **Bloquear modificación**. El usuario de la Consola de administración 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.

Permisos para acceder a las secciones del complemento de administración de Kaspersky Endpoint Security

Alcance funcional	Sección directivas
Android Enterprise	Perfil de trabajo de Android
Antirrobo	Antirrobo
Control de apps	Control de apps
Protección	Protección, análisis, actualización
Control de cumplimiento	Control de cumplimiento
Contenedores	Contenedores
Configuración de dispositivos	Control de dispositivos, sincronización
Administración de dispositivos Samsung	APN, Administración de dispositivos de Samsung, contenedores KNOX
Administración de sistemas	Opciones avanzadas, Wi-Fi
Protección web	Protección web

Permisos para acceder a las secciones del complemento de administración de Kaspersky Device Management para iOS

Alcance funcional	Sección directivas
Adicional	Clips web, fuentes, AirPlay, AirPrint
Exchange ActiveSync	General, contraseña, sincronización, restricciones de funciones, restricciones de aplicaciones
General	General, inicio de sesión único, Protección web, Wi-Fi, nombre de punto de acceso (APN), Exchange ActiveSync, correo electrónico, opciones de carga personalizadas
LDAP (calendario/contactos)	LDAP, calendario, contactos, Calendario suscrito
Limitaciones y seguridad	Restricción de la función, restricciones para las aplicaciones, restricciones para el contenido multimedia, contraseña, VPN, proxy HTTP global, certificados, SCEP

Categorías de aplicación

Control de apps admite la categorización de aplicaciones. El modo de funcionamiento configurado para la categoría de la aplicación se aplica a todas las aplicaciones en esta categoría. La categoría de cada aplicación la determina el servicio en la nube de Kaspersky Security Network.

Categorías de aplicación

Categorías	Descripción
Entretenimiento	Aplicaciones para entretenimiento interactivo.
Clientes de MI, aplicaciones de mensajería móviles	Aplicaciones para mensajería instantánea, comunicación de voz y vídeo mediante IP.
Redes sociales	Aplicaciones para usar redes sociales y blogs.
Software de empresa	Aplicaciones para cálculos de impuestos, administración de operaciones bancarias, gestión de hojas de cálculo, contabilidad y otras aplicaciones orientadas a la empresa. Editores de texto.
Hogar, familiares, aficiones, salud	Aplicaciones con recetas, sugerencias de diseño. Aplicaciones para entrenar, mantener una planificación de ejercicios, recibir sugerencias sobre dietas, nutrición saludable, seguridad y prevención de accidentes.
Medicina	Aplicaciones que contienen catálogos de síntomas y medicaciones, aplicaciones para profesionales de la salud, revistas y noticias de asistencia médica.
Multimedia	Servicios para suscripción de películas, reproductores multimedia y reproductores de vídeo. Servicios musicales, reproductores, emisiones de radio.
Software de diseño gráfico	Aplicaciones para utilizar con una cámara, editores de gráficos, aplicaciones para administrar y publicar fotos.
Complementos para leer noticias y canales RSS	Aplicaciones para leer periódicos, revistas, blogs, agregadores de noticias.
Tiempo atmosférico	Aplicaciones que muestran el pronóstico del tiempo.
Aplicaciones de educación	Lectores de libros, manuales, libros de texto, diccionarios, tesauros, enciclopedias. Aplicaciones que facilitan el estudio para exámenes, materiales didácticos, diccionarios, juegos de desarrollo, herramientas de estudio de idiomas.
Compra en línea	Aplicaciones para comprar en línea y ofertar en subastas, cupones de regalo, herramientas de comparación de precios, aplicaciones para listas de compras, aplicaciones para leer comentarios sobre productos.
Herramientas de inicio	Aplicaciones destinadas a rediseñar el escritorio, widgets, funciones rápidas.
Sistemas operativos y utilidades	Aplicaciones del sistema que proporcionan la administración del sistema operativo, interacción del usuario y administración de la memoria RAM.
Visores de mapas	Guías de ciudades, información sobre empresas locales, herramientas de planificación de viajes.
Otras aplicaciones	Bibliotecas de software, versiones de demostración técnica de aplicaciones. Aplicaciones no incluidas en ninguna categoría.
Transporte	Aplicaciones para utilizar transportes públicos, herramientas de navegación, aplicaciones para conductores.
Juegos	Videoconsola, Sorteos, Carreras, Otro, Casino, Juegos de cartas, Música, Juegos de

	mesa, Tutoriales, Rompecabezas, Aventuras, Juegos de rol, Simuladores, Crucigramas, Juegos de deportes, Estrategias, Acción.
Navegadores	Aplicaciones para visualizar sitios web, contenidos de documentos y archivos web. Aplicaciones para administrar aplicaciones web.
Herramientas de desarrollo	Aplicaciones diseñadas para desarrollar software. Depuradores, compiladores, editores de códigos, editores de interfaces gráficas de usuario.
Aplicaciones de SO	Aplicaciones entregadas junto con el sistema operativo y necesarias para el funcionamiento adecuado del sistema operativo.
Aplicaciones de Internet	Administradores de descargas, clientes de correo, aplicaciones de búsqueda web y otras aplicaciones para facilitar la navegación por Internet.
Software de la infraestructura de red	Aplicaciones para administrar servidores, dispositivos de almacenamiento de datos, equipo de red, software dentro de una red corporativa, automatización e integración de la infraestructura completa.
Software de red	Aplicaciones para organizar la colaboración de un grupo de usuarios en varios dispositivos, comunicación entre dispositivos.
Herramientas de sistema	Aplicaciones proporcionadas simultáneamente con el sistema operativo: administradores de archivos, herramientas de archivo, herramientas para el diagnóstico del hardware y el software, herramientas de optimización de memoria, desinstaladores, herramientas de administración del procesador.
Software de seguridad	Aplicaciones de protección de datos del dispositivo. Las aplicaciones que detectan y neutralizan amenazas en el dispositivo. Firewalls. Aplicaciones de cifrado de datos.
Gestores de descarga	Aplicaciones para descargar archivos desde fuentes externas.
Aplicaciones para almacenar archivos en Internet	Aplicaciones para administrar el almacenamiento online de archivos, notas y multimedia.
Sistemas de referencia	Lectores de libros, manuales, libros de texto, diccionarios, tesauros, enciclopedias de Wikipedia.
Aplicaciones de correo electrónico	Aplicaciones usadas para enviar y recibir mensajes de correo electrónico.

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 Antivirus para proteger el dispositivo contra virus y otro software malicioso.

El componente Antivirus 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 del antivirus.

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.

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, bloqueadas y requeridas. El componente Control de apps se utiliza para instalar aplicaciones recomendadas y requeridas, para actualizarlas y para eliminar aplicaciones bloqueadas.

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 apps permite eliminar aplicaciones bloqueadas que infrinjan los requisitos de seguridad corporativa.

Kaspersky Endpoint Security debe estar habilitado como un servicio de funciones de accesibilidad para garantizar el correcto funcionamiento del Control de apps. Si no habilitó este servicio durante el Asistente de configuración inicial para la aplicación, puede habilitar Kaspersky Endpoint Security como un servicio de funciones de accesibilidad en la sección **Estado** para seleccionar la notificación apropiada, o en la configuración del dispositivo (**Configuración de Android** → **Accesibilidad** → **Servicios**).

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 pirata informático tenga la capacidad de desbloquear el dispositivo, Kaspersky Endpoint Security debe estar habilitado como un servicio de funciones de accesibilidad en dispositivos móviles que ejecuten Android 7.0 o versiones posteriores.

