kaspersky

Kaspersky Security for Mobile

Contenido

Ayuda de Kaspersky Security for Mobile

Novedades

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

Kit de distribución

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

- Acerca de la administración de dispositivos móviles en Kaspersky Security Center Web Console y Cloud Console
  - Funciones clave de administración de dispositivos móviles en Kaspersky Security Center Web Console y Cloud Console
  - Acerca de la aplicación Kaspersky Endpoint Security for Android
  - Acerca de la aplicación Kaspersky Security for iOS
  - Acerca del complemento de Kaspersky Security for Mobile (Devices)
  - Acerca del complemento de Kaspersky Security for Mobile (Policies)
  - Requisitos de hardware y software
  - Consideraciones y problemas conocidos
- Despliegue de una solución de administración de dispositivos móviles en Kaspersky Security Center Web Console o Cloud Console
  - Escenarios de despliegue
  - Preparación de Kaspersky Security Center Web Console y Cloud Console para el despliegue
    - Configuración del Servidor de administración para la conexión de dispositivos móviles
    - Creación de un grupo de administración
    - Creación de una regla para asignar automáticamente un dispositivo a grupos de administración
  - Despliegue de complementos de administración
    - Instalación de complementos de administración a partir de la lista de paquetes de distribución disponibles
    - Instalando los complementos de administración desde el paquete de distribución
  - Despliegue de la aplicación móvil
    - Despliegue de la aplicación móvil mediante el uso de Kaspersky Security Center Web Console o Cloud Console
    - Activación de la aplicación móvil
    - Proporcionar los permisos necesarios para la aplicación Kaspersky Endpoint Security for Android
  - Administración de certificados
    - Visualización de la lista de certificados
    - Definición de la configuración de certificados
    - Creación de un certificado
    - Renovación de un certificado
    - Eliminación de un certificado
  - Intercambio de información con Firebase Cloud Messaging
- Administración de dispositivos móviles en Kaspersky Security Center Web Console y Cloud Console
  - Conexión de dispositivos móviles a Kaspersky Security Center
  - Movimiento de dispositivos móviles no asignados a grupos de administración
  - Envío de comandos a dispositivos móviles
  - Eliminación de dispositivos móviles de Kaspersky Security Center
- Administración de directivas de grupo
  - Directivas de grupo para administrar dispositivos móviles
  - Visualización de la lista de directivas de grupo
  - Visualización de los resultados de la distribución de directivas
  - Creación de una directiva de grupo
  - Modificación de una directiva de grupo
  - Copia de una directiva de grupo

Movimiento de una directiva a otro grupo de administración
Eliminación de una directiva de grupo
Definición de la configuración de directivas
Configuración de la protección antivirus
Configuración de la protección en tiempo real
Configuración de la ejecución automática de análisis antivirus en un dispositivo móvil
Configuración de las actualizaciones de bases de datos antivirus
Definición de la configuración de desbloqueo del dispositivo
Configuración de la protección de datos de dispositivos robados o extraviados
Configuración del control de aplicaciones
Configuración del control de cumplimiento de dispositivos móviles con requisitos corporativos de seguridad
Cómo activar y desactivar las reglas de cumplimiento
Cómo editar reglas de cumplimiento
Cómo añadir reglas de cumplimiento
Cómo eliminar reglas de cumplimiento
Lista de criterios de incumplimiento
Lista de acciones en caso de incumplimiento
Configuración del acceso del usuario a sitios web
Configuración de restricciones de las funciones
Protección de Kaspersky Endpoint Security for Android contra eliminación
Configuración de la sincronización de dispositivos móviles con Kaspersky Security Center
Kaspersky Security Network
Intercambio de información con Kaspersky Security Network
Cómo activar y desactivar Kaspersky Security Network
Intercambio de información con Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics
Configuración de notificaciones en dispositivos móviles
Detección de pirateos del dispositivo
Definición de la configuración de las licencias
Configuración de eventos
Configuración de eventos sobre la instalación, actualización y eliminación de aplicaciones en los dispositivos de los usuarios
Carga de la red
Trabajar en la Consola de administración basada en MMC
Principales casos de uso
Acerca de Kaspersky Security for Mobile
Funciones clave de administración de dispositivos móviles en la Consola de administración basada en MMC
Acerca de la aplicación de Kaspersky Endpoint Security for Android
Acerca de Kaspersky Device Management for iOS
Acerca de un buzón de correo de Exchange
Instalación del complemento de administración Kaspersky Endpoint Security for Android
Acerca del complemento de administración Kaspersky Device Management for iOS
Requisitos de hardware y software
Consideraciones y problemas conocidos
Despliegue
Arquitectura de la solución
Escenarios comunes de implementación de la solución integrada
Escenarios de implementación de Kaspersky Endpoint Security for Android
Escenarios de implementación para el perfil de MDM para iOS

- Preparación de la Consola de administración para la implementación de la solución integrada
  - Configuración del Servidor de Administración para la conexión de dispositivos móviles
  - Visualización de la carpeta Administración de dispositivos móviles en la Consola de administración
  - Creación de un grupo de administración
  - Creación de una regla para asignación automática de dispositivos a grupos de administración
  - Creación de un certificado general
- Instalación de Kaspersky Endpoint Security for Android
  - Permisos
  - Instalación de Kaspersky Endpoint Security for Android mediante un enlace de Google Play
  - Otros métodos de instalación de Kaspersky Endpoint Security for Android
    - Instalación manual desde Google Play o Huawei AppGallery
    - Crear y configurar un paquete de instalación
    - Creación de un paquete de instalación independiente
  - Configuración de los ajustes de sincronización
- Activación de la aplicación Kaspersky Endpoint Security for Android
- Instalación de un perfil de MDM para iOS
  - Acerca de los modos de administración de dispositivos iOS
  - Instalación a través de Kaspersky Security Center
- Instalación de complementos de administración
- Actualización de una versión anterior de la aplicación
  - Actualización de la versión anterior de Kaspersky Endpoint Security for Android
  - Instalación de una versión anterior de Kaspersky Endpoint Security for Android
  - Actualización de versiones anteriores de complementos de administración
- Eliminación de Kaspersky Endpoint Security for Android
  - Eliminación remota de la aplicación
  - Permitir que los usuarios eliminen la aplicación
  - Eliminación de la aplicación por parte del usuario

Configuración y administración

- Primeros pasos
  - Inicio y cierre de la aplicación
  - Creación de un grupo de administración
  - Directivas de grupo para administrar dispositivos móviles
    - Creación de una directiva de grupo
    - Configuración de los ajustes de sincronización
    - Administrar revisiones de directivas de grupo
    - Eliminar una directiva de grupo
    - Restricción de permisos para configurar directivas de grupo
- Protección
  - Configuración de la protección antivirus en dispositivos Android
  - Protección de dispositivos Android en Internet
  - Protección de datos de dispositivos robados o extraviados
    - Envío de comandos a un dispositivo móvil
    - Desbloqueo de un dispositivo móvil
    - Cifrado de datos
  - Configuración de la seguridad de la contraseña de desbloqueo de dispositivos
    - Configuración de una contraseña de desbloqueo segura para un dispositivo Android
    - Configuración de una contraseña de desbloqueo segura para dispositivos MDM de iOS
    - Configuración de una contraseña de desbloqueo segura para dispositivos EAS

- Configuración de una red privada virtual (VPN)
  - Configuración de VPN en dispositivos Android (solo Samsung)
  - Configuring VPN on iOS MDM devices
- Configuración de firewall en dispositivos Android (solo Samsung)
- Protección de Kaspersky Endpoint Security for Android contra eliminación
- Detección de pirateos del dispositivo (acceso root)
- Configuración de un proxy HTTP global en dispositivos de MDM de iOS
- Adición de certificados de seguridad de dispositivos de MDM de iOS
- Adición de un perfil de SCEP a dispositivos de MDM de iOS

Control

- Configuración de restricciones
  - Consideraciones especiales para dispositivos con Android versión 10 o posterior
  - Configuración de restricciones para dispositivos Android
  - Configuración de las restricciones de las funciones del dispositivo iOS con MDM
  - Configuración de las restricciones de las funciones del dispositivo EAS
- Configuración del acceso del usuario a sitios web
  - Configuración del acceso a sitios web en dispositivos Android
  - Configuración del acceso a sitios web en dispositivos MDM de iOS
- Control de cumplimiento de dispositivos Android con requisitos de seguridad corporativa
- Control de inicio de la aplicación
  - Control de inicio de la aplicación en dispositivos Android
  - Configuración de restricciones del dispositivo EAS para aplicaciones
- Inventario del software en dispositivos Android
- Configuración de la visualización de dispositivos Android en Kaspersky Security Center

Administración

- Configuración de conexión a una red Wi-Fi
  - Conexión de dispositivos Android a una red Wi-Fi
  - Conexión de dispositivos MDM de iOS a una red Wi-Fi
- Configuración de correo electrónico
  - Configuración de un buzón de correo en dispositivos MDM de iOS
  - Configuración de un buzón de correo de Exchange en dispositivos MDM de iOS
  - Configuración de un buzón de correo de Exchange en dispositivos Android (solo Samsung)
- Administración de aplicaciones móviles de terceros
- Configurar notificaciones de Kaspersky Endpoint Security for Android
- Conexión de dispositivos de MDM de iOS a AirPlay
- Conexión de dispositivos de MDM de iOS a AirPrint
- Configuración del Nombre de punto de acceso (APN)
  - Configuración de APN en dispositivos Android (solo Samsung)
  - Configuración de APN en dispositivos MDM de iOS
- Configuración del perfil de trabajo de Android
  - Acerca del perfil de trabajo de Android
  - Configuración del perfil de trabajo
- Adición de una cuenta de LDAP
- Adición de una cuenta de calendario
- Adición de una cuenta de un contacto
- Configuración de la suscripción al calendario
- Adición de clips web
- Adición de fuentes

- Administración de la aplicación mediante el uso de los sistemas EMM de terceros (solo Android)
  - Primeros pasos
  - Cómo instalar la aplicación
  - Cómo activar la aplicación
  - Cómo conectar un dispositivo a Kaspersky Security Center
  - Archivo AppConfig
- Carga de la red
- Participación en Kaspersky Security Network
  - Intercambio de información con Kaspersky Security Network
  - Activación y desactivación del uso de Kaspersky Security Network
  - Uso de Kaspersky Private Security Network
- Provisión de datos a servicios de terceros
  - Intercambio de información con Firebase Cloud Messaging
  - Intercambio de información con Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics
- Aceptación global de declaraciones adicionales
- Samsung KNOX
  - Instalación de la aplicación Kaspersky Endpoint Security for Android mediante la inscripción móvil de KNOX
    - Crear un perfil MDM de KNOX
    - Añadir dispositivos a la inscripción móvil de KNOX
    - Instalación de la aplicación
  - Configuración de los contenedores KNOX
    - Acerca de los contenedores KNOX
    - Activación de Samsung KNOX
    - Configuración de firewall en KNOX
    - Configuración de un buzón de correo de Exchange en KNOX
- Apéndices
  - Permisos para configurar directivas de grupo
  - Categorías de aplicación

Uso de la aplicación Kaspersky Endpoint Security for Android

- Funciones de la aplicación
- Ventana principal de un vistazo
- Análisis del dispositivo
- Ejecución de análisis programado
- Cambio del modo de protección
- Actualizaciones de bases de datos antivirus
- Actualización de la base de datos planificada
- Qué hacer en caso de pérdida o robo del dispositivo
- Protección web
- Control de aplicaciones
- Obtener certificado
- Sincronizando con Kaspersky Security Center
- Activación de la aplicación Kaspersky Endpoint Security for Android sin Kaspersky Security Center
- Actualización de la app
- Eliminación de la app
- Aplicaciones con un icono de maletín
- Aplicación KNOX

Uso de la aplicación Kaspersky Security for iOS

- Funciones de la aplicación
- Instalación de la aplicación
- Activación de la aplicación
- Activar la aplicación con un código de activación
- Ventana principal de un vistazo
- Actualización de la app
- Eliminación de la app

Licencia de aplicaciones
- Acerca del Contrato de licencia de usuario final
- Información sobre la licencia
- Acerca de la suscripción
- Acerca de la clave
- Acerca del código de activación
- Acerca del fichero llave
- Provisión de datos en Kaspersky Endpoint Security for Android
- Provisión de datos en Kaspersky Security for iOS

Póngase en contacto con Servicio de soporte técnico
- Cómo conseguir soporte técnico
- Soporte técnico a través de Kaspersky CompanyAccount

Fuentes de información sobre la aplicación

Glosario
- Activación de la aplicación
- Administrador de dispositivos
- Administrador de Kaspersky Security Center
- Archivo de manifiesto
- Bases de datos antivirus
- Categorías de Kaspersky
- Certificado del servicio Push Notification de Apple (APN)
- Código de activación
- Código de desbloqueo
- Complemento de administración de la aplicación
- Contrato de licencia de usuario final
- Control de cumplimiento
- Cuarentena
- Directiva
- Dispositivo de MDM de iOS
- Dispositivo EAS
- Dispositivo supervisado
- Estación de trabajo del administrador
- Fichero llave
- Grupo de administración
- IMAP
- Kaspersky Private Security Network (KSN privada)
- Kaspersky Security Network (KSN)
- Licencia
- Paquete de instalación
- Paquete de instalación independiente
- Perfil de MDM para iOS

Perfil de trabajo de Android
Perfil del aprovisionamiento
Phishing
Plazo de la licencia
POP3
Servidor de Administración
Servidor de dispositivo móvil Exchange
Servidor de dispositivos móviles de MDM de iOS
Servidor proxy
Servidor web de Kaspersky Security Center
Servidores de actualizaciones de Kaspersky
Solicitud de firma de certificado
SSL
Suscripción
Tarea de grupo
Virus
Información sobre el código de terceros
Avisos de marcas comerciales

Ayuda de Kaspersky Security for Mobile

Kaspersky Security for Mobile 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 for Mobile dependen de la consola de Kaspersky Security Center que utiliza como interfaz para proteger y administrar los dispositivos móviles.

Seleccione la sección necesaria 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

En diversas secciones de Ayuda se describen funcionalidades y operaciones disponibles para usuarios de las aplicaciones Kaspersky Endpoint Security for Android y Kaspersky Security for iOS.

Novedades

Kaspersky Security for iOS, versión técnica 1

La nueva aplicación Kaspersky Security for iOS está diseñada para proteger y gestionar los dispositivos iOS y iPadOS corporativos. La aplicación ofrece las siguientes funciones clave:

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

Kaspersky Endpoint Security for Android, versión técnica 42

- Mejoras en la interfaz de usuario de la aplicación Kaspersky Endpoint Security for Android.
- La aplicación Kaspersky Endpoint Security for Android ahora necesita el permiso "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 for Android, versión técnica 41

- Mejoras en la interfaz de usuario de la aplicación Kaspersky Endpoint Security for Android.
- Mejoras en la interfaz de usuario de 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 for Android, versión técnica 40

- Mejoras y correcciones de errores generales.

Kaspersky Endpoint Security for 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 relativa al procesamiento de la información para fines 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 for Android en dispositivos.

- Mejoras y correcciones de errores generales.

Kaspersky Endpoint Security for Android, versión técnica 33

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

Kaspersky Endpoint Security for Android, versión técnica 32

- La aplicación Kaspersky Endpoint Security for Android se ha modificado para admitir los requisitos actualizados de Android.

Kaspersky Endpoint Security for Android, versión técnica 31

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

Kaspersky Endpoint Security for Android, versión técnica 30

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

Kaspersky Endpoint Security for Android, versión técnica 29

- Ahora, la aplicación Kaspersky Endpoint Security for Android funciona con Android 12.

Kaspersky Endpoint Security for Android, versión técnica 27

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

Kaspersky Endpoint Security for Android, versión técnica 26

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

Kaspersky Endpoint Security for 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 for Android, versión técnica 20

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

Kaspersky Endpoint Security for 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 solucionado varios errores y se ha mejorado la estabilidad de uso.

Kaspersky Endpoint Security for Android, versión técnica 18

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

Kaspersky Endpoint Security for 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 solucionado varios errores y se ha mejorado la estabilidad de uso.

Kaspersky Endpoint Security for Android, versión técnica 16

- Ahora, Kaspersky Endpoint Security for Android funciona con Android 11.

- Android 11 ha introducido nuevos requisitos para los permisos de geolocalización y cámara. Puede leer más acerca de las nuevas reglamentaciones 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 for 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 for Android, versión técnica 13

- Nuevo diseño de la interfaz de usuario de Kaspersky Endpoint Security for Android.

- Ahora todas las secciones de ayuda están en línea.

- Las direcciones IP de los dispositivos administrados ahora se envían a Kaspersky Security Center y pueden verse en las secciones de información del dispositivo.

Kaspersky Endpoint Security for Android, versión técnica 12

- Se agregó la capacidad de aceptar de forma remota 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 app omite estos pasos durante el proceso de instalación de la app.

- Se añadió la capacidad de editar el nombre del dispositivo en Kaspersky Security Center para usuarios que utilizan VMware AirWatch. Añadimos una nueva opción al archivo de configuración, que se utiliza para configurar la app. Puede añadir 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 for Android, versión técnica 11

Se han solucionado varios errores y se ha mejorado la estabilidad de uso.

Kaspersky Endpoint Security for Android, versión técnica 10

- Ahora, Kaspersky Security for Mobile es compatible con Kaspersky Security Center 12.

- Se ha interrumpido la compatibilidad con Kaspersky Safe Browser en Kaspersky Security Center 12. Puede utilizar las funciones de Kaspersky Safe Browser cuando use Kaspersky Security Center 11 o versiones anteriores.

- Se han solucionado varios errores y se ha mejorado la estabilidad de uso.

Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 3

- Compatibilidad comprobada de Kaspersky Endpoint Security for Android en Microsoft Intune (una solución de Gestión de Movilidad Empresarial (EMM)). Kaspersky participa en la Comunidad AppConfig para garantizar que la app funcione con soluciones de EMM de terceros.

- Se agregó la capacidad de desactivar las notificaciones y los mensajes emergentes cuando la app está 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 app está en segundo plano, la app 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 app.

- Se agregó 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 for Android omitirá el paso de aceptación en el Asistente de configuración inicial.

- Se agregó la Declaración relativa al procesamiento de datos para el uso de Protección web (Declaración de Protección web). Debe aceptar la declaración para usar la Protección web. Kaspersky Endpoint Security for Android usa Kaspersky Security Network (KSN) para analizar sitios web. La Declaración de Protección web contiene los términos y 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 solucionado varios errores y se ha mejorado la estabilidad de uso.

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 for iOS)	Disponible (mediante la aplicación Kaspersky Security for iOS)
Administración de dispositivos móviles			
Añadido de dispositivos mediante un enlace de Google Play	Disponible	Disponible	Disponible
Añadido de dispositivos mediante un enlace de App Store	No disponible	Disponible	Disponible
Añadido de dispositivos iOS mediante un perfil de MDM para iOS	Disponible	No disponible	No disponible
Añadido 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 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 bases de datos antivirus	Disponible	Disponible	Disponible
Configuración de la protección de datos de dispositivos robados o extraviados	Disponible	Disponible	Disponible
Configuración del acceso del usuario a sitios web	Disponible	Disponible	Disponible
Configuración del control de aplicaciones	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	Disponible	No disponible	No disponible

conexión a una red Wi-Fi			
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 for Mobile puede incluir varios componentes, según la versión de la 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 los 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 for Android para administrar la aplicación mediante el sistema de administración remota de Kaspersky Security Center.

- `Klmdminst.exe`

  Instalador del complemento de administración de Kaspersky Device Management for iOS para administrar la aplicación mediante el sistema de administración remota de Kaspersky Security Center.

Archivo de la aplicación Kaspersky Endpoint Security for Android

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

Archivos auxiliares

- `sc_package_xx.exe`

  Carpeta comprimida de extracción automática que contiene los archivos necesarios para instalar la aplicación Kaspersky Endpoint Security for 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 for 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 for Android y los contenedores para dispositivos iOS.

Documentación

- Ayuda de Kaspersky Security for Mobile.

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 mediante el uso de los siguientes componentes:

- **Aplicación Kaspersky Endpoint Security for Android**

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

- **Aplicación Kaspersky Security for iOS**

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

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

  Kaspersky Security for Mobile (Devices) proporciona la interfaz para 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)**

  Kaspersky Security for Mobile (Policies) le permite definir las opciones de configuración para los dispositivos conectados a Kaspersky Security Center mediante el uso de las 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 los dispositivos móviles, así como los equipos cliente y los 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 for Mobile proporciona 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 for 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 for 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 dispositivos móviles de acuerdo con los requisitos 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 for Android y Kaspersky Security for iOS.
- Las notificaciones de administrador sobre el estado y los eventos de las aplicaciones Kaspersky Endpoint Security for Android y Kaspersky Security for iOS pueden comunicarse en Kaspersky Security Center o por correo electrónico.
- Control de cambios de configuración de la directiva (historial de revisiones).