- Activar una alarma sonora en el dispositivo, incluso si el sonido del dispositivo está deshabilitado.
- Obtener las coordenadas del mapa de la ubicación del dispositivo.
- Borrar los datos almacenados en el dispositivo.
- Restablecer la configuración de fábrica.
- Tomar, de forma secreta, una foto de la persona utilizando el dispositivo.

Para habilitar operaciones antirrobo, Kaspersky Endpoint Security debe estar habilitado como administrador del dispositivo. Si no concediera derechos del administrador del dispositivo durante la configuración inicial de apps, puede conceder derechos de administrador a Kaspersky Endpoint Security en la sección **Estado** al seleccionar 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.

Para activar la Protección web:

- Kaspersky Endpoint Security debe estar activado como un servicio de funciones de accesibilidad.
- Debe aceptar la Declaración sobre el procesamiento de datos para usar Protección web (Declaración de Protección web). Kaspersky Endpoint Security utiliza Kaspersky Security Network (KSN) para analizar los 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 es necesario que realice 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.

La Protección web en los dispositivos Android solo funciona en el navegador Google Chrome (incluida la función de Pestañas personalizadas), el navegador Huawei y el navegador de Internet de Samsung. La Protección web para el Navegador de Samsung no bloquea sitios en un dispositivo móvil si se utiliza un perfil de trabajo y la Protección web está habilitada solo para el perfil de trabajo.

Ventana principal de un vistazo

La apariencia de la ventana principal apenas difiere según las diferentes resoluciones de pantalla.

La apariencia de la pantalla principal cambia en caso de problemas que podrían llevar a una reducción del nivel de protección, infección del dispositivo o pérdida de información.

La sección **Estado** muestra la siguiente información:

- Problemas en la protección de su dispositivo.
- Información sobre si su dispositivo cumple con los requisitos de seguridad corporativa.
- Información sobre el estado de protección de su dispositivo.

Puede abrir la sección **Estado** si toca la parte superior de la ventana principal de Kaspersky Endpoint Security.

Problemas en protección del dispositivo

Los problemas de protección se agrupan por categorías. Para cada problema, se enumeran acciones que pueden utilizarse para solucionarlo.

La sección **Estado** también muestra una lista de objetos omitidos detectados por la aplicación. La lista de amenazas omitidas puede cambiar, por ejemplo, si un archivo sospechoso se eliminara o se moviera. Para recibir una lista actualizada de amenazas, ejecute un análisis completo del dispositivo. Para garantizar la protección confiable de sus datos, elimine todas las amenazas detectadas.

Existen dos tipos de problemas de protección:

- *Problemas de notificación*. Resaltados en amarillo. Los problemas de notificación informan al usuario acerca de eventos que pueden afectar la seguridad del dispositivo (por ejemplo, el hecho de que el último análisis se haya realizado hace más de 14 días o el hecho de que una aplicación instalada recientemente no se haya analizado). Puede ocultar un problema de notificación. Podrá volver a acceder a la información acerca del problema desde el menú **Problemas ocultos**.
- *Críticos*. Resaltados en rojo. Los problemas críticos notifican al usuario sobre eventos de importancia crítica para la seguridad del dispositivo (como el hecho de que las bases de datos antivirus no se hayan actualizado

durante mucho tiempo o que se haya instalado una aplicación bloqueada en el dispositivo). No es posible ocultar un problema crítico.

Control de cumplimiento

La aplicación revisa de forma automática si el dispositivo cumple los requerimientos de seguridad corporativa. La información sobre si el dispositivo cumple o no los requisitos necesarios de seguridad corporativa se muestra en la sección **Estado**.

- Motivo por el cual el dispositivo no cumple con los requisitos de seguridad corporativa (por ejemplo, se han detectado aplicaciones bloqueadas en el dispositivo).
- 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.

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 antivirus están desactualizadas o una aplicación recién instalada no se ha analizado).

Análisis del dispositivo

El antivirus tiene varias limitaciones:

- Cuando el antivirus se está ejecutando, una amenaza detectada en la memoria externa del dispositivo (por ejemplo, una tarjeta SD) no se puede neutralizar automáticamente en el Perfil de trabajo (Aplicaciones con el icono de un maletín, Configuración del perfil de trabajo de Android). Kaspersky Endpoint Security para Android no tiene el acceso a la memoria externa en el Perfil de trabajo. La información sobre los objetos detectados se muestra en la sección **Estado** 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 aplicación omite esos archivos sin notificarle que se omitieron.

Para iniciar un análisis del dispositivo:

1. Presione **Análisis** en el panel de inicio rápido de la ventana principal de Kaspersky Endpoint Security.
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 del dispositivo completo accesible para la 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.

El administrador puede restringir el acceso a la configuración del análisis de virus.

Para configurar el análisis de virus:

1. En el panel de inicio rápido en la ventana principal de Kaspersky Endpoint Security, presione → **Configuración** → **Antivirus** → **Análisis**.
2. Si desea que la aplicación detecte adware y aplicaciones que podrían ser utilizadas por hackers para causar daños a su dispositivo o datos cuando la aplicación realiza un análisis, active el interruptor **Adware, marcadores y otros**.
3. Haga clic en **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.
   - **Solicitar acción**

     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. La información sobre amenazas omitidas se muestra en la sección **Estado** de la aplicación. Para cada amenaza omitida, la aplicación le proporciona acciones que puede realizar para eliminar la amenaza. La lista de amenazas omitidas puede cambiar, por ejemplo, si un archivo sospechoso se eliminara o se moviera. Para recibir una lista actualizada de amenazas, ejecute un análisis completo del dispositivo. Para garantizar la protección confiable de sus datos, elimine todas las amenazas detectadas.

Se registra la información sobre amenazas detectadas y las acciones tomadas sobre ellas en los informes de la aplicación (→ **Informes**). Puede elegir mostrar informes sobre las operaciones del antivirus.

Ejecución de un análisis programado

El antivirus tiene varias limitaciones:

- Cuando el antivirus se está ejecutando, una amenaza detectada en la memoria externa del dispositivo (por ejemplo, una tarjeta SD) no se puede neutralizar automáticamente en el Perfil de trabajo (Aplicaciones con el icono de un maletín, Configuración del perfil de trabajo de Android). Kaspersky Endpoint Security para Android no tiene el acceso a la memoria externa en el Perfil de trabajo. La información sobre los objetos detectados se muestra en la sección **Estado** 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 aplicación omite esos archivos sin notificarle que se omitieron.

Para configurar la programación del análisis completo para un dispositivo:

1. En el panel de inicio rápido en la ventana principal de Kaspersky Endpoint Security, presione → **Configuración** → **Antivirus** → **Análisis**.

2. Presione **Programación** y seleccione la frecuencia de análisis completo:

   - **Semanal**
   - **A diario**
   - **Deshabilitado**
   - **Después de la actualización de la base de datos**

3. Haga clic en **Día de inicio** y seleccione el día de la semana en que desea que comience el análisis completo.

4. Haga clic en **Hora de inicio** y seleccione la hora para comenzar el análisis completo.

Un análisis completo del dispositivo se iniciará de acuerdo a la programación.

> En Android 12 o una versión posterior, la aplicación puede realizar esta tarea más tarde de lo especificado si el dispositivo está en modo de ahorro de batería.

Cambio del modo de Protección

La Protección en tiempo real le permite detectar amenazas en los archivos que se abren y analizar aplicaciones mientras se instalan en el dispositivo en tiempo real. Las bases de datos antivirus 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 el panel de inicio rápido en la ventana principal de Kaspersky Endpoint Security, presione → **Configuración** → **Antivirus** → **Modo de protección en tiempo real**.