Kaspersky Security for Mobile incluye los siguientes componentes de protección y administración:

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

Acerca de la aplicación Kaspersky Endpoint Security for Android

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

La aplicación Kaspersky Endpoint Security for Android incluye los siguientes componentes:

- **Antivirus**. Este componente detecta y neutraliza amenazas en el dispositivo mediante el uso de 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:
  - **Localización**. Le permite obtener las coordenadas de la ubicación del dispositivo.
  - **Alarma**. Provoque que el dispositivo emita un sonido de alarma fuerte.
  - **Borrado**. 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 "Apuestas, loterías, sorteos" o "Comunicación por Internet").
- **Control de aplicaciones.** Este componente le permite instalar aplicaciones recomendadas y necesarias en el dispositivo por medio de un enlace directo al paquete de distribución o un enlace a Google Play. Control de aplicaciones le permite eliminar las aplicaciones bloqueadas que infringen los requisitos corporativos de seguridad.
- **Control de cumplimiento.** Este componente le permite comprobar si los dispositivos administrados cumplen con los requisitos corporativos de seguridad e imponer restricciones a determinadas funciones de los dispositivos que no los cumplan.

Puede configurar los componentes de la aplicación Kaspersky Endpoint Security for 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 for iOS

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

La aplicación Kaspersky Security for 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 si define los parámetros de las directivas de grupo.
- **Detección de liberación**. Cuando Kaspersky Security for iOS detecta una liberación, muestra un mensaje crítico y le informa sobre el problema.

Acerca del complemento de Kaspersky Security for Mobile (Devices)

Kaspersky Security for Mobile (Devices) proporciona la interfaz para 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 los 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 despliegue".

Acerca del complemento de Kaspersky Security for Mobile (Policies)

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

Requisitos de hardware y software

En esta sección, se enumeran los requisitos de hardware y software para el ordenador del administrador que se usa a fin de instalar el complemento Kaspersky Security for Mobile (Devices) y el complemento 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:

- 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 for Android puede funcionar en los siguientes sistemas EMM de otros fabricantes:

- 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 for Android

Estos son los requisitos de hardware y software de la aplicación Kaspersky Endpoint Security for 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 instala 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 for iOS

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

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

La aplicación Kaspersky Security for iOS tiene los siguientes requisitos de software:

- iOS 14.1 o posterior
- iPadOS 14.1 o posterior

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

Consideraciones y problemas conocidos

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

Problemas conocidos de Kaspersky Security for iOS

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

Problemas conocidos de Kaspersky Endpoint Security for 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 for Android solo se instala en la memoria principal del dispositivo.
- En dispositivos con Android 7.0, puede ocurrir un error al intentar desactivar derechos del administrador para Kaspersky Endpoint Security for Android en la configuración del dispositivo si Kaspersky Endpoint Security for Android tiene prohibido superponerse en otras ventanas. La causa de este problema es un defecto conocido en Android 7.
- Kaspersky Endpoint Security for Android en dispositivos con el sistema operativo Android 7.0 o posterior no admite el modo multiventana.
- Kaspersky Endpoint Security for Android no funciona en dispositivos de Chromebook con sistema operativo de Chrome.
- Kaspersky Endpoint Security for Android no funciona en dispositivos Samsung con sistemas operativos Android (edición Go).
- Al utilizar la aplicación Kaspersky Endpoint Security for Android con sistemas de EMM de terceros (por ejemplo, VMWare AirWatch), solo están disponibles los componentes Antivirus y Protección Web. El administrador puede ajustar la configuración de Antivirus y Protección Web en la consola del sistema de EMM. En este caso, las notificaciones sobre el funcionamiento de la aplicación solo están disponibles en la interfaz de la app Kaspersky Endpoint Security for Android (Informes).

Problemas conocidos al actualizar la versión de la aplicación

- Solo puede actualizar Kaspersky Endpoint Security for Android a la versión más reciente de la aplicación. Kaspersky Endpoint Security for Android no se puede revertir a una versión más antigua.

Problemas conocidos en el funcionamiento del Antivirus

- Debido a limitaciones técnicas, Kaspersky Endpoint Security for 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 en busca de nuevas amenazas cuya información no se haya añadido todavía a las bases de datos antivirus, debe activar el uso de Kaspersky Security Network. *Kaspersky Security Network (KSN)* es una infraestructura de servicios en la nube que proporciona acceso a la base de conocimiento en línea de Kaspersky con información sobre la reputación de los archivos, los recursos web y el 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 algunos dispositivos, Kaspersky Endpoint Security for Android no detecta dispositivos conectados por USB OTG. No es posible ejecutar un análisis antivirus en estos 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 en 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 for Android no detecta la descarga de archivos maliciosos en la memoria del dispositivo. Antivirus puede detectar los archivos maliciosos cuando estos se ejecutan o durante un análisis antivirus del dispositivo. La causa de este problema es un defecto conocido en Android 6.0. Para garantizar la seguridad del dispositivo, se recomienda configurar análisis antivirus planificados.

Problemas conocidos en el funcionamiento de Protección Web

- La Protección web en 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 Protección Web funcione, debe activar el uso de Kaspersky Security Network. Protección Web bloquea los sitios web según los datos de KSN sobre la reputación y la categoría de los sitios web.
- Los sitios web bloqueados pueden permanecer desbloqueados por Protección Web en dispositivos con Android 6.0 con la versión 51 de Google Chrome (o cualquier versión anterior) instalada si el sitio web se abre de las siguientes formas (este problema es causado por un defecto conocido en Google Chrome):
  - Desde los resultados de búsqueda.
  - Desde la lista de marcadores.
  - Desde el historial de búsqueda.

- Mediante la función de autocompletar direcciones web.
- Abriendo el sitio web en una nueva pestaña de Google Chrome.

- Los sitios web bloqueados pueden quedar desbloqueados en la versión de Google Chrome 50 (o cualquier versión anterior) si el sitio web se abrió desde los resultados de búsqueda de Google cuando la función **Combinar pestañas y aplicaciones** está activada en la configuración del navegador. La causa de este problema es un defecto conocido en Google Chrome.
- En Google Chrome, los sitios web bloqueados podrían permanecer desbloqueados si el usuario los abre desde aplicaciones de terceros, por ejemplo, desde una aplicación de cliente de MI. Este problema se debe al modo en que funciona el servicio de Accesibilidad con la función de pestañas personalizadas de Chrome.
- En Samsung Internet Browser, los sitios web bloqueados podrían permanecer desbloqueados si el usuario los abre en segundo plano desde el menú contextual o desde aplicaciones de terceros, por ejemplo, desde una aplicación de cliente de MI.
- Kaspersky Endpoint Security for Android debe estar configurado como función de accesibilidad para garantizar un correcto funcionamiento de Protección web.
- Los sitios web permitidos se pueden bloquear en el Navegador de Samsung en el modo de Protección web **Solo se permiten los sitios web de la lista** cuando la página se actualiza. Los sitios web se bloquean si una expresión regular contiene configuración avanzada (por ejemplo, `^https?:\/\/example\.com\/pictures\/`). Se recomienda usar expresiones regulares sin configuración adicional (por ejemplo, `^https?:\/\/example\.com`).

Problemas conocidos en el funcionamiento del Antirrobo

- Para el envío oportuno de comandos a dispositivos Android, la aplicación utiliza el servicio Firebase Cloud Messaging (FCM). Si FCM no se configura, los comandos se enviarán 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 for Android debe estar configurado como el administrador del dispositivo.
- Para bloquear dispositivos con Android 7.0 o posterior, Kaspersky Endpoint Security for Android debe estar configurado como función de accesibilidad.
- En algunos dispositivos, los comandos de Antirrobo pueden dar un error al ejecutar si el modo de Ahorro de Batería está activado en el dispositivo. Este defecto 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 el funcionamiento del Control de aplicaciones

- Kaspersky Endpoint Security for Android debe estar configurado como función de accesibilidad para garantizar el correcto funcionamiento del Control de aplicaciones.
- Para que el Control de aplicaciones (categorías de apps) funcione, debe activar el uso de Kaspersky Security Network. El Control de aplicaciones determina la categoría de una aplicación según los datos que disponibles en KSN. Para utilizar KSN, el dispositivo móvil debe estar conectado a Internet. Para el Control de aplicaciones, puede añadir aplicaciones individuales a las listas de aplicaciones bloqueadas y permitidas. En este caso, KSN no es necesario.

- Al configurar el Control de aplicaciones, se recomienda desactivar la casilla **Bloquear aplicaciones del sistema**. El bloqueo de aplicaciones del sistema puede causar problemas en el funcionamiento 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 app 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 app 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.

- En dispositivos con Android 7.1.1, si la contraseña de desbloqueo no cumple con los requisitos corporativos de seguridad (Control de cumplimiento), la app del sistema Configuración puede funcionar incorrectamente cuando se intenta cambiar la contraseña de desbloqueo mediante Kaspersky Endpoint Security for Android. La causa de este problema es un defecto conocido en 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 introduce la contraseña de desbloqueo de la pantalla si los datos del dispositivo están cifrados. Este problema está relacionado con funciones específicas del servicio de accesibilidad con firmware MIUI.

Problemas conocidos con la protección ante la eliminación de la app

- Kaspersky Endpoint Security for Android debe estar configurada como el administrador del dispositivo.

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

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

Problemas conocidos al configurar las restricciones del dispositivo

- En dispositivos con Android 10.0 o versiones posteriores, no se admite la prohibición del uso de redes Wi-Fi.

- En dispositivos con Android 10.0 o versiones posteriores, el uso de la cámara no se puede prohibir completamente.

- En los dispositivos con Android 11 o posterior, Kaspersky Endpoint Security for Android debe estar configurado como función de accesibilidad. Kaspersky Endpoint Security for Android solicita al usuario que configure la app como una función de Accesibilidad a través del Asistente de configuración inicial. El usuario puede omitir este paso o desactivar este servicio en la configuración del dispositivo más adelante. 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 for Android primero intenta obtener la ubicación precisa del dispositivo. Si esto no fue posible, se devuelve la ubicación aproximada del dispositivo solo si se ha recibido 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 for Android o añadirla manualmente a la lista de aplicaciones que se inician cuando arranca el sistema operativo. Si la aplicación no está incluida en la lista, Kaspersky Endpoint Security for 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. Solo puede desbloquear el dispositivo usando un código de desbloqueo único.

- En ciertos dispositivos (por ejemplo, Meizu y Asus) con Android 6.0 o posterior, después de cifrar los datos y reiniciar el dispositivo Android, debe introducir una contraseña numérica para desbloquear el dispositivo. Si el usuario utiliza una contraseña gráfica para desbloquear el dispositivo, debe convertir la contraseña gráfica a una contraseña numérica. Para obtener más información sobre la conversión de contraseñas gráficas en contraseñas numéricas, consulte el sitio web del Servicio de soporte técnico del fabricante del dispositivo móvil. Este problema está relacionado con el funcionamiento del servicio Funciones de accesibilidad.

- En algunos dispositivos Huawei con el sistema operativo Android 5.X, después de configurar Kaspersky Endpoint Security for Android como función de accesibilidad, se muestra un mensaje incorrecto sobre la falta de los derechos correspondientes. Para esconder este mensaje, active la aplicación como aplicación protegida en la configuración del dispositivo.

- En algunos dispositivos de Huawei con Android 5.X o 6.X, cuando el modo del Ahorro de Batería se activa para Kaspersky Endpoint Security for 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 for Android manualmente. Se recomienda desactivar el modo de Ahorro de batería para Kaspersky Endpoint Security for Android en la configuración del dispositivo.

- En dispositivos Huawei con firmware EMUI que ejecutan Android 7.0, el usuario puede ocultar la notificación relativa al estado de la protección de Kaspersky Endpoint Security for Android. Este problema se debe a algunas características del software de Huawei.

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

- En dispositivos Xiaomi con firmware MIUI que ejecuta Android 6.0, el icono de Kaspersky Endpoint Security for Android se puede ocultar 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 for Android. Este problema ocurre debido a un defecto conocido en el parche de seguridad para Android de Google. Para asegurar el buen funcionamiento, los privilegios requeridos se deben conceder manualmente en la configuración del dispositivo.

- En ciertos dispositivos de Samsung que ejecutan Android 7.0 o posterior, cuando el usuario intenta configurar métodos no admitidos para desbloquear el dispositivo (por ejemplo, una contraseña gráfica), el dispositivo se puede bloquear si las condiciones siguientes se cumplen: la protección de eliminación de Kaspersky Endpoint

Security for Android está activada y se cumplen los requisitos de seguridad de la contraseña de desbloqueo de pantalla. Para desbloquear el dispositivo, debe enviar un comando especial al dispositivo.

- En ciertos dispositivos de Samsung no es posible bloquear el uso de huellas digitales para desbloquear la pantalla.
- La Protección web no puede activarse en algunos dispositivos Samsung si el dispositivo está conectado a una red 3G/4G, tiene activado 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 de Samsung, si la contraseña de desbloqueo no cumple con los requisitos corporativos de seguridad, Kaspersky Endpoint Security for Android no bloquea el uso de huellas digitales para desbloquear la pantalla.
- En algunos dispositivos Honor y Huawei, no puede restringir el uso de Bluetooth. Cuando Kaspersky Endpoint Security for Android intenta restringir el uso de Bluetooth, el sistema operativo muestra una notificación con las opciones para rechazar o permitir la restricción. El usuario puede rechazar esta restricción y continuar usando Bluetooth.
- En los dispositivos Blackview, el usuario puede borrar la memoria de la aplicación Kaspersky Endpoint Security for Android. Como consecuencia, la protección y la administración del dispositivo se desactivan, todas las configuraciones definidas se vuelven ineficaces y la aplicación Kaspersky Endpoint Security for 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 for Android, y no se puede reemplazar porque es parte del sistema operativo Android.
- En algunos dispositivos que ejecutan Android 11, la aplicación Kaspersky Endpoint Security for Android se bloquea inmediatamente después del inicio. La causa de este problema es un defecto conocido en Android 11.

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

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

Escenarios de despliegue

Despliegue en Kaspersky Security Center Web Console

El despliegue 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 el despliegue
2. Despliegue de complementos de administración
3. Despliegue 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.

Despliegue en Kaspersky Security Center Cloud Console

El despliegue 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 el despliegue
2. Despliegue 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 el despliegue

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

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 for Android o Kaspersky Security for 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. Active el botón **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 **Abrir puerto para dispositivos móviles** está desactivado o se ha seleccionado 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 uso del 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 la instalación del Servidor de administración. Si lo desea, reemplace el certificado emitido a través del Servidor de administración por otro certificado o vuelva a emitir el certificado que se generó mediante el Servidor de administración.

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

a. Seleccione la sección **Certificados**.

b. Defina la configuración necesaria.

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 que ha realizado en la configuración y salir de la ventana de propiedades del Servidor de administración.

Después de configurar la conexión del dispositivo móvil, puede instalar la aplicación Kaspersky Endpoint Security for Android o Kaspersky Security for 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 for Android y Kaspersky Security for 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 asignación automática de dispositivos en los que instalar las aplicaciones para este grupo. A continuación, configure los parámetros que son comunes para todos los dispositivos utilizando una directiva de grupo.

Para crear un grupo de administración:

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 **Añadir**.

4. En la ventana **Nombre del nuevo grupo de administración** que se abre, introduzca un nombre para el grupo y, a continuación, haga clic en el botón **Añadir**.

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 for Android o Kaspersky Security for iOS está instalada en los dispositivos móviles, se muestran en la página **DESCUBRIMIENTO Y DESPLIEGUE** > **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 Y DESPLIEGUE** > **DESPLIEGUE 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 **Activar regla** para aplicar la regla inmediatamente después de crearla.

   Puede activar la regla en cualquier momento posterior mediante el uso del botón en la página **REGLAS DE MOVIMIENTO**.

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

   a. Active el botón **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*.

Despliegue 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 está utilizando 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 en cualquier momento el Asistente de inicio rápido de forma manual.

  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 del lanzamiento de nuevas versiones de las aplicaciones de 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 de paquetes de distribución disponibles

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 **Añadir**.

   Se abre la lista de versiones actualizadas de las aplicaciones de 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 instala y se agrega 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 **Añadir**.

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

Para 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 **Añadir**.

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

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

Despliegue de la aplicación móvil

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

Despliegue de la aplicación móvil mediante el uso de Kaspersky Security Center Web Console o Cloud Console

La aplicación móvil se despliega en los dispositivos móviles de los usuarios que tienen cuentas de usuario añadidas en Kaspersky Security Center. Para obtener más información sobre las cuentas de usuario en Kaspersky Security Center:

- 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) para 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 for Android. La aplicación puede instalarse a través del procedimiento de instalación estándar en la plataforma Android. Después de instalar la aplicación, el usuario debe proporcionar los permisos necesarios.

  Algunos dispositivos Huawei y Honor no tienen servicios de Google y, por lo tanto, no tienen acceso a las aplicaciones de Google Play. Si algunos usuarios de los dispositivos Huawei y Honor no pueden instalar la aplicación desde Google Play, se les debe indicar que instalen la aplicación desde Huawei App Gallery.

- En un dispositivo iOS, el usuario recibe un enlace de App Store para descargar la aplicación Kaspersky Security for iOS. La aplicación puede instalarse a través del 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 mientras se instale la aplicación y podrá cancelar la conexión si la dirección que se muestra no coincide con la dirección que usted envió.

El enlace incluye los siguientes datos:

- Configuración de sincronización de Kaspersky Security Center
- Certificado general

Para desplegar 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 **Añadir**.
   - 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 **Añadir dispositivo móvil**. En este caso, omita el paso 3.

   Para continuar con el asistente, utilice el botón **Siguiente**.
2. Elija el sistema operativo de los dispositivos que desea añadir:
   - **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. Elija direcciones de correo electrónico para enviar el vínculo:
   - **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 una confirmación de que se ha enviado el enlace para añadir un dispositivo móvil.

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

Cuando el usuario instala la aplicación Kaspersky Endpoint Security for Android o Kaspersky Security for 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 los datos en caso de extravío o robo 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 for Android o Kaspersky Security for 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 de la **Administración de dispositivos móviles** es conectar dispositivos móviles con Kaspersky Security Center y administrarlos.

Para obtener información detallada sobre cómo obtener la licencia de Kaspersky Security Center y las opciones de licencias*:*

- 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 for Android o Kaspersky Security for iOS en un dispositivo móvil se realiza proporcionando información de licencia válida a la aplicación. Se proporciona información sobre la licencia al dispositivo móvil junto con la directiva cuando el dispositivo se sincroniza 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 tendrá que sincronizar manualmente el dispositivo y Kaspersky Security Center.

Si Kaspersky Security Center no está desplegado 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 de 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 desea configurar.
   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.
2. En la página de 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 que ha realizado en la directiva y salir de la ventana de 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 for Android

Ciertas funciones de la aplicación Kaspersky Endpoint Security for Android requieren permisos. Kaspersky Endpoint Security for 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 for Android sin proporcionar los permisos obligatorios.

En ciertos dispositivos (por ejemplo, Huawei, Meizu y Xiaomi), en la configuración del dispositivo debe añadir manualmente Kaspersky Endpoint Security for Android a la lista de aplicaciones que se inician cuando arranca el sistema operativo. Si la aplicación no está incluida en la lista, Kaspersky Endpoint Security for Android deja de realizar todas sus funciones después de que el dispositivo móvil se reinicia.

En dispositivos con Android 11 o versiones posteriores, debe desactivar 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 for Android

Permiso	Función de la aplicación
Teléfono (obligatorio 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: toma 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 for 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 aplicaciones
	Restricción del uso de la cámara, Bluetooth y Wi-Fi
Cámara	Antirrobo: toma 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 for 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 conceder el permiso "Mientras se usa la aplicación" cuando se lo pida.
Ubicación	Antirrobo: localización del dispositivo En los dispositivos con Android 10.0 o posterior, el usuario debe conceder el permiso "Todo el tiempo" cuando se le solicite.
Accesibilidad	Antirrobo: bloqueo del dispositivo (solo para Android 7.0 y versiones posteriores)
	Protección web
	Control de aplicaciones
	Protección de eliminación de aplicaciones (solo para Android 7.0 y versiones posteriores)
	Visualización de advertencias de Kaspersky Endpoint Security for Android (solo para Android 10.0 y 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 le 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:

- 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 le permiten ver los certificados móviles de usuario aplicados, sus estados y propiedades.

Para ver la lista de los certificados móviles de usuario aplicados:

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** que contiene información sobre los certificados móviles de usuario aplicados. Puede ver los detalles de un certificado haciendo 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 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 desactivada, los certificados se deben volver a emitir manualmente a medida que caducan. De forma predeterminada, esta opción está desactivada.

- **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 ventana emergente **Certificados móviles**, haga clic en **Añadir** para iniciar el **Asistente de creación de certificado móvil**. Para continuar con el asistente, utilice el botón **Siguiente**.

4. Seleccione los usuarios o los 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 for 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 for 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 for 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 después de finalizar el Asistente**.

   - Si ha seleccionado **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:

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 ha reemitido**.

Eliminación de un certificado

Puede eliminar los 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, tendrá que reinstalar la aplicación Kaspersky Endpoint Security for Android en este.

Para eliminar un certificado móvil:

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 for Android utiliza el servicio Firebase Cloud Messaging (FCM) para garantizar la entrega oportuna de comandos a los dispositivos móviles y la sincronización forzada cuando se cambia la configuración de la directiva.

Para utilizar el servicio Firebase Cloud Messaging, debe ajustar la configuración del servicio en Kaspersky Security Center Web Console o Cloud Console.

Para activar Firebase Cloud Messaging en Kaspersky Security Center Web Console o Cloud Console:

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 activado.

Para obtener un ID del remitente y la Clave del servidor:

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. Active Google Firebase Cloud Messaging for Android.

6. Siga las instrucciones en pantalla para crear credenciales.

7. Recupera 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 la configuración de Firebase Cloud Messaging no se ajusta, los comandos del dispositivo móvil y la configuración de directiva se entregarán cuando el dispositivo se sincronice con Kaspersky Security Center según la planificación establecida en la directiva (por ejemplo, cada 24 horas). En otras palabras, los comandos y la configuración de directiva se entregarán con retraso.

Con el fin de admitir la funcionalidad principal del producto, usted acepta proporcionar automáticamente al servicio Firebase Cloud Messaging el ID único de la instalación de la aplicación (ID de instancia) y los siguientes datos:

- Información sobre el software instalado: versión de la aplicación, ID de la aplicación, versión de compilación de la aplicación, nombre del paquete de la aplicación.
- Información sobre el equipo en el que está instalado el software: versión del sistema operativo, ID del dispositivo, versión de los servicios de Google.
- Información sobre FCM: ID de la aplicación en FCM, ID de usuario en FCM, versión de protocolo.

Los datos se transmiten a los servicios de Firebase a través de una conexión segura. El acceso y la protección de la información se rigen conforme a las pertinentes condiciones de uso del servicio 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 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 de comandos a dispositivos móviles (solo para Android).

Para administrar los 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 mediante el uso de 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 mientras se instale 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 **Añadir**.

   - 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 **Añadir dispositivo móvil**. En este caso, omita el paso 3.

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

2. Elija el sistema operativo de los dispositivos que desea añadir:

   - **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. Elija direcciones de correo electrónico para enviar el vínculo:

   - **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 una confirmación de que se ha enviado el enlace para añadir un dispositivo móvil.

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

Cuando el usuario instala la aplicación Kaspersky Endpoint Security for Android o Kaspersky Security for 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 for Android o Kaspersky Security for iOS está instalada en los dispositivos móviles, se muestran en la página **DESCUBRIMIENTO Y DESPLIEGUE** > **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 Y DESPLIEGUE** > **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 de grupos de administración emergente, 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 bloqueará.

- **Desbloquear dispositivo**

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, no se modifica la contraseña de desbloqueo de pantalla.

- **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 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 for Android primero intenta obtener la ubicación precisa del dispositivo. Si esto no fue posible, se devuelve la ubicación aproximada del dispositivo solo si se ha recibido no más de 30 minutos antes. De lo contrario, el comando **Localizar dispositivo** falla.

- **Activar alarma**

  El dispositivo móvil emite 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 for Android requiere permisos específicos para ejecutar los comandos. Cuando el Asistente de configuración inicial se está ejecutando, Kaspersky Endpoint Security for 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, no será posible ejecutar comandos.

En los dispositivos con Android 10.0 o posterior, el usuario debe conceder el permiso "Todo el tiempo" para acceder a la ubicación. En los dispositivos con Android 11.0 o posterior, el usuario también debe conceder 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 las directivas de grupo en Kaspersky Security Center Web Console y Cloud Console.

Directivas de grupo para administrar dispositivos móviles

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

Puede usar una directiva para establecer la configuración tanto de dispositivos particulares como de un grupo de dispositivos. En el caso de un grupo de dispositivos, la configuración de administración puede definirse en la ventana de propiedades de la directiva de grupo.

Cada parámetro que se representa en una directiva tiene un atributo de bloqueo que indica si tal ajuste permite modificarse en las directivas de los niveles de jerarquía anidados (para grupos anidados y Servidores de administración secundarios) en la configuración de la aplicación local.

Los valores de la configuración establecida en la configuración de directiva y de la aplicación local se guardan en el Servidor de Administración, se aplican a los dispositivos móviles durante la sincronización y se guardan en los dispositivos como las configuraciones actuales. Si el usuario ha especificado otros valores de configuración que no se han bloqueado, en la siguiente sincronización del dispositivo con el Servidor de Administración, son los nuevos valores de configuración los que se transmiten al Servidor de Administración y se guardan en la configuración local de la aplicación, y no aquellos valores que había especificado previamente el administrador.

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 información breve 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 haciendo clic en el botón **Configurar directiva**.

Creación de una directiva de grupo

Kaspersky Security Center Web Console y Cloud Console le permiten crear directivas de grupo con el fin de administrar los 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 aplica al grupo de **dispositivos administrados**.

3. Haga clic en **Añadir** 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 for Android**
   - **Kaspersky Security for iOS**

5. Escriba el nombre de la nueva directiva en el campo **Nombre**. Si especifica el nombre de una directiva existente, se agregará (1) al final automáticamente.

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 utilizará en el dispositivo como directiva activa.

   - **Inactiva**

     El asistente guarda la directiva creada en el Servidor de Administración como directiva de copia de seguridad. Esta directiva podrá activarse en el futuro tras un determinado evento. Si fuera necesario, una directiva inactiva se puede activar.

     Pueden crearse varias directivas para una aplicación en el grupo, pero solo una de ellas puede estar activa. Al crearse una directiva activa, se desactiva automáticamente la que estaba activa previamente.

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

   - Si activa **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 desactiva **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 activa **Forzar la herencia de la configuración en las directivas secundarias** en el grupo de administración principal, esto habilita la opción **Heredar la configuración de la directiva principal** para cada directiva secundaria. En este caso, no puede desactivar 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 activada y la opción **Forzar la herencia de la configuración en las directivas secundarias** está desactivada.

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 la administración de 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 de 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 desea configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione 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 que ha realizado en la directiva y salir de la ventana de 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 añade 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 añade 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.

Solo puede eliminar 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 de directivas de grupo emergente, 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

Esta sección describe cómo definir la configuración de las directivas de Kaspersky Security Center para administrar dispositivos móviles.

Puede definir la configuración de la 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 for Android detecta los siguientes tipos de objetos:

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

Debido a limitaciones técnicas, Kaspersky Endpoint Security for Android no puede analizar archivos con un tamaño de 2 GB o más. Durante un análisis, la aplicación omite los archivos de gran tamaño sin notificar la omisión.

Configuración de la protección en tiempo real

Puede definir estos parámetros de directivas solo para dispositivos Android.

Para configurar la protección en tiempo real:

1. Abra la ventana de 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 desea configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione 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** > **Protección básica**.

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

   - Para activar la protección en tiempo real del dispositivo móvil contra amenazas, seleccione la casilla **Activar la protección antivirus en tiempo real**.

   - Especifique el nivel de protección:

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

     - Para activar la protección ampliada del dispositivo móvil contra amenazas, seleccione **Analizar todas las aplicaciones y supervisar las acciones con archivos**.

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

       En dispositivos con Android 8.0 o posterior, Kaspersky Endpoint Security for Android analiza archivos que el usuario modifica, mueve, instala y guarda, así como copias de archivos. Kaspersky Endpoint Security for Android no analiza archivos cuando están abiertos, o archivos de origen cuando se copian.

   - Para activar el análisis adicional de nuevas aplicaciones antes de iniciarlas por primera vez en el dispositivo del usuario con la ayuda del servicio en la nube de Kaspersky Security Network, seleccione la casilla **Protección adicional de Kaspersky Security Network**.

   - Para bloquear el software publicitario y las aplicaciones que pueden utilizar 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 debe llevarse a cabo al detectar una amenaza:

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

     Los objetos detectados se eliminarán automáticamente. No se requiere ninguna otra acción del usuario. Antes de eliminar un objeto, Kaspersky Endpoint Security for Android creará una copia de seguridad del archivo y lo guardará en cuarentena.

   - **Eliminar**

     Los objetos detectados se eliminarán automáticamente. No se requiere ninguna otra acción del usuario. Antes de eliminar un objeto, Kaspersky Endpoint Security for Android mostrará una notificación temporal sobre la detección del objeto.

   - **Omitir**

     Si los objetos detectados se han omitido, Kaspersky Endpoint Security for Android advierte al usuario sobre problemas en la protección del dispositivo. Puede ver más información sobre los objetos omitidos en la sección **Estado** de la aplicación. Para cada amenaza omitida, la app proporciona acciones que el usuario puede realizar para eliminar la amenaza. La lista de objetos omitidos puede cambiar, por ejemplo, si un archivo malicioso se elimina o se mueve. Para recibir una lista actualizada de amenazas, ejecute un análisis completo del dispositivo. Para asegurarse de que sus datos siguen estando protegidos, elimine todos los objetos detectados.

5. Haga clic en el botón **Guardar** para guardar los cambios que ha realizado en la directiva y salir de la ventana de 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 un dispositivo móvil

Puede definir estos parámetros de directivas solo para dispositivos Android.

Para configurar la ejecución automática de análisis antivirus en un dispositivo móvil:

1. Abra la ventana de 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 desea configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione 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** > **Protección básica**.

3. Para bloquear el software publicitario y las aplicaciones que pueden utilizar los 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. No se requiere ninguna otra acción del usuario. Antes de eliminar un objeto, Kaspersky Endpoint Security for Android creará una copia de seguridad del archivo y lo guardará en cuarentena.

   - **Eliminar**

     Los objetos detectados se eliminarán automáticamente. No se requiere ninguna otra acción del usuario. Antes de eliminar un objeto, Kaspersky Endpoint Security for Android mostrará una notificación temporal sobre la detección del objeto.

   - **Omitir**

     Si los objetos detectados se han omitido, Kaspersky Endpoint Security for Android advierte al usuario sobre problemas en la protección del dispositivo. Puede ver más información sobre los objetos omitidos en la sección **Estado** de la aplicación. Para cada amenaza omitida, la app proporciona acciones que el usuario puede realizar para eliminar la amenaza. La lista de objetos omitidos puede cambiar, por ejemplo, si un archivo malicioso se elimina o se mueve. Para recibir una lista actualizada de amenazas, ejecute un análisis completo del dispositivo. Para asegurarse de que sus datos siguen estando protegidos, elimine todos los objetos detectados.

   - **Preguntar al usuario**

     La app Kaspersky Endpoint Security for Android muestra una notificación que solicita al usuario que elija la acción que debe llevarse a cabo con el objeto detectado: **Omitir** o **Eliminar**.

     Cuando la aplicación detecta varios objetos, 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 for Android debe estar configurado como función de accesibilidad para garantizar la visualización de las notificaciones en dispositivos móviles con Android 10.0 o versiones posteriores. Kaspersky Endpoint Security for Android solicita al usuario que configure la app como una función de Accesibilidad a través del Asistente de configuración inicial. El usuario puede omitir este paso o desactivar este servicio en la configuración del dispositivo más adelante. En este caso, Kaspersky Endpoint Security for Android muestra una ventana del sistema Android que solicita al usuario elegir la acción que debe llevarse a cabo 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 automático del sistema de archivos del dispositivo.

   Seleccione una de las siguientes opciones:

   - **Desactivado**

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

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

     El sistema de archivos del dispositivo se analizará automáticamente cada vez que se actualice la base de datos antivirus.

- **Diariamente**

  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 a la semana.

  Si selecciona esta opción, también puede seleccionar el día de la semana en el que desea ejecutar el análisis en la lista desplegable y especificar la hora del análisis en el campo **Hora de inicio**.

En Android 12 o versiones posteriores, 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 que ha realizado en la directiva y salir de la ventana de 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 bases de datos antivirus

Puede definir estos parámetros de directivas solo para dispositivos Android.

Para configurar las actualizaciones de la base de datos antivirus:

1. Abra la ventana de 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 desea configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione 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** > **Actualizar base de datos**.

3. En la sección **Actualizar base de datos**, configure la programación de actualizaciones automáticas de las bases de datos en el dispositivo del usuario.

   Seleccione una de las siguientes opciones:

   - **Desactivado**

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

   - **Diariamente**

     Las bases de datos antivirus se actualizarán todos los días.

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

- **Semanalmente**

  Las bases de datos antivirus se actualizarán una vez a la semana.

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

En Android 12 o versiones posteriores, 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 la actualización de las bases de datos**, especifique el origen de las actualizaciones desde el cual Kaspersky Endpoint Security for Android recibirá e instalará las actualizaciones de las bases de datos antivirus:

   - **Servidores de Kaspersky**

     Kaspersky Endpoint Security for Android utilizará un servidor de actualización de Kaspersky como origen de actualizaciones para descargar bases de datos antivirus en el dispositivo del usuario.

   - **Servidor de administración**

     Disponible solo si usa Kaspersky Security Center Web Console.

     Kaspersky Endpoint Security for Android utilizará el repositorio del Servidor de Administración de Kaspersky Security Center como origen de actualizaciones para descargar bases de datos antivirus en el dispositivo del usuario.

   - **Otro origen**

     Kaspersky Endpoint Security for Android utilizará un servidor de terceros como origen de actualizaciones para descargar 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 actualizaciones para las bases de datos antivirus**.

5. Si desea que Kaspersky Endpoint Security for Android descargue actualizaciones de la base de datos de acuerdo con la programación de las actualizaciones cuando el dispositivo esté en itinerancia, seleccione la casilla **Permitir actualización de las bases de datos en itinerancia** en la sección **Actualizar las bases de datos antivirus durante itinerancia**.

6. Haga clic en el botón **Guardar** para guardar los cambios que ha realizado en la directiva y salir de la ventana de 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 protegido un dispositivo móvil, debe configurar el uso de una contraseña que el usuario debe proporcionar cuando el dispositivo sale del modo de suspensión.

Puede imponer restricciones a la actividad del usuario en el dispositivo si la contraseña de desbloqueo no es segura (por ejemplo, bloquear el dispositivo). Puede imponer restricciones con el componente Control de cumplimiento.

En ciertos dispositivos de Samsung que ejecutan 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 las condiciones siguientes se cumplen: la protección de eliminación de Kaspersky Endpoint Security for Android está activada y se cumplen los requisitos de seguridad de la contraseña de desbloqueo de pantalla. Para desbloquear el dispositivo, debe enviar un comando especial al dispositivo.

Para configurar la seguridad de la contraseña de desbloqueo de dispositivos:

1. Abra la ventana de 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 desea configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione 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** > **Protección básica**.

3. Si desea que la aplicación compruebe si se ha establecido una contraseña de desbloqueo, seleccione la casilla **Requerir 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 definidos por el administrador.

4. Especifique el número mínimo de caracteres que debe tener 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 versiones posteriores se determinan en base a las siguientes reglas:

   - Si la extensión de la contraseña requerida es de 1 a 4 símbolos, la app solicitará que el usuario establezca una contraseña con seguridad media. Debe ser numérica (PIN) con una secuencia que no tenga números repetidos ni 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 app solicitará que el usuario establezca una contraseña con seguridad alta. Debe ser numérica (PIN) con una secuencia que no tenga números repetidos ni 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 tenga la capacidad de usar huellas digitales para desbloquear la pantalla, seleccione la casilla **Permitir el uso de huellas digitales (para dispositivos con Android 9 o anterior)**. Si la contraseña de desbloqueo no cumple con los requisitos corporativos de seguridad, no se puede usar un escáner de huellas digitales para desbloquear la pantalla.

   En dispositivos con Android 10.0 o versiones posteriores, no se admite el uso de huellas digitales para desbloquear la pantalla.

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

   En ciertos dispositivos de Samsung no es posible bloquear el uso de huellas digitales para desbloquear la pantalla.

   En ciertos dispositivos de Samsung, si la contraseña de desbloqueo no cumple con los requisitos corporativos de seguridad, Kaspersky Endpoint Security for 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 con los siguientes métodos:

   - Presione el dedo en el escáner de huella digital (método principal).
   - Introduzca la contraseña de desbloqueo (método de reserva).

6. Haga clic en el botón **Guardar** para guardar los cambios que ha realizado en la directiva y salir de la ventana de 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 extraviados

Puede definir estos parámetros de directivas solo para dispositivos Android.

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

Para garantizar la protección de los datos de dispositivos robados o extraviados, Kaspersky Endpoint Security for Android debe configurarse como una función de accesibilidad. Kaspersky Endpoint Security for Android solicita al usuario que configure la app como una función de Accesibilidad a través del Asistente de configuración inicial. El usuario puede omitir este paso o desactivar este servicio en la configuración del dispositivo más adelante.

Para configurar la protección de los datos de dispositivos robados o extraviados:

1. Abra la ventana de 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 desea configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione 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** > **Protección básica**.

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

   - Especifique el número de caracteres del código de desbloqueo.

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

4. Haga clic en el botón **Guardar** para guardar los cambios que ha realizado en la directiva y salir de la ventana de 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 aplicaciones

Puede definir estos parámetros de directivas solo para dispositivos Android.

Control de aplicaciones 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 aplicaciones permitidas, bloqueadas, obligatorias y recomendadas según los requisitos corporativos de seguridad. Debido al Control de aplicaciones, Kaspersky Endpoint Security solicita al usuario instalar las aplicaciones obligatorias y recomendadas, además de eliminar las aplicaciones bloqueadas. Es imposible iniciar aplicaciones bloqueadas en el dispositivo móvil del usuario.

En Kaspersky Security Center Web Console y Cloud Console, puede administrar aplicaciones en los dispositivos de los usuarios aplicando reglas predefinidas. Puede configurar dos tipos de reglas de **Control de aplicaciones**: reglas de aplicación 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 se encargan de especificar las categorías de apps.

*Para configurar **Control de aplicaciones**:*

1. Abra la ventana de 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 desea configurar.

- En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

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

3. En la tabla ubicada debajo de la sección **Control de aplicaciones**, añada reglas para definir las aplicaciones que se controlarán.

   - Para añadir una regla para una aplicación específica:

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

     b. En la ventana **Regla de la aplicación** que se abre, elija la acción que se llevará a cabo con las aplicaciones comprendidas por la regla creada.

     c. Especifique la aplicación que estará sujeta a la regla completando el **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 añade a la lista de reglas de **Control de aplicaciones**.

   - Para añadir una regla para una categoría de aplicaciones:

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

     b. En la ventana **Regla de categoría** que se abre, seleccione la categoría de la aplicación en la lista desplegable.

     Las aplicaciones dentro de la categoría seleccionada estarán sujetas a la regla creada.

     c. En la sección **Modo de funcionamiento**, seleccione la acción que se realizará al intentar iniciar cualquier aplicación dentro de la categoría seleccionada: **Aplicaciones bloqueadas** o **Aplicaciones permitidas**.

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

     e. Haga clic en **Guardar**.

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

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

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

   - Si desea que Kaspersky Endpoint Security for 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 funcionamiento**, elija si las reglas que añade definirán aplicaciones permitidas o bloqueadas:

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

     Si desea que Kaspersky Endpoint Security for Android impida el inicio de las aplicaciones del sistema en el dispositivo móvil del usuario (como Calendario, Cámara y Ajustes), en el modo **Aplicaciones bloqueadas**, seleccione la casilla **Bloquear aplicaciones del sistema**.

     > Los expertos de Kaspersky recomiendan no usar aplicaciones del 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 dispositivos móviles, en la sección **Informe de aplicaciones**, seleccione la casilla **Enviar una lista de apps instaladas en todos los dispositivos móviles**.

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

7. Haga clic en el botón **Guardar** para guardar los cambios que ha realizado en la directiva y salir de la ventana de 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 corporativos de seguridad

> Puede definir estos parámetros de directivas solo para dispositivos Android.