2. Seleccione el modo de Protección del dispositivo:

   - **Deshabilitado**. La protección está deshabilitada.
   - **Recomendado**. El antivirus analiza solo las aplicaciones instaladas y los archivos de la carpeta Descargas. El antivirus analiza las nuevas aplicaciones ni bien se las instala.
   - **Extendido**. El antivirus analiza todos los archivos en busca de objetos maliciosos cuando se realiza alguna acción en ellos (por ejemplo, cuando se los guarda, mueve o modifica). El antivirus analiza las nuevas aplicaciones ni bien se las instala.

La información sobre el modo de protección actual se muestra en la descripción del componente.

El administrador puede restringir el acceso a la configuración de Protección en tiempo real.

Para habilitar Protección en la nube (KSN):

1. Presione → **Configuración** → **Antivirus** en el panel de inicio rápido en la ventana principal de Kaspersky Endpoint Security.
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 de Kaspersky para consultar por la reputación de los archivos y aplicaciones. El análisis se realiza para amenazas cuya información aún no se ha añadido a las bases de datos antivirus, pero que ya está disponible en KSN. El servicio en la nube de Kaspersky Security Network permite el funcionamiento completo del antivirus y reduce la posibilidad de falsas alarmas. Solo el administrador puede deshabilitar por completo el uso de Kaspersky Security Network.

Para configurar Protección en tiempo real:

1. En el panel de inicio rápido en la ventana principal de Kaspersky Endpoint Security, presione → **Configuración** → **Antivirus** → **Modo de protección en tiempo real**.
2. Si desea que la aplicación detecte adware y aplicaciones que podrían ser utilizadas por hackers para causar daños a su dispositivo o datos cuando la aplicación realiza un análisis, active el interruptor **Adware, marcadores y otros**.
3. Haga clic en **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.

   - **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. La información sobre amenazas omitidas se muestra en la sección **Estado** de la aplicación. Para cada amenaza omitida, la aplicación le proporciona acciones que puede realizar para eliminar la amenaza. La lista de amenazas omitidas puede cambiar, por ejemplo, si un archivo sospechoso se eliminara o se moviera. Para recibir una lista actualizada de amenazas, ejecute un análisis completo del dispositivo. Para garantizar la protección confiable de sus datos, elimine todas las amenazas detectadas.

Se registra la información sobre amenazas detectadas y las acciones tomadas sobre ellas en los informes de la aplicación (→ **Configuración** → **Informes**). Puede elegir mostrar informes sobre las operaciones del antivirus.

Actualizaciones de la base de datos del antivirus

Para actualizar las bases de datos del antivirus de la aplicación:

Presione **Actualización de bases de datos** en el panel de inicio rápido en la ventana principal de Kaspersky Endpoint Security.

Actualización de la base de datos programada

La aplicación puede actualizar las bases de datos del antivirus de forma automática de acuerdo al programa que se ha especificado.

Para configurar una actualización programada:

1. En el panel de inicio rápido en la ventana principal de Kaspersky Endpoint Security, presione → **Configuración** → **Antivirus** → **Actualización de bases de datos**.
2. Haga clic en **Programación** y seleccione la frecuencia de actualización:
   - **Semanal**
   - **A diario**
   - **Deshabilitado**
3. Haga clic en **Día de inicio** y seleccione el día de la semana en que desea realizar la actualización.
4. Haga clic en **Hora de inicio** y seleccione la hora para comenzar la actualización.

La actualización de las bases de datos del antivirus se iniciará de acuerdo a la programación.

En Android 12 o una versión posterior, la aplicación puede realizar esta tarea más tarde de lo especificado si el dispositivo está en modo de ahorro de batería.

Qué hacer en caso de pérdida o robo del dispositivo

Ante el robo o pérdida de un dispositivo, contacte al administrador de su sistema. El administrador puede ejecutar comandos antirrobo en el dispositivo de manera remota de acuerdo a los requisitos de seguridad corporativa.

Si se envía un comando de restablecimiento completo al dispositivo, se perderá el control sobre el mismo y los demás comandos Antirrobo no podrán funcionar.

Protección web

Para activar la Protección web:

- Kaspersky Endpoint Security debe estar activado como un servicio de funciones de accesibilidad.
- Debe aceptar la Declaración sobre el procesamiento de datos para usar Protección web (Declaración de Protección web). Kaspersky Endpoint Security utiliza Kaspersky Security Network (KSN) para analizar los 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 es necesario que realice 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.

La Protección web en los dispositivos Android solo funciona en el navegador Google Chrome (incluida la función de Pestañas personalizadas), el navegador Huawei y el navegador de Internet de Samsung. La Protección web para el Navegador de Samsung no bloquea sitios en un dispositivo móvil si se utiliza un perfil de trabajo y la Protección web está habilitada solo para el perfil de trabajo.

Para utilizar la Protección web en todo momento mientras navega en la web, establezca Google Chrome o Samsung Internet 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. Presione → **Configuración** → **Protección web** en el panel de inicio rápido en la ventana principal de Kaspersky Endpoint Security.
2. Active el interruptor de **Protección web**.
3. Presione **Establecer navegador predeterminado**.

   Este botón se muestra cuando la Protección web está habilitada y no se estableció un navegador compatible como navegador predeterminado.

   Se inicia el asistente de selección de navegador predeterminado.
4. Siga las instrucciones del asistente.

El asistente establece Google Chrome o los navegadores de Samsung o Huawei como navegador predeterminado. La Protección web analiza en todo momento los sitios web que visita.

Control de la aplicación

Control de apps comprueba que las aplicaciones instaladas en un dispositivo móvil cumplan con los requisitos de seguridad corporativa. En Kaspersky Security Center, el administrador crea listas de apps permitidas, bloqueadas, obligatorias y recomendadas según los requisitos de seguridad corporativa. Debido a Control de apps, Kaspersky Endpoint Security le pide que instale las aplicaciones obligatorias y recomendadas, y que elimine las aplicaciones bloqueadas. Es imposible iniciar aplicaciones bloqueadas en su dispositivo móvil.

Para instalar aplicaciones obligatorias y recomendadas, o para eliminar aplicaciones bloqueadas:

1. Vaya a la sección **Estado** de Kaspersky Endpoint Security.
2. Seleccione las tareas de Control de apps.
3. Realice las acciones recomendadas.

Obtener certificado

Para obtener un certificado para acceder a los recursos de la red corporativa:

1. Presione → **Configuración** → **Adicional** → **Obtener certificado** en el panel de inicio rápido en la ventana principal de Kaspersky Endpoint Security.
2. Especifique sus credenciales de la cuenta de la red corporativa.
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.

Sincronizando 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. Debe establecer la configuración de sincronización si instaló Kaspersky Endpoint Security mediante Google Play. 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. Presione → **Configuración** → **Sincronización** en el panel de inicio rápido en la ventana principal de Kaspersky Endpoint Security.
2. En la sección **Configuración de sincronización** especifique los valores de la siguiente configuración:
   - **Servidor**
   - **Puerto**
   - **Grupo**
   - **Correo electrónico corporativo**

   El administrador puede ocular la configuración de sincronización.
3. Presione **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 de error que dice que su licencia caducará pronto o que ya caducó, y que su dispositivo no está conectado al Servidor de administración, presione **Activar**.
2. En la ventana de activación, ingrese el código de activación que le dio el administrador y presione **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.

Actualización de la aplicación

Kaspersky Endpoint Security se puede actualizar de las siguientes maneras:

- De forma manual mediante Google Play. Puede descargar la versión nueva de la aplicación desde Google Play 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 Google Play

El administrador puede bloquear la actualización de la aplicación desde Google Play.

La aplicación puede actualizarse desde Google Play siguiendo el procedimiento de actualización estándar de la plataforma Android. Para actualizar la aplicación deben cumplirse las siguientes condiciones:

- Se debe tener una cuenta de Google.
- El dispositivo debe estar asociado a su cuenta de Google.
- El dispositivo debe estar conectado a Internet.

Para obtener más información sobre cómo crear una cuenta de Google, vincular el dispositivo a la cuenta o usar Google Play Store, consulte el sitio web de ayuda de Google.

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.

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 de la aplicación.
- 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 de la aplicación

Para eliminar Kaspersky Endpoint Security del dispositivo:

1. En el panel de inicio rápido en la ventana principal de Kaspersky Endpoint Security, presione → **Desinstalar la aplicación**.

   Esto inicia el Asistente de eliminación remota.

2. Siga las instrucciones del asistente.

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 7.0 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

Icono de la aplicación en el perfil de trabajo de Android

Las aplicaciones marcadas con el icono de un maletín (apps corporativas) se almacenan en el perfil de trabajo de Android del dispositivo (de aquí en adelante, también "perfil de trabajo"). El *perfil de trabajo de Android* 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.

El perfil de trabajo le 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 perfil de trabajo en el dispositivo, se instalan las siguientes aplicaciones corporativas automáticamente en el perfil de trabajo: Google Play Market, Google Chrome, Descargas, Kaspersky Endpoint Security para Android, y otras.

Aplicación KNOX

La aplicación KNOX abre un contenedor KNOX en su dispositivo. Un *contenedor KNOX* es un entorno seguro en su dispositivo que tiene su propio escritorio, panel de inicio, aplicaciones y widgets. El administrador puede administrar apps 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*.

Uso de la aplicación Kaspersky Security para iOS

Esta sección de Ayuda describe las funciones y operaciones que están disponibles para los usuarios de la app Kaspersky Security 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 Security 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. Protección web también comprueba la actividad en línea de las aplicaciones de su dispositivo.

Para que la Protección web funcione, debe permitir que la aplicación agregue una configuración de VPN.

Detección de liberación

Cuando Kaspersky Security para iOS detecta una liberación, muestra un mensaje crítico e informa al administrador sobre el problema.

La aplicación no puede garantizar la seguridad de su dispositivo, ya que una liberación omite las características de seguridad y puede causar varios problemas, como 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

Para instalar la aplicación Kaspersky Security para iOS:

1. Busque el mensaje de correo electrónico con la invitación del administrador para instalar la aplicación Kaspersky Security para iOS desde la App Store.
2. Vaya a la App Store de una de las siguientes maneras:
   - Toque el vínculo del 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. Descargue e instale la aplicación desde la App Store siguiendo el procedimiento de instalación estándar en la plataforma iOS.

La aplicación Kaspersky Security para iOS se instala en su dispositivo. Para proteger el dispositivo, active la aplicación.

Activación de la aplicación

Para activar la aplicación Kaspersky Security para iOS, siga los siguientes 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 VPN para comprobar los sitios web en busca de phishing y proteger su dispositivo contra el malware.
5. Permita que la aplicación envíe notificaciones automáticas. La aplicación utiliza notificaciones para informarle los problemas de seguridad y el estado de su licencia.

La aplicación Kaspersky Security para iOS en su dispositivo está activada.

Activar la aplicación con un código de activación

Cuando instala la aplicación Kaspersky Security 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 presione **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.

La aplicación Kaspersky Security para iOS en su dispositivo está activada.

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 Security 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.

Eliminación de la aplicación

Para eliminar la aplicación Kaspersky Security 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 Security para iOS se elimina de su dispositivo.

Licencia de aplicaciones

Esta sección proporciona información sobre los términos generales relacionados con la licencia de Kaspersky Security para dispositivos móviles.

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 Kaspersky Security para dispositivos móviles.

Le recomendamos que lea detenidamente los Términos y condiciones del EULA antes de utilizar Kaspersky Security para dispositivos móviles.

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

- Durante la instalación de componentes de Kaspersky Security para dispositivos móviles.
- 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 Security 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.

Al confirmar que acepta el Contrato de licencia de usuario final (EULA) al instalar los componentes de Kaspersky Security para dispositivos móviles, indica que usted acepta los Términos y condiciones del Contrato de licencia de usuario final. Si no acepta los términos del Contrato de licencia de usuario final, debe cancelar la instalación de los componentes de Kaspersky Security para dispositivos móviles y abstenerse de utilizarlos.

Información sobre la licencia

Una licencia es un derecho de duración limitada a fin de utilizar la solución integrada Kaspersky Security para dispositivos móviles que se le proporciona conforme a las condiciones del Contrato de licencia de usuario final.

Una licencia actual le da derecho a los siguientes tipos de servicios:

- Utilizar aplicaciones en dispositivos móviles conforme a las condiciones del Contrato de licencia de usuario final.
- Recibir asistencia técnica.

El ámbito de los servicios disponibles y la duración de uso de la aplicación dependen del tipo de licencia con que se ha activado la aplicación.

Se proporcionan los tipos de licencia siguientes:

- *Prueba*.

Licencia gratuita con el fin de probar Kaspersky Security para dispositivos móviles.

La licencia de evaluación es válida durante 30 días. Cuando la licencia de prueba caduque, las aplicaciones móviles Kaspersky Endpoint Security para Android o Kaspersky Security para iOS dejarán de realizar la mayoría de sus funciones excepto la sincronización con el Servidor de administración. Para continuar usando la aplicación, debe adquirir la versión comercial.

- *Comercial*.

  Licencia que se proporciona al adquirir Kaspersky Security para dispositivos móviles.

  Cuando la licencia comercial expira, la aplicación móvil continúa 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:

    - **Antivirus**. Se encuentran disponibles Protección en tiempo real y Análisis antivirus del dispositivo, pero las actualizaciones de la base de datos antivirus 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, SafetyNet Attestation, 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 de grupo).

  - Aplicación Kaspersky Security para iOS:

    - **Sincronización con el Servidor de administración**.

    Kaspersky Security para iOS deja de intercambiar información con Kaspersky Security Network si la licencia de prueba caduca o si falta una licencia (el código de activación se elimina de la directiva de grupo).

  Los demás componentes de la aplicación móvil no están disponibles para el usuario del dispositivo. El administrador puede usar políticas del grupo para administrar estos componentes en el modo de funcionalidad limitada. No puede usar políticas del grupo para configurar los otros componentes de la aplicación.

  Para seguir utilizando todas las funciones de la aplicación, es preciso renovar la licencia comercial. A fin de asegurar la protección máxima de su equipo contra todas las amenazas de seguridad, le recomendamos renovar el plazo de la licencia o comprar una nueva antes de que caduque la actual.

Acerca de la suscripción

Suscripción para Kaspersky Security para dispositivos móviles es una petición para utilizar la aplicación móvil con los parámetros seleccionados (fecha de caducidad de la suscripción, cantidad de dispositivos móviles protegidos). Puede pedir la suscripción para Kaspersky Security para dispositivos móviles a su proveedor de servicios (por ejemplo, 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 Kaspersky Security para dispositivos móviles siga funcionando tras haber caducado el plazo de suscripción limitada, es necesario 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 utilizar Kaspersky Security para dispositivos móviles con suscripción, es preciso aplicar el código de activación facilitado por el 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 Kaspersky Security para dispositivos móviles.

Acerca de la clave

Una *clave* es una secuencia de bits que puede aplicar para activar y después utilizar la solución integrada de Kaspersky Security para dispositivos móviles conforme a las condiciones del Contrato de licencia de usuario final. Los especialistas de Kaspersky generan las claves.

Puede agregar una clave para la aplicación móvil mediante un fichero llave 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 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 añadir claves, las puede sustituir por otras.

  No puede activar la aplicación Kaspersky Security para iOS con un fichero llave.

- 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 se muestra en la interfaz de la aplicación móvil como una secuencia alfanumérica única.