El Control de cumplimiento le permite supervisar los dispositivos Android para verificar el cumplimiento de los requisitos corporativos de seguridad y tomar acciones en caso de incumplimiento. Los requisitos corporativos de seguridad regulan la utilización del dispositivo por parte del usuario. 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 suficientemente segura. El control de cumplimiento se basa en una lista de reglas. Una regla de cumplimiento incluye los componentes siguientes:

- Criterio de incumplimiento del dispositivo.
- Acción que se tomará en el dispositivo si el usuario no resuelve el incumplimiento en el período asignado.
- Período de tiempo asignado para que el usuario resuelva el incumplimiento (por ejemplo, 24 horas).

  Cuando finalice el período especificado, se llevará a cabo la acción seleccionada en el dispositivo del usuario.

  > En Android 12 o versiones posteriores, 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:

- Active o desactive las reglas de cumplimiento existentes.
- Edite una regla de cumplimiento existente.
- Añada una nueva regla.
- Elimine una regla.

Cómo activar y desactivar las reglas de cumplimiento

Puede definir estos parámetros de directivas solo para dispositivos Android.

Para activar o desactivar las reglas existentes de control de cumplimiento de dispositivos móviles con requisitos corporativos de seguridad:

1. Abra la ventana de 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 desea configurar.
   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.
2. En la página de propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Controles de seguridad**.
3. En la sección **Control de cumplimiento**, active o desactive las reglas de cumplimiento existentes con los botones en la columna **Estado**.
4. Haga clic en el botón **Guardar** para guardar los cambios que ha realizado en la directiva y salir de la ventana de propiedades de la directiva.

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

Cómo editar reglas de cumplimiento

Puede definir estos parámetros de directivas solo para dispositivos Android.

Si desea editar una regla para controlar el cumplimiento de los dispositivos móviles con los requisitos corporativos de seguridad:

1. Abra la ventana de 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 desea configurar.

- En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

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

3. En la sección **Control de cumplimiento**, seleccione la regla que desea editar y, a continuación, haga clic en **Editar**.

4. En la ventana **Regla** que se abre, edite la regla de la siguiente manera:

   a. En la columna **Acción**, configure la lista de acciones a realizar en caso de incumplimiento de la regla añadiendo nuevas acciones, editando las acciones existentes o eliminándolas.

   b. Opcionalmente, especifique el período en el que un usuario puede corregir el incumplimiento en la columna **Tiempo de 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 que ha realizado en la directiva y salir de la ventana de propiedades de la directiva.

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

Cómo añadir reglas de cumplimiento

Puede definir estos parámetros de directivas solo para dispositivos Android.

Si desea añadir una regla para controlar el cumplimiento de los dispositivos móviles con los requisitos corporativos de seguridad:

1. Abra la ventana de 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 desea configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la página de 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 **Regla** que se abre, defina la regla de la siguiente manera:

   a. Seleccione el criterio de incumplimiento de la regla.

   b. Haga clic en **Añadir** y, a continuación, seleccione la acción que se realizará en caso de incumplimiento de la regla en la columna **Acción**.

   Puede añadir varias acciones.

   c. Especifique el período en el que un usuario puede corregir el incumplimiento en la columna **Tiempo de 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 que ha realizado en la directiva y salir de la ventana de propiedades de la directiva.

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

Cómo eliminar reglas de cumplimiento

Puede definir estos parámetros de directivas solo para dispositivos Android.

Si desea eliminar una regla para controlar el cumplimiento de los dispositivos móviles con los requisitos corporativos de seguridad:

1. Abra la ventana de 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 desea configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

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

3. En la sección **Control de cumplimiento**, seleccione la regla que desea eliminar y, a continuación, haga clic en **Eliminar**.

4. Haga clic en el botón **Guardar** para guardar los cambios que ha realizado en la directiva y salir de la ventana de 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 corporativos de seguridad, Kaspersky Endpoint Security for Android puede verificar el dispositivo con los siguientes criterios:

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

  Debe activarse la protección en tiempo real.

  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**.

  La base de datos antivirus de Kaspersky Endpoint Security for Android debe actualizarse periódicamente.

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

- **Hay aplicaciones bloqueadas instaladas**.

  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 aplicaciones".

- **Hay aplicaciones de categorías bloqueadas instaladas**.

  El dispositivo no debe tener aplicaciones instaladas que pertenezcan a 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 aplicaciones".

- **No se han instalado todas las aplicaciones necesarias**.

  El dispositivo debe tener instaladas aplicaciones específicas 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 aplicaciones".

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

  El dispositivo debe tener una versión permitida del sistema operativo.

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

- **Hace mucho tiempo que no se ha sincronizado el dispositivo**.

  El dispositivo debe sincronizarse periódicamente con el Servidor de administración.

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

- **El dispositivo ha sido rooteado**.

  El dispositivo no debe estar rooteado.

Para obtener más información, consulte la sección "Detección de pirateos del dispositivo (acceso root)".

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

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

Lista de acciones en caso de incumplimiento

Puede definir estos parámetros de directivas solo para dispositivos Android.

Si el usuario no soluciona el incumplimiento en el plazo especificado, las siguientes acciones están disponibles:

- **Bloquear todas las aplicaciones excepto las aplicaciones 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 el motivo para bloquear el dispositivo no se rectifica después de desbloquear el dispositivo, este se bloqueará de nuevo después del plazo 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 la VPN corporativas, y el nombre del punto de acceso (APN).

- **Realizar restablecimiento completo del dispositivo a la configuración de fábrica**.

  Se eliminan todos los datos del dispositivo móvil y se restablecen los valores de fábrica de la configuración.

Configuración del acceso del usuario 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, luego, bloquea los sitios web que distribuyen códigos maliciosos y los sitios web de phishing diseñados para robar datos confidenciales y acceder 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 le permite restringir el acceso a determinados sitios web o categorías de sitios web (por ejemplo, páginas web con las categorías "**Apuestas, loterías, sorteos**" o "**Comunicación por Internet**").

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

Para garantizar el funcionamiento correcto de la Protección web, Kaspersky Endpoint Security for Android debe configurarse como una función de accesibilidad. Kaspersky Endpoint Security for Android solicita al usuario que configure la app como una función de Accesibilidad a través del Asistente de configuración inicial. El usuario puede omitir este paso o desactivar este servicio en la configuración del dispositivo más adelante.

En dispositivos iOS, el usuario debe permitir que la aplicación Kaspersky Security for iOS añada una configuración de VPN para que Protección web funcione.

Para configurar el acceso de los usuarios a sitios web:

1. Abra la ventana de 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 desea configurar.
   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.
2. En la página de propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **Controles de seguridad**.
3. En la sección **Protección web**, seleccione la casilla **Activar Protección web** para activar la función.
4. Para dispositivos Android, puede seleccionar una de las siguientes opciones:
   - Para restringir el acceso de los usuarios a sitios web en función de su contenido:
     a. Seleccione **Bloquear sitios web de categorías especificadas**.
     b. Seleccione las casillas ubicadas junto a las categorías de sitios web a las que Kaspersky Endpoint Security for Android bloqueará el acceso.

     Si la Protección web está activada, el acceso de los usuarios a los sitios web de las categorías **Suplantación de identidad** y **Sitios de malware** siempre está bloqueado.
   - Para especificar la lista de sitios web permitidos:
     a. Seleccione **Permitir solo los sitios web especificados**.
     b. Cree una lista de sitios web añadiendo direcciones de sitios web a los que la aplicación no bloqueará el acceso. Kaspersky Endpoint Security for Android solo admite expresiones regulares. Al escribir la dirección de un sitio web permitido, utilice las siguientes plantillas:
        - `http:\/\/www\.example\.com.*`: Se permiten todas las páginas secundarias del sitio web (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 los protocolos 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 que ha realizado en la directiva y salir de la ventana de 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 de las funciones

Puede definir estos parámetros de directivas solo para dispositivos Android.

Kaspersky Security Center Web Console 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 utilizar el Wi-Fi, la cámara y el Bluetooth en el dispositivo sin restricciones.

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

1. Abra la ventana de 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 desea configurar.
   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.
2. En la página de 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 desactivar el módulo Wi-Fi en el dispositivo móvil del usuario, seleccione la casilla **Prohibir el uso de Wi-Fi**.

     En dispositivos con Android 10.0 o versiones posteriores, no se admite la prohibición del uso de redes Wi-Fi.

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

  En dispositivos con Android 10.0 o versiones posteriores, el uso de la cámara no se puede prohibir completamente.

  En los dispositivos con Android 11 o posterior, Kaspersky Endpoint Security for Android debe estar configurado como función de accesibilidad. Kaspersky Endpoint Security for Android solicita al usuario que configure la app como una función de Accesibilidad a través del Asistente de configuración inicial. El usuario puede omitir este paso o desactivar este servicio en la configuración del dispositivo más adelante. Si este es el caso, no podrá restringir el uso de la cámara.

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

  En Android 12 o versiones posteriores, puede desactivarse el uso de Bluetooth 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 que ha realizado en la directiva y salir de la ventana de 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 for Android contra eliminación

Para protección del dispositivo móvil y cumplimiento normativo con los requisitos corporativos de seguridad, puede activar la protección contra eliminación de Kaspersky Endpoint Security for Android. En este caso, el usuario no puede eliminar la aplicación con la interfaz de Kaspersky Endpoint Security for Android. Al eliminar la aplicación con las herramientas del sistema operativo Android, se le indicará al usuario que desactive los derechos de administrador para Kaspersky Endpoint Security for Android. Después de desactivar los derechos, el dispositivo móvil se bloqueará.

Para activar la protección contra eliminación de Kaspersky Endpoint Security for Android:

1. Abra la ventana de 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 desea configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la página de 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 eliminar Kaspersky Endpoint Security for Android del dispositivo**.

   Para proteger la aplicación contra la eliminación en dispositivos con Android 7.0 o versiones posteriores, Kaspersky Endpoint Security for Android debe estar configurado como función de accesibilidad. Cuando el Asistente de configuración inicial se está ejecutando, Kaspersky Endpoint Security for 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 que ha realizado en la directiva y salir de la ventana de propiedades de la directiva.

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

Si se intenta 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 de dispositivos móviles, debe definir la configuración de sincronización. La sincronización de dispositivos móviles con Kaspersky Security Center se puede realizar de las siguientes formas:

- **Según programación.** La sincronización mediante programación se realiza con el protocolo http. Puede configurar la programación de sincronización en las propiedades de la directiva. Las modificaciones en la configuración de directivas, comandos y 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 versiones posteriores, 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 automáticas del servicio de FCM (Firebase Cloud Messaging). La sincronización forzada se quiere principalmente para la entrega oportuna de comandos a un dispositivo móvil. Si desea usar la sincronización forzada, asegúrese de que la configuración de FCM esté definida en Kaspersky Security Center.

Para configurar la sincronización de dispositivos móviles con Kaspersky Security Center:

1. Abra la ventana de 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 desea configurar.

- En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la página de 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 período de sincronización.

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

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

   De forma predeterminada, la sincronización en itinerancia está activada.

5. Haga clic en el botón **Guardar** para guardar los cambios que ha realizado en la directiva y salir de la ventana de 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 for Android y Kaspersky Security for iOS utilizan datos recopilados de usuarios de todo el mundo. *Kaspersky Security Network* se ha diseñado para procesar dichos datos.

Kaspersky Security Network (KSN) es una infraestructura de servicios en la nube que permite acceder a la base de conocimientos en línea de Kaspersky con información sobre la reputación de los archivos, los recursos web y el 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. La participación 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 hace posible llevar un seguimiento de amenazas en tiempo real. Los archivos o las partes de archivos que pueden ser aprovechados por intrusos para dañar el ordenador o el contenido del usuario también se pueden enviar a Kaspersky para su análisis adicional.

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

- Los componentes Antivirus, Protección web y Control de aplicaciones en la aplicación Kaspersky Endpoint Security for Android.

- El componente Protección web en la aplicación Kaspersky Security for 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 el Intercambio de información con Kaspersky Security Network.

Si se rechaza la participación en KSN, se reduce el nivel de protección, con riesgo de infección del dispositivo y 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 for Android

Para mejorar la protección en tiempo real, Kaspersky Endpoint Security for 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 en línea de Kaspersky para comprobar la reputación de 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 usar todas las funciones 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 los usuarios según listas de categorías permitidas y bloqueadas (por ejemplo, la categoría "Comunicación por Internet").

- **Control de aplicaciones.** La aplicación determina la categoría de la aplicación para restringir el inicio de aplicaciones que no cumplan con los requisitos corporativos de seguridad 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 aplicaciones está disponible en el Contrato de licencia de usuario final. Al aceptar los términos y las condiciones del Contrato de licencia, acepta transferir esta información.

La información sobre los tipos de datos enviados a Kaspersky cuando se usa KSN durante el funcionamiento de Protección web está disponible en la Declaración sobre el procesamiento de datos para Protección web. Al aceptar los términos y las condiciones de la Declaración, acepta transferir esta información.

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

La provisión de datos a KSN es voluntaria. Si lo desea, puede desactivar el intercambio de datos con KSN.

Intercambio de información en Kaspersky Security for iOS

Para mejorar la protección en tiempo real, Kaspersky Security for 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 for iOS.

La provisión de datos a KSN es voluntaria. Si lo desea, puede desactivar el intercambio de datos con KSN.

Envío de estadísticas a KSN desde aplicaciones de Android o iOS

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

- El usuario del dispositivo debe leer y aceptar los términos de la Declaración de Kaspersky Security Network.
- Debe configurar las opciones de la directiva de grupo para permitir que las estadísticas se envíen a KSN.

Puede dejar de 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.

Cómo activar y desactivar Kaspersky Security Network

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

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

Activar o desactivar el uso de Kaspersky Security Network:

1. Abra la ventana de 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 desea configurar.
   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.
2. En la página de propiedades de la directiva, seleccione **CONFIGURACIÓN DE LA APLICACIÓN** > **KSN y Estadísticas**.
3. Para activar o desactivar el uso de Kaspersky Security Network, seleccione o cancele la selección de la casilla **Utilizar Kaspersky Security Network**.
4. Si el uso de Kaspersky Security Network está activado y acepta enviar datos a Kaspersky, seleccione la casilla **Permitir el envío de estadísticas a Kaspersky Security Network**. Estos datos ayudarán a la aplicación móvil a responder a amenazas con mayor rapidez, mejorar el rendimiento de los componentes de protección y disminuir la probabilidad de falsas alarmas.

5. Haga clic en el botón **Guardar** para guardar los cambios que ha realizado en la directiva y salir de la ventana de 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 for 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 se desactiva de manera predeterminada.

Para activar el intercambio de datos:

1. Abra la ventana de 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 desea configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la página de 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 que ha realizado en la directiva y salir de la ventana de 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 las notificaciones de Kaspersky Endpoint Security for Android distraigan al usuario del dispositivo móvil, puede desactivar 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. No se puede eliminar una notificación del estado de protección. La notificación muestra el estado de protección del dispositivo (por ejemplo,) y el número de problemas, si los hay. El usuario del dispositivo puede tocar el estado de protección del dispositivo y ver la lista de problemas en la aplicación.

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

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

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

Un usuario del dispositivo Android puede desactivar todas las notificaciones desde Kaspersky Endpoint Security for Android en la configuración de la barra de notificaciones. Si las notificaciones se desactivan, el usuario no supervisa el funcionamiento de la aplicación y puede perderse información importante (por ejemplo, información sobre fallos durante la sincronización del dispositivo con Kaspersky Security Center). En este caso, para comprobar el estado de funcionamiento de la aplicación, el usuario debe abrir Kaspersky Endpoint Security for Android.

Para configurar la visualización de notificaciones sobre el funcionamiento de Kaspersky Endpoint Security for Android en un dispositivo móvil:

1. Abra la ventana de 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 desea configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

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

3. En la sección **Notificaciones**, configure la visualización de 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 for 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. La aplicación también muestra notificaciones cuando el usuario está trabajando con la aplicación (por ejemplo, cuando el usuario actualiza las bases de datos antivirus manualmente).

Los expertos de Kaspersky recomiendan activar las notificaciones y los mensajes emergentes. Si desactiva las notificaciones y los mensajes emergentes cuando la app está en segundo plano, la app 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 app.

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

4. Haga clic en el botón **Guardar** para guardar los cambios que ha realizado en la directiva y salir de la ventana de propiedades de la directiva.

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

Detección de pirateos del dispositivo

Kaspersky Security Center Web Console le permite detectar actos de piratería del dispositivo (acceso root) en dispositivos Android y liberaciones en dispositivos iOS. Los archivos de sistema están desprotegidos en un dispositivo pirateado y, por lo tanto, se pueden modificar. Además, las apps de terceros de fuentes desconocidas podrían instalarse en dispositivos pirateados. Después de detectar un intento de pirateo, recomendamos que restaure inmediatamente el funcionamiento normal del dispositivo.

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

- *Servicio integrado de Kaspersky Endpoint Security for Android.* Un servicio de Kaspersky que comprueba si el usuario de un dispositivo móvil ha obtenido privilegios de acceso root (Kaspersky Mobile Security SDK).

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

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

- *Servicio integrado de Kaspersky Security for iOS.* Un servicio de Kaspersky que comprueba si se liberó un dispositivo móvil (Kaspersky Mobile Security SDK).

Si el dispositivo es pirateado, recibirá una notificación. Puede ver las notificaciones de piratería en Kaspersky Security Center Web Console, en la pestaña **SUPERVISIÓN E INFORMES** > **PANEL**. También puede desactivar las notificaciones sobre pirateos en la configuración de notificación de eventos.

En dispositivos Android, puede imponer restricciones a la actividad del usuario en el dispositivo si el dispositivo está pirateado (por ejemplo, bloquear el dispositivo). Puede imponer restricciones con el componente Control de cumplimiento. Para hacerlo, 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 for Android o Kaspersky Security for iOS en un dispositivo móvil se realiza proporcionando información de licencia válida a la aplicación. Se proporciona información sobre la licencia al dispositivo móvil junto con la directiva cuando el dispositivo se sincroniza 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 tendrá que 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 de 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 desea configurar.

   - En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **DISPOSITIVOS** > **MÓVILES** > **DISPOSITIVOS**. Haga clic en el dispositivo móvil que pertenece a la directiva que desea configurar y, a continuación, seleccione la directiva en la pestaña **DIRECTIVAS ACTIVAS Y PERFILES DE DIRECTIVAS**.

2. En la página de 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 que ha realizado en la directiva y salir de la ventana de 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 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.

- **Fallo funcional**

  Un fallo funcional indica un problema grave, un error o un mal funcionamiento que se produjo 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 finalización exitosa de una operación o un procedimiento, o del 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:

- Añada o elimine un tipo de evento de la lista de tipos de eventos que se envían a Kaspersky Security Center.
- Defina 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 de 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 y 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 reconteo 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**, añada el tipo de evento informativo **Una aplicación se ha instalado o eliminado (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. Active 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 la 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
Implementación inicial de la aplicación, MB	0,08	17,76	17,84
Actualización inicial de las bases de datos antivirus (el volumen de tráfico puede variar 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 regular de las bases de datos antivirus (el volumen de tráfico puede variar debido al tamaño de las bases de datos antivirus), MB	0,08	3,06	3,14
Ejecución de comandos Antirrobo. Localizar el dispositivo (el volumen de tráfico puede variar debido a las especificaciones de la cámara integrada y a 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 diario medio, 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 mediante el uso de la Consola de administración basada en MMC de Kaspersky Security Center.

Principales casos de uso

INSTALACIÓN

¿Cómo instalo de forma remota Kaspersky Endpoint Security for Android?

¿Cómo puedo impedir que un usuario pueda eliminar Kaspersky Endpoint Security for Android?

¿Cómo activo Kaspersky Endpoint Security for Android?

PROTECCIÓN

¿Cómo bloqueo un dispositivo que ha sido extraviado o robado?

¿Cómo me protejo frente a las amenazas de Internet?

¿Cómo prohíbo el uso de una contraseña vacía?

UTILIZACIÓN DE SOLUCIONES DE TERCEROS

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

VMware AirWatch, MobileIron, IBM Maas360, SOTI MobiControl

CONTROL

¿Cómo impido que un usuario pueda ejecutar juegos en un dispositivo?

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

¿Cómo puedo detectar acceso root?

ADMINISTRACIÓN

¿Cómo configuro un buzón de correo en un dispositivo?

¿Cómo conecto un dispositivo móvil a Wi-Fi?

¿Cómo instalo una app corporativa?

Acerca de Kaspersky Security for Mobile

Kaspersky Security for Mobile 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 for Mobile incluye los componentes siguientes:

- Aplicación móvil Kaspersky Endpoint Security for Android

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

- Complemento de administración de Kaspersky Endpoint Security for Android

El complemento de administración de Kaspersky Endpoint Security for 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 for iOS.

  El Complemento de Administración Kaspersky Device Management for 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 "dispositivo 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 for Android también podría funcionar como parte del *sistema de administración remota de Kaspersky Endpoint Security Cloud*. Para obtener más información sobre el uso de apps a través de Kaspersky Endpoint Security Cloud, consulte la *Ayuda en línea de Kaspersky Endpoint Security Cloud*.

La aplicación móvil de Kaspersky Endpoint Security for Android también puede funcionar como parte de soluciones EMM de terceros de participantes de comunidad AppConfig.

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

Kaspersky Security for Mobile proporciona 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 aplicación Kaspersky Endpoint Security for Android, así como configuración remota de servicios, aplicaciones y funciones de dispositivos Android.
- Configuración remota de dispositivos móviles de acuerdo con los requisitos 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 los 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 o VPN) que permite que la VPN se pueda utilizar en dispositivos móviles. La VPN solo se puede configurar en dispositivos iOS y Samsung.

- Configuración del estado del dispositivo móvil que se muestra en Kaspersky Security Center cuando las reglas de la directiva se infringen: Crítico, Advertencia, Correcto.
- Configuración de las notificaciones que se muestran al usuario en la aplicación Kaspersky Endpoint Security for Android.
- · Configuración de parámetros en dispositivos compatibles con Samsung KNOX 2.6 o versiones posteriores.
- Configuración de ajustes en dispositivos compatibles con perfiles de trabajo de Android.
- Distribución de la aplicación Kaspersky Endpoint Security for Android mediante la consola Samsung KNOX Mobile Enrollment. La consola Samsung KNOX Mobile Enrollment está diseñada para la instalación por lotes y la configuración inicial de aplicaciones en dispositivos Samsung adquiridos en distribuidores oficiales.
- Se puede realizar una actualización de la aplicación Kaspersky Endpoint Security for 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 for Android pueden comunicarse en Kaspersky Security Center o por correo electrónico.
- Control de cambios de configuración de la directiva (historial de revisiones).

Kaspersky Security for Mobile incluye los siguientes componentes de protección y administración:

- Antivirus (en dispositivos Android)
- Antirrobo (en dispositivos Android)
- Protección web (en dispositivos Android y iOS)
- Control de la aplicación (en dispositivos Android)
- Control de cumplimiento (en dispositivos Android)
- Detección de privilegios de root en dispositivos (para dispositivos Android)

Acerca de la aplicación Kaspersky Endpoint Security for Android

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

La app Kaspersky Endpoint Security for 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 emita un sonido de alarma fuerte.
  - **Foto de identificación** para hacer que el dispositivo tome fotografías con la cámara frontal si alguien intenta desbloquearlo.
  - **Eliminar** datos corporativos para proteger la información confidencial de la empresa.
- **Protección web.** Este componente bloquea los sitios maliciosos diseñados para propagar 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 "Apuestas, loterías, sorteos" o "Comunicación por Internet").
- **Control de aplicaciones.** Este componente le permite instalar aplicaciones recomendadas y necesarias en el dispositivo por medio de un enlace directo al paquete de distribución o un enlace a Google Play. Control de aplicaciones le permite eliminar las aplicaciones bloqueadas que infringen los requisitos corporativos de seguridad.
- **Control de cumplimiento.** Este componente permite comprobar si los dispositivos administrados cumplen con los requisitos corporativos de seguridad e imponer restricciones a determinadas funciones de los dispositivos que no los cumplan.

Acerca de Kaspersky Device Management for iOS

Kaspersky Device Management for iOS garantiza la protección y el control de los dispositivos móviles que se conectan al Kaspersky Security Center e incluye funciones de administración de dispositivos, como:

- **Protección con contraseña**. Esta función le permite establecer requisitos de complejidad de las contraseñas para que los usuarios utilicen contraseñas complejas que cumplan con la política corporativa de contraseñas.
- **Administración de la red**. Esta función le permite añadir redes VPN y de Wi-Fi aprobadas o restringir el acceso a otros.
- **Eliminar datos corporativos**. En caso de que el dispositivo se pierda o sea robado, puede enviarle el comando Eliminar para proteger la información confidencial de la empresa.
- **Protección web**. Este componente bloquea los sitios maliciosos diseñados para propagar 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 "Apuestas, loterías, sorteos" o "Comunicación por Internet").

- **Restricciones de aplicaciones.** Este componente le permite controlar si las aplicaciones nativas del dispositivo, como iTunes, Safari o Game Center, pueden utilizarse en un dispositivo supervisado.

- **Restricciones de las Funciones.** Este componente permite comprobar si los dispositivos administrados cumplen con los requisitos corporativos de seguridad e imponer restricciones a determinadas funciones de 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 Microsoft Exchange Server. Para obtener más información sobre cómo instalar un servidor Exchange, consulte la *ayuda de Kaspersky Security Center*. No se requiere ninguna configuración adicional en dispositivos móviles.

Con un buzón de correo de Exchange, puede ajustar remotamente los dispositivos EAS usando directivas de grupo y 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 parámetros 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.

Instalación del complemento de administración Kaspersky Endpoint Security for Android

El complemento de administración de Kaspersky Endpoint Security for 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 de Kaspersky Endpoint Security para Android puede utilizarse 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 for Android en dispositivos móviles de los usuarios.
- Recibir informes y estadísticas de funcionamiento de la aplicación móvil Kaspersky Endpoint Security for Android en los dispositivos de los usuarios.

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

Acerca del complemento de administración Kaspersky Device Management for iOS

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

- Crear directivas de seguridad de grupo para los dispositivos móviles.
- Definir remotamente la configuración de dispositivos conectados mediante el protocolo Exchange ActiveSync (en lo sucesivo, "dispositivos EAS").
- Definir remotamente la configuración de dispositivos conectados mediante el protocolo MDM para 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 cómo conectar los dispositivos móviles a Kaspersky Security Center mediante el uso de los protocolos Exchange ActiveSync y MDM para iOS, consulte la *ayuda de Kaspersky Security Center*.

El complemento de administración Kaspersky Device Management for 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 for Mobile.

Requisitos de hardware y software para el equipo del administrador

Para implementar la solución completa Kaspersky Security for Mobile, 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 for 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 for iOS, el equipo del administrador debe cumplir estos 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 for 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 for Android

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

La aplicación móvil Kaspersky Endpoint Security for Android también puede usarse como parte del sistema de administración remota de Kaspersky Endpoint Security Cloud (versión 6.0 y superior). Para obtener más información sobre el uso de aplicaciones a través de Kaspersky Endpoint Security Cloud, consulte la *Ayuda de Kaspersky Endpoint Security Cloud*.

La aplicación móvil Kaspersky Endpoint Security for Android puede funcionar en sistemas EMM de otros fabricantes:

- 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 for Android

Estos son los requisitos de hardware y software de la aplicación Kaspersky Endpoint Security for 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 instala 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 de software y hardware:

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

Consideraciones y problemas conocidos

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

Problemas conocidos al instalar aplicaciones

- Kaspersky Endpoint Security for Android solo se instala en la memoria principal del dispositivo.
- En dispositivos con Android 7.0, puede ocurrir un error al intentar desactivar derechos del administrador para Kaspersky Endpoint Security for Android en la configuración del dispositivo si Kaspersky Endpoint Security for Android tiene prohibido superponerse en otras ventanas. La causa de este problema es un defecto conocido en Android 7.
- Kaspersky Endpoint Security for Android en dispositivos con el sistema operativo Android 7.0 o posterior no admite el modo multiventana.
- Kaspersky Endpoint Security for Android no funciona en dispositivos de Chromebook con sistema operativo de Chrome.
- Kaspersky Endpoint Security for Android no funciona en dispositivos Samsung con sistemas operativos Android (edición Go).
- Al utilizar la aplicación Kaspersky Endpoint Security for Android con sistemas de EMM de terceros (por ejemplo, VMWare AirWatch), solo están disponibles los componentes Antivirus y Protección Web. El administrador puede ajustar la configuración de Antivirus y Protección Web en la consola del sistema de EMM. En este caso, las notificaciones sobre el funcionamiento de la aplicación solo están disponibles en la interfaz de la app Kaspersky Endpoint Security for Android (Informes).

Problemas conocidos al actualizar la versión de la aplicación

- Solo puede actualizar Kaspersky Endpoint Security for Android a la versión más reciente de la aplicación. Kaspersky Endpoint Security for Android no se puede revertir a una versión más antigua.
- 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.
- Puede actualizar a través de Google Play si Kaspersky Endpoint Security for Android se instaló desde Google Play. Si la aplicación se instaló mediante otro método, no puede actualizar a través de Google Play.
- Se puede actualizar a través de Kaspersky Security Center si Kaspersky Endpoint Security for Android se instaló desde Kaspersky Security Center. Si la aplicación 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 for 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 el funcionamiento del Antivirus

- Debido a limitaciones técnicas, Kaspersky Endpoint Security for 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 en busca de nuevas amenazas cuya información no se haya añadido todavía a las bases de datos antivirus, debe activar el uso de Kaspersky Security Network. *Kaspersky Security Network (KSN)* es una infraestructura de servicios en la nube que proporciona acceso a la base de conocimiento en línea de Kaspersky con información sobre la reputación de los archivos, los recursos web y el 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 algunos dispositivos, Kaspersky Endpoint Security for Android no detecta dispositivos conectados por USB OTG. No es posible ejecutar un análisis antivirus en estos 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 en 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 for Android no detecta la descarga de archivos maliciosos en la memoria del dispositivo. Antivirus puede detectar los archivos maliciosos cuando estos se ejecutan o durante un análisis antivirus del dispositivo. La causa de este problema es un defecto conocido en Android 6.0. Para garantizar la seguridad del dispositivo, se recomienda configurar análisis antivirus planificados.

Problemas conocidos en el funcionamiento de Protección Web

- La Protección web en 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 activada 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, Protección web puede omitir una amenaza (por ejemplo, `https://trusted.domain.com/phishing/`). Si el dominio no es de confianza, Protección web bloquea los sitios web maliciosos y de phishing.

- Para que Protección Web funcione, debe activar el uso de Kaspersky Security Network. Protección Web bloquea los sitios web según los datos de KSN sobre la reputación y la categoría de los sitios web.

- Los sitios web bloqueados pueden permanecer desbloqueados por Protección Web en dispositivos con Android 6.0 con la versión 51 de Google Chrome (o cualquier versión anterior) instalada si el sitio web se abre de las siguientes formas (este problema es causado por un defecto conocido en Google Chrome):
  - Desde los resultados de búsqueda.
  - Desde la lista de marcadores.
  - Desde el historial de búsqueda.
  - Mediante la función de autocompletar direcciones web.
  - Abriendo el sitio web en una nueva pestaña de Google Chrome.
- Los sitios web bloqueados pueden quedar desbloqueados en la versión de Google Chrome 50 (o cualquier versión anterior) si el sitio web se abrió desde los resultados de búsqueda de Google cuando la función **Combinar pestañas y aplicaciones** está activada en la configuración del navegador. La causa de este problema es un defecto conocido en Google Chrome.
- En Google Chrome, los sitios web bloqueados podrían permanecer desbloqueados si el usuario los abre desde aplicaciones de terceros, por ejemplo, desde una aplicación de cliente de MI. Este problema se debe al modo en que funciona el servicio de Accesibilidad con la función de pestañas personalizadas de Chrome.
- En Samsung Internet Browser, los sitios web bloqueados podrían permanecer desbloqueados si el usuario los abre en segundo plano desde el menú contextual o desde aplicaciones de terceros, por ejemplo, desde una aplicación de cliente de MI.
- Kaspersky Endpoint Security for Android debe estar configurado como función de accesibilidad para garantizar un correcto funcionamiento de Protección web.
- Al introducir a dirección de un sitio web en la configuración de Protección Web, respete las reglas siguientes:
  - Para dispositivos de Android, especifique la dirección en formato de expresiones regulares (por ejemplo, `http:\/\/www\.example\.com.*`).
  - Para dispositivos de MDM de iOS, especifique el protocolo del transferencia de datos HTTP o 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 se permiten los sitios web de la lista** cuando la página se actualiza. Los sitios web se bloquean si una expresión regular contiene configuración avanzada (por ejemplo, `^https?:\/\/example\.com\/pictures\/`). Se recomienda usar expresiones regulares sin configuración adicional (por ejemplo, `^https?:\/\/example\.com`).

Problemas conocidos en el funcionamiento del Antirrobo

- Para el envío oportuno de comandos a dispositivos Android, la aplicación utiliza el servicio Firebase Cloud Messaging (FCM). Si FCM no se configura, los comandos se enviarán 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 for Android debe estar configurado como el administrador del dispositivo.
- Para bloquear dispositivos con Android 7.0 o posterior, Kaspersky Endpoint Security for Android debe estar configurado como función de accesibilidad.

- En algunos dispositivos, los comandos de Antirrobo pueden dar un error al ejecutar si el modo de Ahorro de Batería está activado en el dispositivo. Este defecto 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 con 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 el funcionamiento del Control de aplicaciones

- Kaspersky Endpoint Security for Android debe estar configurado como función de accesibilidad para garantizar el correcto funcionamiento del Control de aplicaciones.
- Para que el Control de aplicaciones (categorías de apps) funcione, debe activar el uso de Kaspersky Security Network. El Control de aplicaciones determina la categoría de una aplicación según los datos que disponibles en KSN. Para utilizar KSN, el dispositivo móvil debe estar conectado a Internet. Para el Control de aplicaciones, puede añadir aplicaciones individuales a las listas de aplicaciones bloqueadas y permitidas. En este caso, KSN no es necesario.
- Al configurar el Control de aplicaciones, se recomienda desactivar la casilla **Bloquear aplicaciones del sistema**. El bloqueo de aplicaciones del sistema puede causar problemas en el funcionamiento 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 de MDM de iOS.
  - Dispositivos Samsung (Exchange ActiveSync).
  - Dispositivos de Android con el cliente de correo de TouchDown instalado.

    En las versiones anteriores de Kaspersky Endpoint Security for Android, puede utilizar Kaspersky Security Center para configurar de forma remota la configuración del perfil de TouchDown en el dispositivo de un usuario. Se ha interrumpido la compatibilidad con TouchDown en Kaspersky Endpoint Security for Android Service Pack 4. Para más detalles, consulte el *sitio web del Soporte Técnico de Symantec*.

    Después de actualizar el complemento de administración de Kaspersky Endpoint Security for Android, la configuración de TouchDown en la directiva queda oculta pero se guarda. Cuando se conecten nuevos dispositivos, la configuración de TouchDown se ajustará después de que se aplique la directiva.

    Después de modificar y guardar la directiva, la configuración de TouchDown se eliminará. 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 app 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 app 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.

- 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 corporativos de seguridad (Control de cumplimiento), la app del sistema Configuración puede funcionar incorrectamente cuando se intenta cambiar la contraseña de desbloqueo mediante Kaspersky Endpoint Security for Android. La causa de este problema es un defecto conocido en 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 introduce la contraseña de desbloqueo de la pantalla si los datos del dispositivo están cifrados. Este problema está relacionado con funciones específicas del servicio de accesibilidad con firmware MIUI.

Problemas conocidos al configurar el Wi-Fi

- En dispositivos que ejecutan Android versión 8.0 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 al configurar el APN

- La configuración remota de APN solo está disponible en dispositivos de MDM de iOS o en dispositivos Samsung.

- Configure APN para dispositivos de MDM de iOS en la sección **Comunicaciones celulares**. La sección **APN** está desfasada. Antes de ajustar la configuración de APN, asegúrese de que la casilla **Aplicar en el dispositivo** en la sección **APN** esté desmarcada.

Problemas conocidos con el Firewall

- El uso de Firewall solo está disponible en dispositivos Samsung.

Problemas conocidos al configurar VPN

- La configuración remota de VPN solo está disponible en los dispositivos siguientes:

  - Dispositivos de MDM de iOS.

  - Dispositivos Samsung.

Problemas conocidos al trabajar con contenedores

- En Kaspersky Security for Mobile Service Pack 3 Maintenance Release 2 no se puede crear contenedores para aplicaciones móviles. Sin embargo, los contenedores que se crearon en versiones anteriores de la aplicación se pueden añadir a dispositivos de 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*.
- Las aplicaciones que contienen más de 65 536 métodos (configuración multidex) no se pueden colocar en contenedores en dispositivos Android.

Problemas conocidos con la protección ante la eliminación de la app

- Kaspersky Endpoint Security for Android debe estar configurada como el administrador del dispositivo.
- Para proteger la aplicación contra la eliminación en dispositivos con Android 7.0 o versiones posteriores, Kaspersky Endpoint Security for Android debe estar configurado como función de accesibilidad.
- En algunos dispositivos de Huawei y Xiaomi, la protección de eliminación de Kaspersky Endpoint Security for Android no funciona. Este problema es causado por las funciones específicas del firmware MIUI 7 y 8 en Xiaomi y del firmware EMUI en Huawei.

Problemas conocidos al configurar las restricciones del dispositivo

- En dispositivos con Android 10.0 o versiones posteriores, no se admite la prohibición del uso de redes Wi-Fi.
- En dispositivos con Android 10.0 o versiones posteriores, el uso de la cámara no se puede prohibir completamente.
- En los dispositivos con Android 11 o posterior, Kaspersky Endpoint Security for Android debe estar configurado como función de accesibilidad. Kaspersky Endpoint Security for Android solicita al usuario que configure la app como una función de Accesibilidad a través del Asistente de configuración inicial. El usuario puede omitir este paso o desactivar este servicio en la configuración del dispositivo más adelante. 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 for Android primero intenta obtener la ubicación precisa del dispositivo. Si esto no fue posible, se devuelve la ubicación aproximada del dispositivo solo si se ha recibido 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 for 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 for Android o añadirla manualmente a la lista de aplicaciones que se inician cuando arranca el sistema operativo. Si la aplicación no está incluida en la lista, Kaspersky Endpoint Security for 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. Solo puede desbloquear el dispositivo usando un código de desbloqueo único.

- En ciertos dispositivos (por ejemplo, Meizu y Asus) con Android 6.0 o posterior, después de cifrar los datos y reiniciar el dispositivo Android, debe introducir una contraseña numérica para desbloquear el dispositivo. Si el usuario utiliza una contraseña gráfica para desbloquear el dispositivo, debe convertir la contraseña gráfica a una contraseña numérica. Para obtener más información sobre la conversión de contraseñas gráficas en contraseñas numéricas, consulte el sitio web del Servicio de soporte técnico del fabricante del dispositivo móvil. Este problema está relacionado con el funcionamiento del servicio Funciones de accesibilidad.

- En algunos dispositivos Huawei con el sistema operativo Android 5.X, después de configurar Kaspersky Endpoint Security for Android como función de accesibilidad, se muestra un mensaje incorrecto sobre la falta de los derechos correspondientes. Para esconder este mensaje, active la aplicación como aplicación protegida en la configuración del dispositivo.

- En algunos dispositivos de Huawei con Android 5.X o 6.X, cuando el modo del Ahorro de Batería se activa para Kaspersky Endpoint Security for 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 for Android manualmente. Se recomienda desactivar el modo de Ahorro de batería para Kaspersky Endpoint Security for Android en la configuración del dispositivo.

- En dispositivos Huawei con firmware EMUI que ejecutan Android 7.0, el usuario puede ocultar la notificación relativa al estado de la protección de Kaspersky Endpoint Security for Android. Este problema se debe a algunas características del software de Huawei.

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

- En dispositivos Xiaomi con firmware MIUI que ejecuta Android 6.0, el icono de Kaspersky Endpoint Security for Android se puede ocultar 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 for Android. Este problema ocurre debido a un defecto conocido en el parche de seguridad para Android de Google. Para asegurar el buen funcionamiento, los privilegios requeridos se deben conceder manualmente en la configuración del dispositivo.

- En ciertos dispositivos de Samsung que ejecutan Android 7.0 o posterior, cuando el usuario intenta configurar métodos no admitidos para desbloquear el dispositivo (por ejemplo, una contraseña gráfica), el dispositivo se puede bloquear si las condiciones siguientes se cumplen: la protección de eliminación de Kaspersky Endpoint Security for Android está activada y se cumplen los requisitos de seguridad de la contraseña de desbloqueo de pantalla. Para desbloquear el dispositivo, debe enviar un comando especial al dispositivo.

- En ciertos dispositivos de Samsung no es posible bloquear el uso de huellas digitales para desbloquear la pantalla.

- La Protección web no puede activarse en algunos dispositivos Samsung si el dispositivo está conectado a una red 3G/4G, tiene activado 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 de Samsung, si la contraseña de desbloqueo no cumple con los requisitos corporativos de seguridad, Kaspersky Endpoint Security for Android no bloquea el uso de huellas digitales para desbloquear la pantalla.