Kaspersky puede bloquear la clave, por ejemplo, en caso de incumplimiento de las condiciones del Contrato de licencia. Si la clave está bloqueada, la aplicación móvil deja de realizar todas sus funciones excepto la sincronización con el Servidor de administración. Para continuar usando la aplicación, deberá añadir una clave 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 Security para iOS. El código de activación se envía a la dirección de correo electrónico que se ha especificado tras adquirir la solución integrada de Kaspersky Security para dispositivos móviles o bien después de pedir la versión de evaluación de Kaspersky Security para dispositivos móviles.

Para activar la aplicación móvil con un código de activación, se necesita acceder a Internet para conectarse a 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 fichero llave

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 Security para iOS con un fichero llave.

El archivo de clave se envía a la dirección de correo electrónico que especificó tras adquirir la solución integrada de Kaspersky Security para dispositivos móviles o bien después de pedir la versión de prueba de Kaspersky Security para dispositivos móviles.

Para activar la aplicación con un fichero llave no hace falta conectarse a los servidores de activación de Kaspersky.

Puede recuperar un fichero llave en caso de pérdida accidental. Es posible que necesite un fichero llave para registrar una Kaspersky CompanyAccount, por ejemplo.

Para recuperar un fichero llave, efectúe una de las acciones siguientes:

- 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

La versión móvil de Kaspersky Security cumple con las Normativas Generales de Protección de Datos (GDPR).

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 procesamiento 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 Security for Mobile (Devices) 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:

- **Antivirus.** La aplicación obtiene acceso a la base de conocimientos de Kaspersky para consultar por la reputación de los archivos y aplicaciones. El análisis se realiza para amenazas cuya información aún no se ha añadido a las bases de datos antivirus, pero que ya está disponible en KSN. El servicio en la nube de Kaspersky Security Network permite el funcionamiento completo del antivirus y reduce la posibilidad de falsas alarmas.

- **Protección 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 aplicaciones 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 Antivirus y Control de apps 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 Acuerdo de licencia de usuario final

Con el fin de verificar el uso legítimo del Software, en los casos en que el Código de Activación se use para activar tal Software, 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 IPv4 del servicio web a la que se accedió; tamaño del contenido de la solicitud a la infraestructura del titular de los derechos; ID del protocolo; código de activación del Software; tipo de compresión de datos; ID del software; conjunto de identificadores del Software que pueden activarse en el dispositivo del usuario; localización de Software; versión completa del Software; ID de dispositivo único; fecha y hora en el dispositivo del usuario; ID de instalación del Software (PCID); versión del SO, número de compilación del SO, número de actualización del SO, edición del SO, información ampliada de la edición del SO; modelo del dispositivo; familia del sistema operativo; 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 procesa; encabezado de la licencia del Software; ID de un centro de activación regional; fecha y hora de creación de la clave de la licencia del Software; ID de la licencia del Software; ID del modelo de información usado para proporcionar la licencia del software; fecha y hora de caducidad de la licencia del Software; estado actual de la clave de la licencia del Software; tipo de licencia del Software usada; tipo de licencia usada para activar el Software; ID del 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 procesa; suma de comprobación del objeto que se procesa; ID del componente del software;

- ID del registro desencadenado en las bases de datos antivirus del software; marca de tiempo del registro desencadenado en las bases de datos antivirus del software; tipo de registro desencadenado en las bases de datos antivirus del software; nombre del malware detectado o del software lícito que puede usarse para ocasionar daños al dispositivo o a los datos de usuario;

- nombre de la tienda desde donde se instaló la aplicación; nombre del paquete de la aplicación; clave pública usada para firmar el archivo APK; suma de comprobación del certificado usado para firmar el archivo APK; marca de tiempo del certificado digital;

- versión completa del Software; ID de actualización del Software; tipo de Software instalado; el identificador de la configuración; el resultado de la acción del software; código de error;

- números que derivan del archivo APK de la aplicación Android según ciertas reglas matemáticas y que no permiten restaurar el contenido del archivo original; estos datos no contienen nombres de archivos, rutas de archivos, direcciones, números de teléfono ni otra información personal de los usuarios.

Si utiliza los servidores de actualización del Titular del Derecho a fin de descargar las Actualizaciones, el Usuario Final, para aumentar la eficacia del procedimiento de actualización, acepta proporcionar periódicamente al Titular del Derecho la siguiente información:

- ID del Software derivado de la licencia; versión completa del Software; ID de la licencia del Software; tipo de licencia del Software usada; ID de instalación del Software (PCID); ID de inicio de la actualización del Software; dirección web que se procesa.

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 desencadenado en las bases de datos antivirus del software; marca de tiempo del registro desencadenado en las bases de datos antivirus del software; tipo de registro desencadenado en las bases de datos antivirus del software; hora y fecha de 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 ampliada de la edición del SO; versión de Service Pack del SO; características de detección; suma de comprobación (MD5) del objeto que se procesa; nombre del objeto que se procesa; mensaje que indica si el objeto que se procesa es un archivo PE; suma de comprobación (MD5) de la máscara que bloqueó el servicio web; suma de comprobación (SHA256) del objeto que se procesa; tamaño del objeto que se procesa; código del tipo de objeto; la decisión del Software sobre el objeto que se procesa; ruta hacia el objeto que se procesa; código de directorio; versión del componente del Software; versión de las estadísticas enviadas; dirección del servicio web a la que se accedió (URL, IP); tipo de cliente usado para acceder al servicio web; dirección IPv4 del servicio web a la que se accedió; dirección IPv6 del servicio web a la que se accedió; dirección web del origen de la solicitud de servicio web (referenciador); dirección web que se procesa;

- información sobre los objetos analizados (versión de la aplicación de AndroidManifest.xml); la decisión del Software sobre la aplicación; método usado para obtener la decisión del Software sobre la aplicación; nombre del paquete de Installer de la tienda; nombre del paquete (o nombre de distribución) de AndroidManifest.xml; categoría de Google SafetyNet; mensaje que indica si SafetyNet está habilitado en el dispositivo; valor SHA256 de la respuesta de Google SafetyNet; esquema de firma APK para el certificado APK; código de versión del Software instalado; número de serie del certificado que se usó para firmar el archivo APK; nombre del archivo APK que se está instalando; ruta del archivo APK que se está instalando; emisor del certificado que se usó 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 enviadas; algoritmo para calcular la huella digital del certificado digital; hash MD5 del archivo APK instalado; hash MD5 del archivo DEX ubicado dentro del archivo APK; permisos otorgados de manera dinámica a la aplicación; versión del software de terceros; mensaje que indica si la aplicación es la mensajería SMS predeterminada; mensaje que indica si la aplicación tiene derechos de Administrador del dispositivo; mensaje que indica si la aplicación se encuentra en el catálogo del sistema; mensaje que indica si la aplicación usa servicios de accesibilidad);

- información sobre objetos y actividades potencialmente maliciosos (contenido en fragmentos del objeto que se está procesando; fecha y hora de caducidad del certificado; fecha y hora de emisión del certificado; ID de la clave de la tienda de claves utilizada para el cifrado; protocolo usado para intercambiar datos con KSN; orden de fragmentos del objeto que se procesa; datos del registro interno, generados por el módulo del Software antivirus para un objeto que se procesa; 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 firma del objeto; configuración y nombre del propietario del certificado; huella digital del certificado digital del objeto analizado y algoritmo de dispersión; fecha y hora de la última modificación del objeto que se procesa; fecha y hora de creación de un objeto que se procesa; los objetos o las partes de los objetos que se procesan; descripción de un objeto que se procesa como se define en las propiedades del objeto; formato del objeto que se procesa; tipo de suma de comprobación para el objeto que se procesa; suma de comprobación (MD5) del objeto que se procesa; nombre del objeto que se procesa; suma de comprobación (SHA256) del objeto que se procesa; tamaño del objeto que se procesa; nombre del proveedor del Software; la decisión del Software sobre el objeto que se procesa; versión del objeto que se procesa; origen de la decisión tomada para el objeto que se procesa; suma de comprobación del objeto que se procesa; nombre de la aplicación principal; ruta hacia el objeto que se procesa; información acerca de los resultados de comprobación de la firma del archivo; clave de sesión de inicio; algoritmo de cifrado para la clave de sesión de inicio; tiempo de almacenamiento para el objeto que se procesa; algoritmo para calcular la huella digital del certificado digital);