- Después de ejecutar comandos de Antirrobo (por ejemplo Localizar, Bloqueo del dispositivo, Desbloquear, y Foto de identificación), el certificado general y el certificado de VPN se pueden eliminar en algunos dispositivos de Samsung. Se deben reinstalar los certificados para continuar. Este problema ocurre debido al estándar de seguridad del perfil de protección fundamental de dispositivos móviles (Mobile Device Fundamentals Protection Profile, MDFPP).

- En algunos dispositivos Honor y Huawei, no puede restringir el uso de Bluetooth. Cuando Kaspersky Endpoint Security for Android intenta restringir el uso de Bluetooth, el sistema operativo muestra una notificación con las opciones para rechazar o permitir la restricción. El usuario puede rechazar esta restricción y continuar usando 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 for Android. Como consecuencia, la protección y la administración del dispositivo se desactivan, todas las configuraciones definidas se vuelven ineficaces y la aplicación Kaspersky Endpoint Security for 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 for Android, y no se puede reemplazar porque es parte del sistema operativo Android.

- En algunos dispositivos que ejecutan Android 11, la aplicación Kaspersky Endpoint Security for Android se bloquea inmediatamente después del inicio. La causa de este problema es un defecto conocido en Android 11.

Despliegue

Esta sección de Ayuda está pensada para especialistas que instalan Kaspersky Security for Mobile, así como para especialistas que proporcionan soporte técnico a organizaciones que usan Kaspersky Security for Mobile.

Arquitectura de la solución

Kaspersky Security for Mobile incluye los componentes siguientes:

- Aplicación móvil Kaspersky Endpoint Security for Android

  La aplicación Kaspersky Endpoint Security for Android garantiza la protección de dispositivos móviles frente a 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.

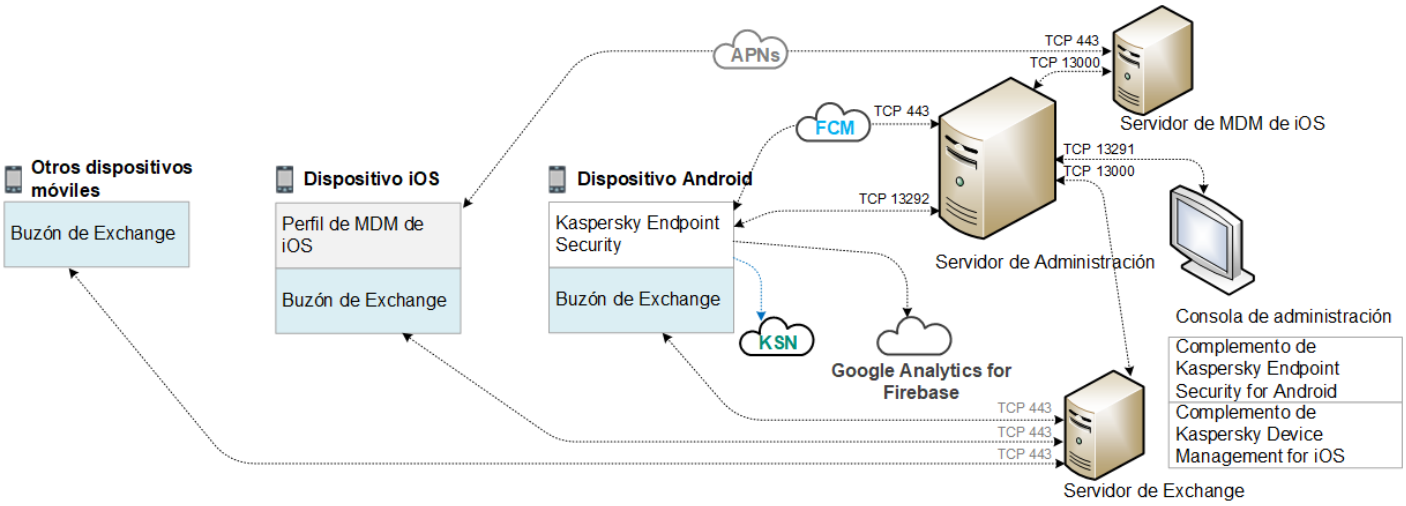
- Complemento de administración de Kaspersky Endpoint Security for Android

  El complemento de administración de Kaspersky Endpoint Security for 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 for iOS.

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

La arquitectura de la solución integrada de Kaspersky Security for Mobile se muestra en la figura a continuación.



Arquitectura de Kaspersky Security for Mobile

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 implementación de la solución integrada

En esta sección se describen los escenarios comunes de implementación de la solución integrada Kaspersky Security for Mobile.

Pueden usarse distintos modos de instalación para la solución integrada en dispositivos de Android y dispositivos de 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 implementación correspondiente.

Escenarios de implementación de Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android se puede implementar en dispositivos móviles de la red corporativa de diferentes formas. Puede usar el escenario de implementación más adecuado para su organización o combinar varios escenarios de implementación.

Para obtener más información sobre la implementación de Kaspersky Endpoint Security for Android en Kaspersky Endpoint Security Cloud, consulte la *ayuda de Kaspersky Endpoint Security Cloud*.

Implementación de Kaspersky Endpoint Security for Android mediante Kaspersky Security Center

Puede implementar Kaspersky Endpoint Security for 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

La implementación de Kaspersky Endpoint Security for 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 for 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 for 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 for Android desde Google Play

Se recomienda emplear el escenario de implementación de Google Play si no es posible la instalación remota.

Los usuarios de dispositivos instalan de forma independiente Kaspersky Endpoint Security for 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. Tras haber instalado la aplicación en el dispositivo, debe realizar preparativos adicionales antes de empezar a utilizarla: configure la conexión al Servidor de Administración e instale un certificado general.

Implementación de Kaspersky Endpoint Security for Android a través de inscripción móvil KNOX

La instalación de Kaspersky Endpoint Security for Android consiste en añadir un perfil MDM de KNOX a dispositivos móviles. El perfil MDM de KNOX contiene un enlace a una aplicación instalada en el Servidor web de Kaspersky Security Center u otro servidor. Después de instalar la aplicación en el dispositivo móvil, también debe instalar un certificado general.

Puede leer sobre la instalación a través de la inscripción móvil KNOX en la sección Samsung KNOX.

Escenarios de implementación 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:

- Ajustar remotamente la configuración de 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 terceros.

Un perfil de MDM para iOS se puede implementar en dispositivos móviles de la red corporativa de diferentes formas. Puede usar el escenario de implementación más adecuado para su organización o combinar varios escenarios de implementación.

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 sobre 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 cómo implementar 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

La implementación 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 sobre cómo crear un perfil de MDM para iOS, consulte la *ayuda de Kaspersky Security Center*.

Preparación de la Consola de administración para la implementación de la solución integrada

En esta sección se incluyen instrucciones sobre la preparación de la Consola de administración para la implementación 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 de Servidor → puertos Adicionales**.

3. Selecciona la casilla de verificación **Abrir puerto 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 clientes móviles**, especifique el puerto que utilizarán los dispositivos móviles para conectarse al Servidor de administración para la activación de la aplicación Kaspersky Endpoint Security for Android. El puerto 17100 se utiliza de forma predeterminada.

6. Haga clic en **Aceptar**.

Visualización de la carpeta Administración de dispositivos móviles 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

Para llevar a cabo una configuración centralizada de la aplicación Kaspersky Endpoint Security for Android instalada en los dispositivos móviles de los usuarios, deben aplicarse 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 asignación automática de dispositivos en los que instalar las aplicaciones para 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 **Equipos administrados**.
2. En el espacio de trabajo de la carpeta o subcarpeta **Equipos administrados**, seleccione la pestaña **Dispositivos**.
3. Haga clic en el botón **Grupo nuevo**.

   Esto abre la ventana en la cual puede crear un nuevo grupo.
4. En la ventana **Nombre de 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

Solo podrá administrar de forma centralizada la configuración de la aplicación Kaspersky Endpoint Security for Android instalada en dispositivos móviles de los usuarios si los dispositivos pertenecen a un grupo de administración creado previamente para el que 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 **Avanzado → 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 una regla para asignar automáticamente dispositivos a un grupo 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 for Android. Para ello, haga clic en **Explorar** a la derecha del campo **Grupo donde mover los dispositivos** y seleccione el grupo en la ventana que aparece.
6. En la sección **Aplicar 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**.

La nueva regla creada aparece en la lista de reglas de asignación de dispositivos de la sección **Mover dispositivos** que hay 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 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 **Emitir 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 de 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 **Generación del certificado** del asistente, haga clic en el botón **Listo** 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 cómo crear certificados y configurar las reglas para emitirlos, consulte la *ayuda de Kaspersky Security Center*.

Instalación de Kaspersky Endpoint Security for Android

En esta sección se describen los métodos de implementación de Kaspersky Endpoint Security for Android en una red corporativa.

Permisos

Para todas las funciones de aplicaciones, Kaspersky Endpoint Security for Android solicita al usuario los permisos requeridos. Kaspersky Endpoint Security for Android solicita los 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 for Android sin proporcionar los permisos obligatorios.

En ciertos dispositivos (por ejemplo, Huawei, Meizu y Xiaomi), en la configuración del dispositivo debe añadir manualmente Kaspersky Endpoint Security for Android a la lista de aplicaciones que se inician cuando arranca el sistema operativo. Si la aplicación no está incluida en la lista, Kaspersky Endpoint Security for Android deja de realizar todas sus funciones después de que el dispositivo móvil se reinicia.

En dispositivos con Android 11 o versiones posteriores, debe desactivar 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 se admiten las funciones Filtro de llamadas y mensajes de texto ni Detector de SIM en Kaspersky Endpoint Security for Android Service Pack 4 Update 4 (Compilación 10.8.0.103). En este caso, Kaspersky Endpoint Security for Android no solicita permisos de administración de SMS al usuario. Para activar Filtro de llamadas y mensajes de texto y todas las funciones de Detector de SIM, debe usar una versión anterior de Kaspersky Endpoint Security for Android.

Permisos solicitados por Kaspersky Endpoint Security for Android

Permiso	Función de la aplicación
Teléfono (obligatorio 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: toma 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 aplicaciones
	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: toma una foto de identificación con la cámara frontal En los dispositivos con Android 11.0 o posterior, el usuario debe conceder el permiso "Mientras se usa la aplicación" cuando se lo pida.
Ubicación	Antirrobo: localización del dispositivo En los dispositivos con Android 10.0 o posterior, el usuario debe conceder el permiso "Todo el tiempo" cuando se le solicite.
Accesibilidad	Antirrobo: bloqueo del dispositivo (solo para Android 7.0 y versiones posteriores)
	Protección web
	Control de aplicaciones
	Protección de eliminación de aplicaciones (solo para Android 7.0 y versiones posteriores)
	Visualización de advertencias de Kaspersky Endpoint Security for Android (solo para Android 10.0 y versiones posteriores)
	Restringir el uso de la cámara (solo para Android 11 o posterior)

Instalación de Kaspersky Endpoint Security for Android mediante un enlace de Google Play

Kaspersky Endpoint Security for Android se instala en los dispositivos móviles de usuarios que tienen 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 for Mobile le permite instalar la aplicación mediante Kaspersky Security Center mediante el uso de un enlace de Google Play.

El usuario recibirá un enlace a Google Play. La aplicación puede instalarse a través del procedimiento de instalación estándar en la plataforma Android. Después de la instalación, no se requiere configuración adicional de Kaspersky Endpoint Security for Android.

Algunos dispositivos Huawei y Honor no tienen servicios de Google y, por lo tanto, acceso a las aplicaciones de Google Play. Si algunos usuarios de los dispositivos Huawei y Honor no pueden instalar la aplicación desde Google Play, se les debe indicar que instalen la aplicación desde Huawei App Gallery.

El enlace 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 for Android y de 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 for Android omite el paso de aceptación durante la instalación de la aplicación.

Para instalar Kaspersky Endpoint Security for 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 las actualizaciones del complemento de administración. Si Kaspersky Security Center detecta actualizaciones, puede instalar la nueva versión del complemento de administración. Cuando se actualiza el complemento de administración, puede aceptar los Términos y condiciones del Contrato de licencia de usuario final (EULA) y las declaraciones adicionales de Kaspersky Endpoint Security for Android. Si el administrador acepta el Contrato de licencia y las declaraciones adicionales en la Consola de administración, Kaspersky Endpoint Security for Android omite el paso de aceptación en 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 for 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 del Kaspersky Endpoint Security for 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 for 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 for 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 enlace 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 for 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 for 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 for Android.

8. Haga clic en **Finalizar** para cerrar el Asistente de Nueva conexión de dispositivo móvil.

Después de instalar Kaspersky Endpoint Security for Android en los dispositivos móviles de los usuarios, podrá ajustar la configuración de dispositivos y aplicaciones con las directivas de grupo. También podrá enviar comandos a dispositivos móviles para la protección de los datos en caso de extravío o robo de los dispositivos.

Otros métodos de instalación de Kaspersky Endpoint Security for Android

Puede instalar Kaspersky Endpoint Security for 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 for 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 for Android desde Google Play, visite el sitio web de soporte técnico de Google.

Para obtener más información sobre el procedimiento de instalación de Kaspersky Endpoint Security for Android desde Huawei AppGallery, visite el sitio web de soporte técnico de HUAWEI.

Algunos dispositivos Huawei y Honor no tienen servicios de Google y, por lo tanto, acceso a las aplicaciones de Google Play. Si algunos usuarios de los dispositivos Huawei y Honor no pueden instalar la aplicación desde Google Play, se les debe indicar que instalen la aplicación desde Huawei App Gallery.

Después de instalar Kaspersky Endpoint Security for 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 for 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 for Android se traslada a la carpeta **Avanzado → 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 utilizando reglas de asignación automáticas.

Este método de instalación es conveniente si desea instalar una versión específica de Kaspersky Endpoint Security for Android.

Para instalar Kaspersky Endpoint Security for 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 incluye 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 Kaspersky Endpoint Security for Android. Se crea sobre la base del paquete de instalación de Kaspersky Endpoint Security for 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 for 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 for 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 for 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 for Android.
- `installer.ini`: 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 for Android.
- `kmlisten.exe`: Herramienta para enviar el paquete de instalación de la aplicación a través de la 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 for Android:

1. En el árbol de la consola, seleccione la carpeta **Avanzado → 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** del asistente, haga clic en el botón **Crear paquete de instalación para la aplicación Kaspersky**.
4. En la ventana **Definir nombre del paquete de instalación** del asistente, ingrese el nombre del paquete de instalación a mostrar 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 for 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 for Android y revocar el Contrato de licencia de usuario final (EULA) para la aplicación. Para obtener más información sobre la forma de revocar el EULA, consulte la *ayuda de Kaspersky Security Center*.

Al finalizar el procedimiento del asistente, el paquete de instalación creado aparece en el área 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 **Avanzado → Instalación remota → Paquetes de instalación**.
2. En el menú contextual del paquete de instalación de Kaspersky Endpoint Security for 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 con el 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 la implementación 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 de 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 **Avanzado → Grupo de redes → Dominios**.

   - En la sección **Acciones durante la instalación**, seleccione la casilla **Solicitar dirección de correo electrónico** si desea que la aplicación solicite a los usuarios que faciliten 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 aplicar la configuración especificada, 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 **Avanzado → Instalación remota → Paquetes de instalación**.

2. Elija el paquete de instalación de Kaspersky Endpoint Security for 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, debe ajustar la configuración de sincronización. La sincronización del dispositivo móvil con Kaspersky Security Center se puede realizar de las siguientes formas:

- **Según programación.** La sincronización mediante según programación se realiza usando el protocolo http. Puede configurar la programación de sincronización en la configuración de la directiva del grupo. Las modificaciones de configuraciones d directivas, comandos y 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 versiones posteriores, 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 usando notificaciones automáticas del servicio de FCM (Firebase Cloud Messaging). La sincronización forzada se quiere principalmente para la entrega oportuna de comandos a un dispositivo móvil. Si desea usar la sincronización forzada, asegúrese de que la configuración de GSM esté configurada 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 que pertenecen los dispositivos de Android.

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 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 itinerancia**.

   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 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 saber más sobre el funcionamiento con comandos para dispositivos móviles, consulte la *ayuda de Kaspersky Security Center*.

Activación de la aplicación Kaspersky Endpoint Security for Android

En Kaspersky Security Center, la licencia puede cubrir varios grupos de funciones. Para asegurarse de que Kaspersky Endpoint Security for Android sea totalmente funcional, 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 de la **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 for Android en un dispositivo móvil se realiza proporcionando información de licencia válida a la aplicación. Se proporciona información sobre la licencia al dispositivo móvil junto con la directiva cuando el dispositivo se sincroniza con Kaspersky Security Center.

Si la activación de la aplicación Kaspersky Endpoint Security for 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 tendrá que 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 Kaspersky Endpoint Security for Android en sus dispositivos manualmente.

Para activar la aplicación Kaspersky Endpoint Security for Android, siga estos pasos:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al que pertenecen los dispositivos de Android.

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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Obtención de 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 almacén de Kaspersky Security Center**.

   Si la aplicación se ha activado sin una clave almacenada en Kaspersky Security Center, Kaspersky Security for Mobile 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 sobre 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 cómo implementar 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 for 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 for iOS para una 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 la aplicación usando directivas de grupo. También podrá enviar comandos a dispositivos móviles para la protección de los datos en caso de extravío o robo de los dispositivos.

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 de Kaspersky Endpoint Security for 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 for iOS ofrece una interfaz para administrar los dispositivos móviles conectados a través del servidor de MDM para iOS y el protocolo Exchange ActiveSync mediante la Consola de administración de Kaspersky Security Center.

Puede instalar los complementos de administración mediante los siguientes métodos:

- Instale un complemento de administración con el Asistente de inicio rápido de Kaspersky Security Center.

  La aplicación le solicita automáticamente que ejecute el Asistente de inicio rápido después de la instalación del Servidor de administración, la primera vez que se conecte. También puede iniciar en cualquier momento el Asistente de inicio rápido de forma manual.

El Asistente de inicio rápido le permite aceptar los Términos y condiciones del Contrato de licencia de usuario final (EULA) para la aplicación de Kaspersky Endpoint Security for Android en la Consola de administración. Si el administrador acepta los términos del Contrato de licencia en la Consola de administración, Kaspersky Endpoint Security for 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 del lanzamiento de nuevas versiones de las aplicaciones de Kaspersky.

- Descarga el paquete de distribución desde una fuente externa e instala el complemento de administración mediante el archivo EXE.

  Por ejemplo, el paquete de distribución del complemento de administración puede descargarse desde 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 las versiones actuales de las aplicaciones de Kaspersky**.

   Se abre la lista de versiones actualizadas de las aplicaciones de Kaspersky.
3. En la sección **Dispositivos móviles**, seleccione el complemento **Kaspersky Endpoint Security for Android** o **Kaspersky Device Management for iOS**.
4. Haga clic en el botón **Descargar paquetes de distribución**.

   Se descargará un paquete de distribución del complemento a 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 for 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 se debe definir la configuración.

Para instalar el complemento de administración Kaspersky Device Management for 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 se debe definir la configuración.

Para asegurarse de que los complementos de administración se han instalado, vea la lista de complementos de administración de aplicaciones instalados, en la ventana de propiedades del Servidor de Administración, en la sección **Avanzado** → **Detalles de los complementos de administración de aplicaciones instalados**.

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 for 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 for Mobile.

- Asegúrese de que Kaspersky Security Center satisfaga los requisitos de software de Kaspersky Security for Mobile.

- Los complementos de administración de Kaspersky Endpoint Security 10.0 Service Pack 2 (compilación 10.6.0.1801) y Kaspersky Device Management for 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 for Android en todos los dispositivos móviles de la organización.

Los términos y condiciones del soporte técnico para las versiones de Kaspersky Security for Mobile 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 aplicaciones**.

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 for Android utilizando los métodos siguientes:

- Si Kaspersky Endpoint Security for 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 for Android se instaló a través de Google Play, puede ver el número de compilación en la configuración de la aplicación (→ **Información de la aplicación**).

Actualización de la versión anterior de Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for 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 for Android comprueba los Términos y condiciones del Contrato de licencia de usuario final (EULA). Si se actualizan los términos del EULA, la aplicación envía una solicitud a Kaspersky Security Center. Si el administrador acepta el EULA en la Consola de administración, Kaspersky Endpoint Security for 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 se realice esta acción, el administrador podrá aceptar los términos del EULA en la Consola de administración para Kaspersky Endpoint Security for Android.

Puede actualizar la aplicación a través de Google Play si Kaspersky Endpoint Security for Android se instaló desde Google Play. Si la aplicación se instaló mediante otro método, no puede actualizarla a través de Google Play.