- tipo de compilación, por ejemplo, "usuario" o "eng"; nombre completo del producto; fabricante del producto/hardware; si se pueden instalar apps desde fuera de Google Play; estado del servicio en la nube para la verificación de las apps de Google; estado del servicio en la nube para la verificación de las apps de Google que se instalan por medio de ADB; nombre en código de desarrollo actual o "REL" para compilaciones de producción; número progresivo de la compilación; cadena de versiones 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; mensaje que indica si el dispositivo tiene acceso a los permisos de administración (root); sistema operativo; nombre del Software; tipo de licencia del Software usada;

- información sobre la calidad de los servicios KSN (protocolo utilizado para intercambiar datos con KSN; ID del servicio KSN al que se accede mediante el Software; fecha y hora en que se dejaron de recibir las estadísticas; cantidad de conexiones de KSN tomadas desde el caché; cantidad de solicitudes para las cuales se encontró una respuesta en la base de datos de solicitudes local; cantidad de conexiones de KSN no exitosas; cantidad de transacciones KSN no exitosas; distribución temporal de las solicitudes a KSN canceladas; distribución temporal de las conexiones a KSN sin éxito; distribución temporal de las transacciones de KSN sin éxito; distribución temporal de las conexiones a KSN exitosas; distribución temporal de las transacciones de KSN exitosas; distribución temporal de las solicitudes a KSN exitosas; distribución temporal de las solicitudes a KSN que expiraron; cantidad de conexiones KSN nuevas; cantidad de solicitudes a KSN sin éxito causadas por errores de enrutamiento; cantidad de solicitudes sin éxito causadas porque KSN estaba deshabilitado en la configuración del Software; cantidad de solicitudes a KSN sin éxito causadas por problemas de la red; cantidad de conexiones a KSN exitosas; cantidad de transacciones de KSN exitosas; cantidad total de solicitudes a KSN; fecha y hora en que se empezaron 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 hacia el archivo APK sin el nombre del archivo; altura de superposición; información sobre el Software superpuesto: hash MD5 del archivo APK; información superpuesta de la aplicación: hash MD5 del archivo classes.dex; información superpuesta de la aplicación: nombre del archivo APK; información superpuesta de la aplicación: ruta hacia el archivo APK sin el nombre del archivo; información superpuesta de la aplicación: nombre del paquete de la aplicación (para la aplicación superpuesta: si el anuncio se muestra en un escritorio vacío, el valor debe ser "ejecutor"); fecha y hora de la superposición; información sobre la aplicación superpuesta: nombre del paquete de la aplicación; ancho de la superposición;

- configuraciones del punto de acceso de Wi-Fi en uso (tipo de dispositivo detectado; configuración de DHCP (sumas de comprobación de la IPv6 local de la puerta de enlace, IPv6 de DHCP, IPv6 de DNS1, IPv6 de DNS2; suma de comprobación de la duración del prefijo de red; suma de comprobación de la dirección de IPv6 local); configuración de DHCP (sumas de comprobación de la dirección IP local de la puerta de enlace, IP de DHCP, IP de DNS1, IP de DNS2 y máscara de subred); mensaje que indica si el dominio DNS existe; suma de comprobación de la dirección IPv6 local asignada; suma de comprobación de la dirección IPv4 local asignada; mensaje que indica si el dispositivo está conectado; tipo de autenticación de la red Wi-Fi; lista de las 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 que admite el punto de acceso Wi-Fi; tipo de cifrado de la red Wi-Fi; hora local del inicio y la finalización de la conexión de la red Wi-Fi; ID de 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 red Wi-Fi basada en el nombre de la red Wi-Fi y la dirección MAC del punto de acceso; fuerza de la señal de Wi-Fi; nombre de la red Wi-Fi; conjunto de protocolos de autenticación que admite esta configuración; protocolo de autenticación usado para una conexión WPA-EAP; protocolo de autenticación interno; conjunto de cifrados de grupo que admite esta configuración; conjunto de protocolos de administración de claves que admite esta configuración; la categoría final de privacidad de la red en el Software; la categoría final de seguridad de la red en el Software; conjunto de cifrados de bloque para WPA que admite esta configuración; conjunto 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 que se realizó el pedido de la licencia del Software; ID del Software derivado de la licencia; número de serie de la clave de la licencia del Software; Localización de Software; mensaje que indica si la participación en KSN está habilitada; ID del Software con licencia; ID de la licencia del 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.

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 utilizando el servicio en la nube 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 de diagnóstico sobre el dispositivo del servicio de SafetyNet Attestation
- información sobre la configuración de Kaspersky Endpoint Security para Android como una función de accesibilidad
- información sobre transiciones entre pantallas de aplicaciones, duración de la sesión, inicio y final de una sesión de pantalla, nombre de 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 la bases de datos antivirus y sincronización con el Servidor Administrativo
- 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: el grupo etario y el género, el identificador de país de residencia y la lista de intereses

- información sobre la computadora del Usuario en la que se instaló el Software: el nombre del fabricante del equipo, el tipo de equipo, el modelo, la 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 que 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.

Certificación de SafetyNet

Durante el uso del Software, se enviarán los siguientes datos a SafetyNet Attestation automáticamente y de manera periódica a fin de alcanzar el propósito declarado:

- hora de verificación del dispositivo
- información sobre el software, nombre y datos de los certificados del software
- resultados de verificación del dispositivo
- verificaciones de identidad aleatorias para verificar los resultados de la verificación del dispositivo

  La transmisión de datos a SafetyNet Attestation se realiza a través de un canal seguro. La información sobre cómo se procesan los datos en SafetyNet Attestation se publica en: https://policies.google.com/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 app
- 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 destrabado o tiene acceso a los permisos de administración (root)
- fuerza de la señal
- duración de los rastros automatizados

- red y la información correspondiente a continuación: código de respuesta, tamaño de la 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 se encuentra 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 del dispositivo
- espacio total del disco y cantidad usada actualmente
- nombre y versión del SO
- RAM total y cantidad usada actualmente
- mensaje que indica si el dispositivo tiene acceso a los permisos de administración (root)
- orientación de la pantalla al momento del evento
- fabricante del producto/hardware
- ID de instalación único
- versión de las estadísticas enviadas
- tipo de excepción de Software
- texto del mensaje de error
- marca que indica que la excepción de Software fue provocada por una excepción anidada
- ID de subproceso
- marca que indica si el marco fue el motivo del error de Software
- marca que indica que el subproceso provocó el cierre inesperado del Software
- información sobre la señal que provocó el cierre inesperado del Software: nombre de la señal, código de la señal, dirección de la señal

- para cada marco asociado con un subproceso, una excepción o un error: el 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 eventos ion que se produjeron antes del cierre inesperado del Software: identificador de 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 está publicada 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 Security para iOS

La versión móvil de Kaspersky Security cumple con las Normativas Generales de Protección de Datos (GDPR).