Actualización de la aplicación mediante Kaspersky Security Center

Kaspersky Endpoint Security for 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 for Android de la versión que cumpla con los requisitos corporativos de seguridad.

Se puede actualizar a través de Kaspersky Security Center si Kaspersky Endpoint Security for Android se instaló desde Kaspersky Security Center. Si la aplicación 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 que pertenecen los dispositivos de Android.
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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Avanzado**.
5. En la sección **Actualización de Kaspersky Endpoint Security for Android**, haga clic en el botón **Seleccionar**.

   Esto abre la ventana **Actualización de Kaspersky Endpoint Security for 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 **Actualización de Kaspersky Endpoint Security for 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 for Android

Si desea evitar la actualización automática de la aplicación y utilizar una versión específica de Kaspersky Endpoint Security for Android, desactive la actualización automática de la aplicación en la configuración de Google Play. Para más detalles, consulte el sitio web del Soporte Técnico de Google.

La actualización automática de Kaspersky Endpoint Security for Android solo está disponible si la aplicación se ha instalado desde Google Play o a través de Kaspersky Security Center usando el enlace de Google Play. Si la aplicación se ha instalado a través de Kaspersky Security Center utilizando un enlace a su propio servidor web (con el paquete de instalación independiente), la actualización automática no está disponible. En este caso, puede utilizar una directiva del grupo para actualizar manualmente Kaspersky Endpoint Security for Android.

Para instalar la versión anterior de Kaspersky Endpoint Security for Android:

1. Elimine Kaspersky Endpoint Security for Android de dispositivos móviles de usuarios.

2. Instale Kaspersky Endpoint Security for Android a través de Kaspersky Security Center usando un enlace a su propio servidor web. Para ello necesitará el paquete de instalación de la versión específica. Puede descargar el paquete de distribución para versiones anteriores de Kaspersky Endpoint Security for Android desde el sitio web del Soporte Técnico de Kaspersky.

Para obtener más información sobre versiones anteriores de Kaspersky Endpoint Security for Android, consulte la *Ayuda para la versión apropiada de Kaspersky Security for Mobile*.

Actualización de versiones anteriores de complementos de administración

Puede actualizar los complementos de administración mediante 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 del lanzamiento de nuevas versiones de las aplicaciones de 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 Kaspersky Endpoint Security for Android y Kaspersky Device Management for iOS, debe descargar la versión más reciente de la aplicación desde la página web de Kaspersky Security for Mobile y ejecutar el Asistente de instalación de cada uno de los dos 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 for Mobile se agregarán a las directivas existentes y tendrán los valores predeterminados.

Si se han añadido nuevos ajustes o se han cambiado 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 una 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 las versiones actuales de las aplicaciones de Kaspersky**.

   Se abre la lista de versiones actualizadas de las aplicaciones de Kaspersky.

3. En la sección **Dispositivos móviles**, seleccione el complemento **Kaspersky Endpoint Security for Android** o **Kaspersky Device Management for iOS**.

4. Haga clic en el botón **Descargar paquetes de distribución**.

   Se descargará un paquete de distribución del complemento a 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 de Kaspersky Endpoint Security for 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 for 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 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 de aplicaciones instaladas, en la ventana de propiedades del Servidor de administración, en la sección **Avanzado** → **Detalles de los complementos de administración de aplicaciones instaladas**.

Eliminación de Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android se puede eliminar de los modos siguientes:

1. Eliminación de la aplicación por parte del usuario

   El usuario elimina Kaspersky Endpoint Security for 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 for 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 que pertenecen los dispositivos de Android.
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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Avanzado**.
5. En la sección **Desinstalar la aplicación Kaspersky Endpoint Security for Android**, seleccione la casilla **Desinstalar Kaspersky Endpoint Security for Android del dispositivo**.
6. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Como consecuencia, Kaspersky Endpoint Security for 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 aquel del que quiera quitar la aplicación.
3. Abra la ventana de propiedades del dispositivo haciendo doble clic en ella.
4. Seleccione **Aplicaciones → Kaspersky Endpoint Security for Android**.
5. Abra la ventana de propiedades de Kaspersky Endpoint Security haciendo doble clic en ella.
6. Seleccione la sección **Avanzado**.
7. En la sección **Eliminación de Kaspersky Endpoint Security for Android**, seleccione la casilla **Desinstalar Kaspersky Endpoint Security for Android del dispositivo**.
8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Como consecuencia, Kaspersky Endpoint Security for Android se elimina del dispositivo móvil 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 versiones posteriores, Kaspersky Endpoint Security for Android debe estar configurado como función de accesibilidad. Cuando el Asistente de configuración inicial se está ejecutando, Kaspersky Endpoint Security for 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 for 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 que pertenecen los dispositivos de Android.
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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Avanzado**.
5. En la sección **Eliminación de Kaspersky Endpoint Security for Android**, seleccione la casilla **Permitir eliminación de Kaspersky Endpoint Security for 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 for Android.

Para permitir la eliminación de la aplicación en la configuración de la aplicación local:

1. En el árbol de la consola, seleccione **Avanzado** → **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 for Mobile**.
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 for Android**, seleccione la casilla **Permitir eliminación de Kaspersky Endpoint Security for 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 for Android.

Eliminación de la aplicación por parte del usuario

Para eliminar de forma independiente Kaspersky Endpoint Security for Android desde un dispositivo móvil, el usuario debe seguir este procedimiento:

1. En la ventana principal de Kaspersky Endpoint Security for Android, pulse → **Desinstale la aplicación**.

   Aparece una solicitud de confirmación en la pantalla.

   Si el botón **Desinstale la aplicación** no se muestra, esto significa que el administrador activó la protección contra la eliminación de Kaspersky Endpoint Security for Android.

2. Confirme la eliminación de Kaspersky Endpoint Security for Android.

Kaspersky Endpoint Security for Android se eliminará del dispositivo móvil del usuario.

Configuración y administración

Esta sección de Ayuda está pensada para especialistas que administran Kaspersky Security for Mobile, así como para especialistas que proporcionan soporte técnico a organizaciones que usan Kaspersky Security for Mobile.

Primeros pasos

En esta sección se describen las acciones recomendadas al empezar a utilizar Kaspersky Security for Mobile.

Inicio y cierre de la aplicación

Kaspersky Security Center automáticamente inicia y detiene complementos de administración de Kaspersky Endpoint Security y Kaspersky Device Management for iOS.

Kaspersky Endpoint Security for Android se inicia durante el arranque del sistema operativo y protege el dispositivo móvil durante la sesión completa. El usuario puede detener la aplicación desactivando todos los componentes de Kaspersky Endpoint Security for Android. Puede usar directivas de grupo para configurar permisos de usuario a fin de administrar componentes de la aplicación.

En ciertos dispositivos (por ejemplo, Huawei, Meizu y Xiaomi), debe añadir manualmente Kaspersky Endpoint Security for Android a la lista de aplicaciones que se inician cuando el sistema operativo arranca (**Seguridad → Permisos → Ejecución automática**). Si la aplicación no está incluida en la lista, Kaspersky Endpoint Security for Android deja de realizar todas sus funciones después de que el dispositivo móvil se reinicia.

También debe desactivar el modo de Ahorro de batería para Kaspersky Endpoint Security for Android. Esto es necesario para que la aplicación se ejecute en segundo plano, por ejemplo, al ejecutar un análisis de virus planificado o al sincronizar el dispositivo con Kaspersky Security Center. Este problema es atribuible a las funciones específicas del software integrado de estos dispositivos.

Creación de un grupo de administración

Para llevar a cabo una configuración centralizada de la aplicación Kaspersky Endpoint Security for Android instalada en los dispositivos móviles de los usuarios, deben aplicarse 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 asignación automática de dispositivos en los que instalar las aplicaciones para 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 **Equipos administrados**.
2. En el espacio de trabajo de la carpeta o subcarpeta **Equipos administrados**, seleccione la pestaña **Dispositivos**.
3. Haga clic en el botón **Grupo nuevo**.

   Esto abre la ventana en la cual puede crear un nuevo grupo.
4. En la ventana **Nombre de 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 del grupo* es un paquete de configuración que permite administrar dispositivos móviles pertenecientes a un grupo de administración y las aplicaciones móviles instaladas en los dispositivos. Puede crear una directiva de grupo utilizando el asistente de directivas.

Puede usar una directiva para establecer la configuración tanto de dispositivos particulares como de un grupo de dispositivos. En el caso de un grupo de dispositivos, la configuración de administración puede definirse en la ventana de propiedades de la directiva de grupo. En el caso de dispositivos por separado, puede definirse en la ventana de la configuración de la aplicación local. La configuración por separado que se especifique en un dispositivo puede diferir de los valores que se establezcan en la directiva para el grupo al que pertenece dicho dispositivo.

Cada parámetro que se representa en una directiva tiene un atributo de bloqueo que indica si tal ajuste permite modificarse en las directivas de los niveles de jerarquía anidados (para grupos anidados y Servidores de administración secundarios) en la configuración de la aplicación local.

Los valores de la configuración establecida en la configuración de directiva y de la aplicación local se guardan en el Servidor de Administración, se aplican a los dispositivos móviles durante la sincronización y se guardan en los dispositivos como las configuraciones actuales. Si el usuario ha especificado otros valores de configuración que no se han bloqueado, en la siguiente sincronización del dispositivo con el Servidor de Administración, son los nuevos valores de configuración los que se transmiten al Servidor de Administración y se guardan en la configuración local de la aplicación, y no aquellos valores que había especificado previamente el administrador.

Para mantener actualizada la seguridad corporativa de dispositivos móviles, puede supervisar los dispositivos de los usuarios a fin de verificar el cumplimiento de la directiva de la administración del grupo.

El indicador de nivel de seguridad se muestra en la parte superior de la ventana de la directiva de 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 alto de protección**: se proporciona un nivel adecuado de protección al dispositivo. Todos los componentes de protección funcionan según la configuración recomendada por Kaspersky.
- **Nivel medio de protección**: el nivel de protección es inferior al recomendado. Algunos componentes de protección críticos están desactivados (por ejemplo, Protección web). Los problemas importantes están marcados con el icono .
- **Nivel bajo de protección**: existen problemas que pueden provocar la infección del dispositivo y la pérdida de datos. Algunos componentes de protección críticos están desactivados (por ejemplo, la protección en tiempo real de dispositivos está desactivada). Los problemas críticos están marcados con el icono .

Para obtener más información sobre cómo administrar las directivas y los grupos de administración de la Consola de administración de Kaspersky Security Center, consulte la *ayuda de Kaspersky Security Center*.

Creación de una directiva de grupo

Esta sección describe el proceso de creación de directivas de grupo para dispositivos en los que se instala la aplicación móvil Kaspersky Endpoint Security for Android, y directivas para dispositivos EAS y dispositivos MDM de iOS.

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 pestaña **Directivas**. El icono que indica el estado de la directiva (activo/inactivo) aparece delante de su nombre. En un grupo pueden crearse varias directivas para diversas aplicaciones. Solo puede estar activa una directiva por aplicación. Al crearse una nueva directiva activa, se desactiva la que estaba activa previamente.

Las directivas se pueden modificar después de su creación.

Crear directiva para administrar dispositivos móviles:

1. En el árbol de la consola, seleccione el grupo de administración para el que quiera crear una 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.

   De este modo, se inicia el asistente de directivas.

Paso 1. Elegir una aplicación para crear una directiva de grupo

En este paso, seleccione la aplicación para la cual desea crear una directiva de grupo en la lista de aplicaciones:

- **Kaspersky Endpoint Security for Android**: para los dispositivos que utilicen la aplicación móvil Kaspersky Endpoint Security for Android.

Se recomienda crear una directiva separada para los dispositivos Huawei y Honor que no tengan los servicios de Google Play. De esta manera, se pueden enviar los enlaces de Huawei AppGallery a los usuarios de dichos dispositivos.

- **Kaspersky Device Management for iOS**: para dispositivos EAS y dispositivos MDM de iOS.

Se puede crear una directiva para dispositivos móviles si el complemento de administración de Kaspersky Endpoint Security for Android y el complemento de administración de Kaspersky Device Management for iOS se instalan en el escritorio del administrador. Si los complementos no están instalados, no aparecerá el nombre de la aplicación correspondiente en la lista de aplicaciones.

Continúe con el siguiente paso del Asistente de directivas.

Paso 2. Introducir un nombre para la directiva de grupo

En este paso, escriba el nombre de la nueva directiva en el campo **Nombre**. Si especifica el nombre de una directiva existente, se agregará (1) al final automáticamente.

Continúe con el siguiente paso del Asistente de directivas.

Paso 3. Crear una directiva de grupo para la aplicación

En este paso, el asistente le pide 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 utilizará en el dispositivo como directiva activa.
- **Directiva inactiva.** El asistente guarda la directiva creada en el Servidor de Administración como directiva de copia de seguridad. Esta directiva podrá activarse en el futuro tras un determinado evento. Si fuera necesario, una directiva inactiva se puede activar.

  Pueden crearse varias directivas para una aplicación en el grupo, pero solo una de ellas puede estar activa. Al crearse una directiva activa, se desactiva automáticamente la que estaba activa previamente.

Salga del asistente.

Configuración de los ajustes de sincronización

Para administrar dispositivos móviles y recibir informes o estadísticas desde dispositivos móviles de usuarios, debe ajustar la configuración de sincronización. La sincronización del dispositivo móvil con Kaspersky Security Center se puede realizar de las siguientes formas:

- **Según programación.** La sincronización mediante según programación se realiza usando el protocolo http. Puede configurar la programación de sincronización en la configuración de la directiva del grupo. Las modificaciones de configuraciones d directivas, comandos y 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 versiones posteriores, 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 usando notificaciones automáticas del servicio de FCM (Firebase Cloud Messaging). La sincronización forzada se quiere principalmente para la entrega oportuna de comandos a un dispositivo móvil. Si desea usar la sincronización forzada, asegúrese de que la configuración de GSM esté configurada 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 que pertenecen los dispositivos de Android.
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 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 itinerancia**.

   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 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 saber más sobre el funcionamiento con comandos para dispositivos móviles, consulte la *ayuda de Kaspersky Security Center*.

Administrar revisiones de directivas de grupo

Kaspersky Security Center le permite rastrear modificaciones de directivas de grupo. Cada vez que guarda cambios realizados en una directiva de grupo, se crea una *revisión*. Cada revisión tiene un número.

Puede administrar revisiones solo para directivas de Kaspersky Endpoint Security for Android. No puede administrar revisiones para una directiva de Kaspersky Device Management for 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 directivas en una revisión seleccionada.
- Guardar revisiones como un archivo .txt.

Para obtener más información sobre cómo administrar las revisiones de las directivas de grupo y otros objetos (por ejemplo, las cuentas de los usuarios), consulte la *ayuda de Kaspersky Security Center*.

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 que pertenecen los dispositivos de Android.
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 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:

   - Número de la revisión de la directiva.
   - Fecha y hora en que se modificó la directiva.
   - El nombre del usuario que modificó la directiva.
   - La acción realizada en la directiva.
   - Descripción de la revisión realizada en la configuración de la directiva.

Eliminar 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 quiera eliminar una directiva.
2. En el área de trabajo del grupo de administración seleccionado de la pestaña **Directivas**, seleccione la directiva de la aplicación correspondiente.
3. En el menú contextual de la directiva, seleccione **Eliminar**.

Al hacerlo, se eliminará la directiva de grupo. Antes de que se aplique la nueva directiva de grupo, los dispositivos móviles pertenecientes al grupo de administración siguen funcionando con la configuración especificada en la directiva eliminada.

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 for Mobile según los deberes de trabajo de los usuarios.

En la interfaz de la Consola de administración, puede configurar los derechos de acceso en la ventana Propiedades del Servidor de Administración de las pestañas **Seguridad** y **Funciones de usuario**. La pestaña **Funciones de usuario** permite agregar funciones de usuario estándares con un conjunto de derechos predefinido. La sección **Seguridad** permite configurar los derechos de un usuario o de un grupo de usuarios, o bien asignar funciones a un usuario o a un grupo de usuarios. Los derechos de usuario de cada aplicación se configuran según los *ámbitos funcionales*.

También puede configurar permisos de usuario específicos para áreas funcionales. Se proporciona la información sobre la correspondencia entre áreas funcionales y pestañas de directivas en el Anexo.

Para cada área funcional, el administrador puede asignar los siguientes permisos:

- **Permitir editar**. El usuario de la Consola de administración tiene permiso para cambiar la configuración de directiva en la ventana de propiedades.
- **Bloquear editar**. Se prohíbe al usuario de la Consola de administración cambiar la configuración de directiva en la ventana de propiedades. No se muestran en la interfaz las pestañas de directiva pertenecientes al ámbito funcional para la cual se ha asignado este derecho.

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 de forma remota la protección de dispositivos móviles en la Consola de administración de Kaspersky Security Center.

Configuración de la protección antivirus en dispositivos Android

Para la detección oportuna de amenazas, virus y otras aplicaciones maliciosas, debería ajustar la configuración para protección en tiempo real y ejecución automática de análisis antivirus.

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

- Virus, gusanos, troyanos y herramientas maliciosas
- Adware
- Apps que pueden utilizar los 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 un icono de maletín, Configuración del perfil de trabajo de Android). Kaspersky Endpoint Security for Android no

tiene acceso a la memoria externa en el perfil de trabajo. La información sobre los objetos detectados se muestra en la sección **Estado** de la app. 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 for 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 definir la configuración de protección en tiempo real de dispositivos móviles:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al que pertenecen los dispositivos de Android.
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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Protección**.
5. En la sección **Protección**, establezca la configuración de la protección de sistema de archivos del dispositivo móvil:
   - Para activar la protección en tiempo real del dispositivo móvil contra amenazas, seleccione la casilla de verificación **Activar protección**.

     Kaspersky Endpoint Security for Android analiza solo nuevas apps y archivos desde la carpeta Descargas.
   - Para activar la protección ampliada del dispositivo móvil contra amenazas, seleccione la casilla de verificación **Modo de protección ampliado**.

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

     > En dispositivos con Android 8.0 o posterior, Kaspersky Endpoint Security for Android analiza archivos que el usuario modifica, mueve, instala y guarda, así como copias de archivos. Kaspersky Endpoint Security for Android no analiza archivos cuando están abiertos, o archivos de origen cuando se copian.
   - Para activar el análisis adicional de nuevas apps antes de iniciarlas por primera vez en el dispositivo del usuario con la ayuda del servicio en la nube de Kaspersky Security Network, seleccione la casilla de verificación **Protección en la nube (KSN)**.
   - Para bloquear el software publicitario y las aplicaciones que pueden utilizar delincuentes para dañar el dispositivo o los datos del usuario, seleccione la casilla de verificación **Detectar software publicitario, 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. No se requiere ninguna otra acción del usuario. Antes de eliminar un objeto, Kaspersky Endpoint Security for Android mostrará una notificación temporal sobre la detección del objeto.
   - **Omitir**

Si los objetos detectados se han omitido, Kaspersky Endpoint Security for Android advierte al usuario sobre problemas en la protección del dispositivo. Puede ver más información sobre los objetos omitidos en la sección **Estado** de la aplicación. Para cada amenaza omitida, la app proporciona acciones que el usuario puede realizar para eliminar la amenaza. La lista de objetos omitidos puede cambiar, por ejemplo, si un archivo malicioso se elimina o se mueve. Para recibir una lista actualizada de amenazas, ejecute un análisis del dispositivo completo. Para asegurarse de que sus datos siguen estando protegidos, elimine todos los objetos detectados.

- **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 la autoejecución 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 que pertenecen los dispositivos de Android.
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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Análisis**.
5. Para bloquear el software publicitario y las aplicaciones que pueden utilizar delincuentes para dañar el dispositivo o los datos del usuario, seleccione la casilla de verificación **Detectar software publicitario, 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. No se requiere ninguna otra acción del usuario. Antes de eliminar un objeto, Kaspersky Endpoint Security for Android mostrará una notificación temporal sobre la detección del objeto.

   - **Omitir**

     Si los objetos detectados se han omitido, Kaspersky Endpoint Security for Android advierte al usuario sobre problemas en la protección del dispositivo. Puede ver más información sobre los objetos omitidos en la sección **Estado** de la aplicación. Para cada amenaza omitida, la app proporciona acciones que el usuario puede realizar para eliminar la amenaza. La lista de objetos omitidos puede cambiar, por ejemplo, si un archivo malicioso se elimina o se mueve. Para recibir una lista actualizada de amenazas, ejecute un análisis del dispositivo completo. Para asegurarse de que sus datos siguen estando protegidos, elimine todos los objetos detectados.

   - **Cuarentena**

   - **Preguntar al usuario**

     La app Kaspersky Endpoint Security for Android muestra una notificación que solicita al usuario que elija la acción que debe llevarse a cabo con el objeto detectado: **Omitir** o **Eliminar**.