Para instalar la aplicación, el usuario de un dispositivo debe leer y aceptar los términos de las siguiente 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

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 Security 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 Security 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 Security 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 Acuerdo de licencia de usuario final

Con el fin de verificar el uso legítimo del Software, en los casos en que el Código de Activación se use para activar tal Software, 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 del Derecho; 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 del protocolo; código de activación del Software; tipo de compresión de datos; ID del software; conjunto de identificadores del Software que pueden activarse en el dispositivo del usuario; localización de Software; versión completa del Software; ID de dispositivo único; fecha y hora en el dispositivo del usuario; ID de instalación del Software (PCID); código de activación del Software usado actualmente; versión del SO, número de compilación del SO, número de actualización del SO, edición del SO, información ampliada de la edición del SO; modelo del dispositivo; código de proveedor móvil; familia del sistema operativo; ID del Software derivado de la licencia; lista de acuerdos presentados al usuario por el Software; tipo de contrato legal aceptado por el usuario mientras usa el Software; versión del contrato legal aceptado por el usuario mientras usa el Software; mensaje que indica si el usuario ha aceptado los términos del contrato legal mientras usa el Software; tipo de suma de comprobación para el objeto que se procesa; encabezado de la licencia del Software; ID de un centro de activación regional; fecha y hora de creación de la clave de la licencia del Software; ID de la licencia del Software; ID del modelo de información usado para proporcionar la licencia del software; fecha y hora de caducidad de la licencia del Software; estado actual de la clave de la licencia del Software; tipo de licencia del Software usada; tipo de licencia usada para activar el Software; ID del Software derivado de la licencia.

El Titular del Derecho también puede usar dicha información para recopilar datos estadísticos sobre la distribución y el uso de Software del Titular del Derecho.

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 del Derecho; dirección del servicio web a la que se accedió (URL, IP); número de puerto; dirección web del origen de la solicitud de servicio web (referenciador).

- versión completa del Software; ID de actualización del Software; tipo de Software instalado; ID del software; el identificador de la configuración; el resultado de la acción del software; código de error.

- dirección web que se procesa; dirección IPv4 del servicio web a la que se accedió; huella digital del certificado digital del objeto analizado y algoritmo de dispersión; tipo de certificado; contenidos del certificado digital que se procesa.

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 sobre la calidad de los servicios KSN (protocolo utilizado para intercambiar datos con KSN; ID del servicio KSN al que se accede mediante el Software; fecha y hora en que se dejaron de recibir las estadísticas; cantidad de conexiones de KSN tomadas desde el caché; cantidad de solicitudes para las cuales se encontró una respuesta en la base de datos de solicitudes local; cantidad de conexiones de KSN no exitosas; cantidad de transacciones KSN no exitosas; distribución temporal de las solicitudes a KSN canceladas; distribución temporal de las conexiones a KSN sin éxito; distribución temporal de las transacciones de KSN sin éxito; distribución temporal de las conexiones a KSN exitosas; distribución temporal de las transacciones de KSN exitosas; distribución temporal de las solicitudes a KSN exitosas; distribución temporal de las solicitudes a KSN que

expiraron; cantidad de conexiones KSN nuevas; cantidad de solicitudes a KSN sin éxito causadas por errores de enrutamiento; cantidad de solicitudes sin éxito causadas porque KSN estaba deshabilitado en la configuración del Software; cantidad de solicitudes a KSN sin éxito causadas por problemas de la red; cantidad de conexiones a KSN exitosas; cantidad de transacciones de KSN exitosas; cantidad total de solicitudes a KSN; fecha y hora en que se empezaron 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 de Software; mensaje que indica si la participación en KSN está habilitada; ID del Software con licencia; ID de la licencia del Software; ID del SO; versión del sistema operativo instalada 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.

Comuníquese 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 conseguir soporte técnico

Si no encuentra una solución a su problema en la documentación de Kaspersky Security para dispositivos móviles o las fuentes de información sobre Kaspersky Security para dispositivos móviles, póngase en contacto con el Servicio de soporte técnico. Los especialistas del Servicio de soporte técnico contestarán todas sus preguntas sobre la instalación y el uso de Kaspersky Security para dispositivos móviles.

Kaspersky ofrece asistencia técnica para Kaspersky Security para dispositivos móviles durante su vida útil (consulte la 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 ponerse en contacto con el Servicio de soporte técnico de una de las siguientes formas:

- Visitando el sitio web del Servicio de soporte técnico
- Enviando una solicitud de Servicio de soporte técnico desde el portal Kaspersky CompanyAccount

Soporte técnico a través de Kaspersky CompanyAccount

Kaspersky CompanyAccount es un portal para las compañías que usan las aplicaciones de 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 única cuenta de Kaspersky CompanyAccount. Esta cuenta única le permite administrar de forma centralizada las solicitudes electrónicas que envían los empleados registrados a Kaspersky, además de administrar los privilegios de estos empleados mediante Kaspersky CompanyAccount.

El portal Kaspersky CompanyAccount está disponible en los siguientes idiomas:

- 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.

Orígenes de información sobre la aplicación

Página web de Kaspersky Endpoint Security para dispositivos móviles en el sitio web de Kaspersky

En la página de Kaspersky Security para dispositivos móviles, podrá encontrar información general sobre la aplicación, sus funciones y sus parámetros de funcionamiento.

En la página web de Kaspersky Security para dispositivos móviles encontrará un enlace a la tienda electrónica. Donde podrá comprar la aplicación o hacer la renovación.

Página web de Kaspersky Security para dispositivos móviles en la Base de conocimientos

La *Base de conocimientos* es una sección del sitio web del Servicio de soporte técnico.

En la página de Kaspersky Security para dispositivos móviles 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.

En los artículos de la Base de conocimientos podrá encontrar respuesta a preguntas no solo relacionadas con Kaspersky Security para dispositivos móviles, sino también con otras aplicaciones de Kaspersky. Además, los artículos de la Base de conocimientos pueden incluir noticias de soporte técnico.

Ayuda en línea

La ayuda en línea de la aplicación incluye archivos de ayuda.

La ayuda contextual de los complementos de actualización de Kaspersky Security para dispositivos móviles ofrece información sobre las ventanas de Kaspersky Security Center: consisten en una descripción de la configuración de Kaspersky Security para dispositivos móviles y en enlaces a las descripciones de las tareas en las que se utiliza esa configuración.

La ayuda completa de las aplicaciones Kaspersky Endpoint Security para Android y Kaspersky Security para iOS proporciona información 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.

Administrador de dispositivos

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.

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.

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.

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.

Bases de datos antivirus

Bases de datos que contienen información sobre amenazas a la seguridad del equipo conocidas por Kaspersky a partir del lanzamiento de las bases de datos antivirus. Las entradas en bases de datos antivirus permiten detectar códigos maliciosos en objetos escaneados. Los especialistas de Kaspersky crean las bases de datos antivirus y las actualizan cada hora.

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.

Certificado del servicio Push Notification de Apple (APN)

Certificado firmado por Apple que le permite utilizar Apple Push Notification. A través de Apple Push Notification, un servidor de MDM para iOS puede administrar los dispositivos iOS.

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.

Complemento de administración de la aplicación

Componente dedicado que ofrece una interfaz para administrar las aplicaciones de Kaspersky mediante la Consola de administración. Cada aplicación que se puede administrar mediante Kaspersky Security Center SPE tiene su propio complemento de administración. El complemento de administración se incluye en todas las aplicaciones de Kaspersky que pueden administrarse mediante Kaspersky Security Center.

Contrato de licencia de usuario final

El contrato entre usted y Kaspersky AO que estipula los términos bajo los cuales puede usar la aplicación.

Control de cumplimiento

Una verificación de que la configuración de un dispositivo móvil y Kaspersky Endpoint Security para Android cumplen con los requisitos de seguridad corporativa. Los requisitos de seguridad corporativa regulan el uso del dispositivo. Por ejemplo, el dispositivo debe tener activada la protección en tiempo real, las bases de datos antivirus deben estar actualizadas y la contraseña del dispositivo debe ser bastante segura. El control de cumplimiento se basa en una lista de reglas. Una regla de cumplimiento incluye los siguientes componentes:

- El criterio de control del dispositivo (por ejemplo, ausencia de aplicaciones prohibidas en el dispositivo)
- El intervalo de tiempo asignado para que el usuario solucione instancias de incumplimiento (por ejemplo, 24 horas)
- La acción que se tomará en el dispositivo si el usuario no resuelve el incumplimiento en el tiempo asignado (por ejemplo, bloqueo del dispositivo)

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.

Desbloquear el código

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.

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.

Dispositivo de MDM de iOS

Un dispositivo móvil iOS controlado por el Servidor de MDM para iOS.

Dispositivo EAS

Dispositivo móvil conectado al Servidor de administración a través del protocolo Exchange ActiveSync.

Dispositivo supervisado

Dispositivo iOS con configuración monitoreada por Apple Configurator, un programa para la configuración grupal de dispositivos iOS. El estado del dispositivo supervisado es *supervisado* en Apple Configurator. Cada vez que un dispositivo supervisado se conecta al equipo, Apple Configurator compara la configuración del dispositivo con la configuración de referencia especificada y, de ser necesario, la redefine. Un dispositivo supervisado no se puede sincronizar con el Apple Configurator instalado en un equipo diferente.

Cada dispositivo supervisado proporciona más configuraciones para redefinir a través de 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, todos los dispositivos móviles no son supervisados.

Estación de trabajo del administrador

El equipo en el que se ha implementado la Consola de administración de Kaspersky Security Center. Si el complemento de administración de aplicaciones está instalado en la estación de trabajo del administrador, este puede gestionar las aplicaciones móviles de Kaspersky Endpoint Security implementadas en los dispositivos de los usuarios.

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.

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.

Kaspersky Private Security Network (KSN privada)

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 de los usuarios 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.

Kaspersky Security Network (KSN)

Una infraestructura de servicios en la nube que proporciona acceso a la base de datos de Kaspersky con información que se actualiza constantemente sobre la reputación de los archivos, los recursos web y el 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.

Licencia

Un derecho limitado para usar la aplicación concedido por el Contrato de licencia de usuario final.

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.

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.

Perfil de MDM para iOS

Perfil que contiene un conjunto de valores de configuración para conectar dispositivos móviles iOS con el Servidor de Administración. Un perfil de MDM de iOS permite distribuir perfiles de configuración de iOS en segundo plano mediante el Servidor de dispositivos móviles de MDM de iOS, y también recibir información de diagnóstico ampliada sobre los dispositivos móviles. Enlace al perfil de MDM de iOS que se debe enviar a un usuario para que el Servidor de dispositivos móviles de MDM de iOS pueda detectar y conectar el dispositivo móvil iOS del usuario.

Perfil de trabajo de Android

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 perfil de trabajo en el dispositivo móvil del usuario, se instalan las siguientes aplicaciones corporativas automáticamente en el perfil de trabajo: Google Play Market, Google Chrome, Descargas, Kaspersky Endpoint Security para Android y otras. Las aplicaciones corporativas instaladas en el perfil de trabajo y las notificaciones de estas aplicaciones se marcan con un icono de maletín rojo. Debe crear una cuenta corporativa de Google separada para la aplicación Google Play Market. Las aplicaciones instaladas en el perfil de trabajo aparecen en la lista común de aplicaciones.

Perfil del aprovisionamiento

Colección de configuraciones para la operación de aplicaciones en dispositivos iOS móviles. Un perfil de aprovisionamiento que contiene información sobre la licencia y está vinculado a una aplicación específica.

Phishing

Tipo de estafa en Internet destinada a obtener el acceso no autorizado a los datos confidenciales de los usuarios.

POP3

Protocolo de red usado por un cliente de correo para recibir mensajes de un servidor de correo.

Servidor de actualizaciones 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.

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.

Servidor de dispositivo móvil Exchange

Un componente de Kaspersky Endpoint Security que le permite conectar dispositivos móviles Exchange ActiveSync al Servidor de administración.

Servidor de dispositivos móviles con MDM de 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).

Servidor proxy

Un servicio de red del equipo que permite que los usuarios hagan solicitudes indirectas a otros servicios de red. En primer lugar, un usuario se conecta a un servidor proxy y solicita un recurso (por ejemplo, un archivo) localizado en otro servidor. Luego, el servidor proxy se conecta al servidor específico y obtiene el recurso de él o devuelve el recurso desde su propia caché (si el proxy posee una caché propia). En algunos casos, una solicitud de usuario o una respuesta del servidor pueden ser modificadas por el servidor proxy para determinados fines.

Servidor web de Kaspersky Security Center

Un componente de Kaspersky Security Center que se instala con el Servidor de administración. Web Server está diseñado para la transmisión, a través de una red, de paquetes de instalación independientes, perfiles de MDM para iOS y archivos desde una carpeta compartida.

Solicitud de firma de certificado

Archivo con la configuración de un Servidor de administración que es aprobado por Kaspersky y luego enviado a Apple para obtener un certificado de APNs.

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.

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.

Tarea de grupo

Tarea pensada para un grupo de administración y ejecutada en todos los dispositivos gestionados que se incluyen en el grupo.

Término de 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.

Virus

Un programa que infecta otros agregando su código a ellos para tomar el control cuando se ejecutan archivos infectados. Esta definición simple permite identificar la acción principal realizada por cualquier virus: la infección.

Información sobre el 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 Security 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 dueños.

PostScript es una marca comercial registrada o una marca comercial de Adobe en los Estados Unidos o en otros países.

AirDrop y AirPrint son marcas comerciales de Apple Inc.

Apple, Apple Configurator, AirPlay, AirPort Express, App Store, Apple TV, Bonjour, Face ID, FaceTime, FileVault, iBooks, iCal, iCloud, iPad, iPadOS, iPhone, iTunes, OS X, Safari, Spotlight y Touch ID son marcas comerciales de Apple Inc. registradas en EE. UU. y otros países y regiones.

Aruba Networks es una marca comercial de Aruba Networks, Inc. en los Estados Unidos y otros países.

La palabra, la marca y los logotipos de Bluetooth son propiedad de Bluetooth SIG, Inc.

Cisco, Cisco AnyConnect e IOS son marcas comerciales registradas o marcas comerciales de Cisco Systems, Inc. o sus empresas afiliadas en los Estados Unidos y otros países.

SecurID es una marca comercial registrada o una marca comercial de EMC Corporation en los Estados Unidos u otros países.

Google, Android, Chrome, Chromebook, Chromium, Crashlytics, Firebase, Google Analytics, Google Chrome, Google Mail, Google Maps, Google Play, Nexus y SPDY son marcas comerciales de Google LLC.

HTC es una marca comercial de HTC Corporation.

Huawei, HUAWEI y EMUI son marcas comerciales de Huawei Technologies Co., Ltd registradas en China y otros países.

IBM y Maas360 son marcas comerciales de International Business Machines Corporation, registradas en muchas jurisdicciones en todo el mundo.

Juniper Networks, Juniper y JUNOS son marcas comerciales o marcas comerciales registradas de Juniper Networks, Inc. en los Estados Unidos y otros países.

Microsoft, ActiveSync, Microsoft Intune, Tahoma, Windows, Windows Mobile y Windows Phone 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.

Oracle y JavaScript son marcas comerciales registradas de Oracle o sus empresas afiliadas.

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.

SOTI y MobiControl son marcas comerciales registradas de SOTI Inc. en los Estados Unidos y en otras jurisdicciones.