Cuando la app detecta varios objetos, 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 for Android debe estar configurado como función de accesibilidad para garantizar la visualización de las notificaciones en dispositivos móviles con Android 10.0 o versiones posteriores. Kaspersky Endpoint Security for Android solicita al usuario que configure la app como una función de Accesibilidad a través del Asistente de configuración inicial. El usuario puede omitir este paso o desactivar este servicio en la configuración del dispositivo más adelante. En este caso, Kaspersky Endpoint Security for Android muestra una ventana del sistema Android que solicita al usuario elegir la acción que debe llevarse a cabo con el objeto detectado: Omitir o Eliminar. Para realizar una acción en varios objetos, debe abrir Kaspersky Endpoint Security.

7. La sección **Análisis programado** permite configurar el inicio automático del análisis completo del sistema de archivos del dispositivo. Para ello, haga clic en el botón **Programación** y especifique la frecuencia y la hora de inicio del análisis completo en la ventana **Programación**.

   En Android 12 o versiones posteriores, 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 for Android analiza todos los archivos, incluido el contenido de los archivos.

Para mantener actualizada la protección del dispositivo móvil, establezca la configuración de la actualización de la base de datos antivirus.

De forma predeterminada, las actualizaciones de la base de datos antivirus se desactivan para cuando el dispositivo esté en itinerancia. Las actualizaciones programadas de las bases de datos antivirus no se llevan a cabo.

Para establecer la configuración de 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 que pertenecen los dispositivos de Android.

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 cualquier columna.

4. En la ventana **Propiedades** de la directiva, seleccione la sección **Actualizar base de datos en itinerancia**.

5. Si desea que Kaspersky Endpoint Security for Android descargue actualizaciones de la base de datos de acuerdo con la programación de las actualizaciones cuando el dispositivo esté en la zona de itinerancia, seleccione la casilla de verificación **Permitir actualización de base de datos en itinerancia** en la sección **Actualizar base de datos en itinerancia**.

   Incluso si se desactiva la casilla de verificación, el usuario puede iniciar manualmente una actualización de la base de datos antivirus cuando el dispositivo esté en itinerancia.

6. En la sección **Origen de la actualización de la base de datos**, especifique el origen de las actualizaciones desde el cual Kaspersky Endpoint Security for Android recibirá e instalará las actualizaciones de bases de datos antivirus:

   - **Servidores de Kaspersky**

Utilización de un servidor de actualizaciones Kaspersky como origen de actualizaciones para descargar las bases de datos de Kaspersky Endpoint Security for 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 ejecución de la tarea de actualización). La lista de datos que se transmite durante las actualizaciones de las bases de datos se incluye 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 for 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 for 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://dominio.com/).

7. En la sección **Actualización de la base de datos planificada**, establezca la configuración de las actualizaciones de la base de datos antivirus automática en el dispositivo del usuario. Para ello, haga clic en el botón **Programación** y especifique la frecuencia y la hora de inicio de las actualizaciones en la ventana **Programación**.

   En Android 12 o versiones posteriores, 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 del usuario de un dispositivo móvil en Internet, active Protección web. Protección web bloquea los sitios web maliciosos que distribuyen un código malicioso y los sitios web de phishing diseñados para robar datos confidenciales y obtener acceso a sus cuentas bancarias. Protección web utiliza el servicio en la nube de Kaspersky Security Network para analizar sitios web antes de abrirlos. Protección web también le permite configurar el acceso de los usuarios a sitios web en función de listas predefinidas de sitios web permitidos y bloqueados.

Kaspersky Endpoint Security for Android debe estar configurada como una función de accesibilidad. Kaspersky Endpoint Security for Android solicita al usuario que configure la app como una función de Accesibilidad a través del Asistente de configuración inicial. El usuario puede omitir este paso o desactivar este servicio en la configuración del dispositivo más adelante.

La Protección web en 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 activada solo para el perfil de trabajo.

Para activar Protección web en el navegador de Samsung, Huawei y Google Chrome:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al que pertenecen los dispositivos de Android.
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 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 relativa al procesamiento de datos para el uso de Protección web (Declaración de Protección web):
   a. Haga clic en el enlace **Declaración de Protección web**.
      Esto abre la ventana **Declaración sobre el procesamiento de datos para el uso de Protección web**. Para aceptar la Declaración de Protección web, debe leer y aceptar la Política de privacidad.
   b. Haga clic en el enlace de la Política de privacidad. Lea y acepte la Política de privacidad.
      Si no acepta la Política 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** → **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**, Protección web no bloquea los sitios en un dispositivo móvil. El usuario del dispositivo móvil no puede activar la Protección web en Kaspersky Endpoint Security.
7. Seleccione la casilla de verificación **Activar 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 extraviados

En esta sección se describe cómo establecer la configuración de protección ante accesos no autorizados en el dispositivo en caso de pérdida o robo de este.

Envío de comandos a un dispositivo móvil

Para proteger los datos de dispositivos móviles perdidos o robados, puede enviar comandos especiales (consulte la tabla a continuación).

Comandos para proteger datos de un dispositivo perdido o robado

Método	Comando	Resultado de la ejecución del comando

de conexión a Kaspersky Security Center		
Kaspersky Endpoint Security for 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, no se modifica la contraseña de desbloqueo de pantalla.
	Localizar dispositivo	Se localiza el dispositivo y se muestra en Google Maps. El proveedor de servicios móviles cobra una tarifa por el envío de SMS y 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 for Android primero intenta obtener la ubicación precisa del dispositivo. Si esto no fue posible, se devuelve la ubicación aproximada del dispositivo solo si se ha recibido no más de 30 minutos antes. De lo contrario, el comando **Localizar dispositivo** falla.
	Foto de identificación	El dispositivo móvil se bloquea. La cámara frontal del dispositivo toma la foto de identificación cuando alguien intenta desbloquear el dispositivo. El proveedor de servicios móviles cobra una tarifa por el envío de SMS y el acceso a Internet. Al intentar desbloquear el dispositivo, el usuario acepta automáticamente la foto de identificación. Si se ha revocado 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 ha revocado 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 emite una alarma. La alarma suena durante 5 minutos (o durante 1 minuto si la carga de la batería del dispositivo es baja).
	Eliminar datos corporativos	Se borran datos de contenedor, cuenta de correo electrónico corporativa, configuración para conectar a la red Wi-Fi corporativa y VPN, nombre de punto de acceso (APN), perfil de trabajo de Android, contenedor KNOX y clave del gestor de licencias de KNOX.
	Restablecer a la configuración de fábrica	Se eliminan todos los datos del dispositivo móvil y se restablecen los valores de fábrica de la configuración. Después de ejecutarse este comando, el dispositivo no podrá recibir o ejecutar comandos subsecuentes.
Perfil de MDM para iOS	Bloquear	El dispositivo móvil se bloquea.
	Desbloquear	Se desactiva el dispositivo móvil que se cierra con un código PIN. El código

		PIN anteriormente especificado se ha restablecido.
	Eliminar datos corporativos	Se eliminan del dispositivo todos los perfiles de configuración y perfiles de aprovisionamiento, el perfil de MDM para iOS y las aplicaciones instaladas para las que se haya seleccionado la casilla **Quitar junto con el perfil MDM para iOS**.
	Restablecer a la configuración de fábrica	Se eliminan todos los datos del dispositivo móvil y se restablecen los valores de fábrica de la configuración. Después de ejecutarse este comando, el dispositivo no podrá recibir o ejecutar comandos subsecuentes.
Buzón de correo de Exchange	Restablecer a la configuración de fábrica	Se eliminan todos los datos del dispositivo móvil y se restablecen los valores de fábrica de la configuración. Después de ejecutarse este comando, el dispositivo no podrá recibir o ejecutar comandos subsecuentes.

Se requieren derechos y permisos especiales para la ejecución de comandos de Kaspersky Endpoint Security for Android. Cuando el Asistente de configuración inicial se está ejecutando, Kaspersky Endpoint Security for Android indica al usuario que conceda a la aplicación todos los derechos y permisos requeridos. El usuario puede omitir estos pasos o desactivar estos permisos en la configuración del dispositivo más adelante. Si hace esto, no será posible ejecutar comandos.

En los dispositivos con Android 10.0 o posterior, el usuario debe conceder el permiso "Todo el tiempo" para acceder a la ubicación. En los dispositivos con Android 11.0 o posterior, el usuario también debe conceder 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 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 aprender más sobre cómo enviar 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 métodos siguientes:

- Envíe el comando de desbloqueo del dispositivo móvil.
- Introduzca el código de desbloqueo de un solo uso en el dispositivo móvil (solo para dispositivos Android).

En ciertos dispositivos (por ejemplo, Huawei, Meizu y Xiaomi), debe añadir manualmente Kaspersky Endpoint Security for Android a la lista de aplicaciones que se inician cuando el sistema operativo arranca. Si la aplicación no se incluye en la lista, puede desbloquear el dispositivo mediante un código de desbloqueo de un solo uso. No puede usar comandos para desbloquear el dispositivo.

Para aprender más sobre cómo enviar comandos desde la lista de dispositivos móviles de la Consola de administración, consulte la *ayuda de Kaspersky Security Center*.

Un *Código de desbloqueo de dispositivo de un solo uso* es un código secreto de la aplicación para desbloquear el dispositivo móvil. El código de un solo uso lo genera la aplicación y es exclusivo de cada dispositivo móvil. Puede cambiar la longitud del código de un solo uso (4, 8 o 16 dígitos) en la configuración de la directiva de grupo en la sección **Antirrobo**.

Para desbloquear el dispositivo móvil usando 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 desee conseguir un código de desbloqueo de un solo uso.
3. Abra la ventana de propiedades del dispositivo móvil haciendo doble clic en ella.
4. Seleccione **Aplicaciones → Kaspersky Endpoint Security for 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 desbloqueo de dispositivo de un solo uso**.
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 escribe el código de un solo uso en la pantalla del dispositivo que está bloqueado por Kaspersky Endpoint Security for 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, no se modifica la contraseña de desbloqueo de pantalla.

Cifrado de datos

Para proteger los datos frente a accesos no autorizados, debe activar el cifrado de todos los datos del dispositivo (por ejemplo, credenciales de cuenta, dispositivos externos y aplicaciones, así como mensajes de correo electrónico, mensajes de texto, contactos, fotos y otros archivos). Para acceder a los datos cifrados, debe especificar una clave especial: la contraseña de desbloqueo del dispositivo. Si los datos se han cifrado, solo se puede acceder a ellos cuando el dispositivo está desbloqueado.

El cifrado de datos se activa de forma predeterminada en dispositivos de iOS bloqueados por la 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 (**Ajustes → Seguridad → Bloqueo de pantalla**).
2. Defina una contraseña de desbloqueo del dispositivo que se ajuste a los requisitos de seguridad corporativos.

   No es recomendable usar un patrón de desbloqueo para desbloquear el dispositivo. En ciertos dispositivos con Android 6.0 o posteriores, después de cifrar los datos y reiniciar el dispositivo Android, debe introducir una contraseña numérica para desbloquear el dispositivo en lugar de un patrón de desbloqueo. Este problema está relacionado con el funcionamiento del servicio Funciones de accesibilidad. Para desbloquear la pantalla del dispositivo en este caso, debe convertir el patrón de desbloqueo en una contraseña numérica. Para obtener más información sobre la conversión de patrones de desbloqueo en contraseñas numéricas, consulte el sitio web de soporte técnico del fabricante del dispositivo móvil.

3. Active el cifrado de todos los datos del dispositivo (**Ajustes → Seguridad → Cifrar datos**).

Configuración de la seguridad de la contraseña de desbloqueo de dispositivos

Para proteger el acceso al dispositivo móvil de un usuario, debería definir una contraseña de desbloqueo del dispositivo.

Esta sección contiene 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 protegido, tiene que configurar el uso de una contraseña que el usuario debe proporcionar cuando el dispositivo sale del modo de suspensión.

Puede imponer restricciones a la actividad del usuario en el dispositivo si la contraseña de desbloqueo no es segura (por ejemplo, bloquear el dispositivo). Puede imponer restricciones usando el componente Control de cumplimiento. Para ello, en la configuración de las reglas de análisis, debe seleccionar el criterio **La contraseña de desbloqueo no se ajusta a los requisitos de seguridad**.

En ciertos dispositivos de Samsung que ejecutan Android 7.0 o posterior, cuando el usuario intenta configurar métodos no admitidos para desbloquear el dispositivo (por ejemplo, una contraseña gráfica), el dispositivo se puede bloquear si las condiciones siguientes se cumplen: la protección de eliminación de Kaspersky Endpoint Security for Android está activada y se cumplen los requisitos de seguridad de la contraseña de desbloqueo de pantalla. Para desbloquear el dispositivo, debe enviar un comando especial al dispositivo.

Para configurar el uso de una contraseña de desbloqueo:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al que pertenecen los dispositivos de Android.
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 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 ha establecido una contraseña de desbloqueo, seleccione la casilla de verificación **Requerir contraseña de desbloqueo de pantalla** en la sección **Bloquear 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 definidos por el administrador.
6. Indique el número 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 versiones posteriores se determinan en base a las siguientes reglas:

- Si la extensión de la contraseña requerida es de 1 a 4 símbolos, la app solicitará que el usuario establezca una contraseña con seguridad media. Debe ser o numérica (PIN) con una secuencia que no tenga números repetidos u ordenados (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 app solicitará que el usuario establezca una contraseña con seguridad alta. Debe ser o numérica (PIN) con una secuencia que no tenga números repetidos u ordenados, o alfabética/alfanumérica (contraseña). 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 digitales**. Si la contraseña de desbloqueo no cumple con los requisitos corporativos de seguridad, 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 for Android no restringe el uso de un escáner de huellas digitales para iniciar sesión en aplicaciones o confirmar compras

   En ciertos dispositivos de Samsung no es posible bloquear el uso de huellas digitales para desbloquear la pantalla. En ciertos dispositivos de Samsung, si la contraseña de desbloqueo no cumple con los requisitos corporativos de seguridad, Kaspersky Endpoint Security for 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 métodos siguientes:

   - Presione el dedo en el escáner de huella digital (método principal).

   - Introduzca la contraseña de desbloqueo (método de reserva).

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 MDM de iOS

Para proteger los datos de los dispositivos MDM de iOS, defina la configuración de seguridad de la contraseña de desbloqueo.

De forma predeterminada, el usuario puede utilizar una contraseña simple. Una *contraseña simple* es una contraseña que contiene caracteres sucesivos o repetitivos, como "abcd" o "2222". El usuario no tiene que introducir una contraseña alfanumérica que incluya símbolos especiales. De forma predeterminada, el período de validez de la contraseña y el número de intentos de introducción de la contraseña no están limitados.

Para definir la configuración de seguridad de una contraseña de desbloqueo de dispositivos MDM de iOS:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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 la contraseña**, seleccione la casilla de verificación **Aplicar configuración en el dispositivo**.

6. Defina la configuración de seguridad de la contraseña de desbloqueo:

   - Para permitir al usuario utilizar una contraseña simple, seleccione la casilla de verificación **Permitir contraseña simple**.

   - Para que el usuario utilice letras y números en la contraseña, seleccione la casilla de verificación **Solicitar valor alfanumérico**.

   - En la lista **Longitud de contraseña mínima**, seleccione la longitud mínima de la contraseña en caracteres.

   - En la lista **Número mínimo de caracteres especiales**, seleccione el número mínimo de caracteres especiales de la contraseña (como "$", "&", "!").

   - En el campo **Validez máxima de la contraseña**, especifique el tiempo en días durante el que la contraseña permanecerá vigente. Cuando este período caduca, Kaspersky Device Management for iOS solicita al usuario que cambie la contraseña.

   - En la lista **Activar bloqueo automático en**, seleccione la cantidad de tiempo tras la cual deberá estar activado el bloqueo automático de dispositivos MDM de iOS.

   - En el campo **Historial de contraseñas**, especifique el número de contraseñas utilizadas (incluida la actual) que Kaspersky Device Management for iOS comparará con la nueva contraseña cuando el usuario decida cambiar la anterior. Si las contraseñas coinciden, se rechaza la nueva contraseña.

   - En la lista **Tiempo máximo para el desbloqueo sin contraseña**, seleccione la cantidad de tiempo tras la cual el usuario podrá desbloquear el dispositivo MDM de iOS sin introducir la contraseña.

   - En **Número máximo de intentos de acceso**, seleccione el número de intentos de acceso que el usuario podrá realizar para introducir la contraseña de desbloqueo del dispositivo MDM de iOS.

7. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Al hacerlo, una vez aplicada la directiva, Kaspersky Device Management for iOS comprobará la seguridad de la contraseña configurada en el dispositivo móvil del usuario. Si el nivel de seguridad de la contraseña de desbloqueo del dispositivo no se ajusta a 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 los datos del dispositivo EAS.

De forma predeterminada, Kaspersky Device Management for iOS no solicita al usuario introducir ni establecer una contraseña de desbloqueo al encender un dispositivo móvil.

Para definir la configuración de seguridad de 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 que pertenecen los dispositivos de EAS.

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 la contraseña**, seleccione la casilla de verificación **Solicitar contraseña**.

6. Defina la configuración de seguridad de la contraseña de desbloqueo:

   - Para que el usuario deba utilizar letras y números en la contraseña, seleccione la casilla de verificación **Solicitar valor alfanumérico**. En el campo **Número mínimo de juegos de caracteres**, especifique el nivel de seguridad de la contraseña alfanumérica. Valores posibles: Entre 1 y 4. El valor "1" corresponde al nivel de seguridad más bajo.

   - Para permitir al usuario utilizar la función de recuperación de la contraseña, seleccione la casilla de verificación **Activar recuperación de contraseñas**.

   - Si desea que los archivos estén cifrados en la memoria del dispositivo, seleccione la casilla de verificación **Requerir cifrado en el dispositivo**.

   - Si desea que los archivos estén cifrados en la tarjeta de memoria, seleccione la casilla de verificación **Requerir cifrado en la tarjeta de memoria**.

   - Para permitir al usuario utilizar una contraseña simple que solo incluya números, seleccione la casilla de verificación **Permitir contraseña simple**.

   - Para limitar el número de intentos de introducción de la contraseña para acceder al dispositivo, seleccione la casilla de verificación **Número máximo de intentos de acceso**. En el campo que hay a la derecha de la casilla de verificación, especifique el número de intentos de introducción de la contraseña que el usuario puede realizar para desbloquear el dispositivo. Si el usuario no introduce la contraseña correcta en el máximo de intentos consecutivos especificado, Kaspersky Device Management for iOS borrará todos los datos del dispositivo.

   - Para especificar la longitud mínima de la contraseña de usuario, seleccione la casilla de verificación **Longitud de contraseña mínima**. Especifique el número mínimo de caracteres de la contraseña en el campo que hay a la derecha de la casilla de verificación. Valores posibles: entre 4 y 16 caracteres.

   - Para que el usuario deba introducir la contraseña cuando el dispositivo lleve algún tiempo inactivo, seleccione la casilla de verificación **Tiempo de inactividad hasta el nuevo intento de introducción de la contraseña (min)**. En el campo que hay a la derecha de la casilla de verificación, especifique el tiempo de inactividad en minutos. Una vez transcurrido ese tiempo, la aplicación le solicita al usuario que introduzca la contraseña.

   - Para limitar el período de validez de la contraseña, seleccione la casilla de verificación **Período de validez de la contraseña (días)**. En el campo que hay a la derecha de la casilla de verificación, especifique el período de validez de la contraseña. Una vez transcurrido ese período, la aplicación solicita al usuario cambiar la contraseña.

   - En el campo **Historial de contraseñas**, especifique el número de contraseñas antiguas más recientes que no pueden reutilizarse.

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 aplicada la directiva, Kaspersky Device Management for iOS comprobará si se ha establecido una contraseña en el dispositivo móvil del usuario. Si no se ha establecido la contraseña de desbloqueo en el dispositivo, se solicitará al usuario que lo haga. A la hora de establecer la contraseña, debe tenerse en cuenta la configuración de directivas. Si se ha establecido la contraseña de desbloqueo del dispositivo pero no se ajusta a la directiva, se solicitará al usuario que la cambie.

Configuración de una red privada virtual (VPN)

Esta sección contiene información sobre cómo configurar los parámetros de la red privada virtual (VPN) para la conexión segura a redes Wi-Fi.

Configuración de VPN en dispositivos Android (solo Samsung)

Para conectar de forma segura un dispositivo Android a redes Wi-Fi y proteger la transferencia de datos, debería ajustar la configuración de VPN (Red privada virtual).

La configuración de VPN solo es posible para dispositivos Samsung.

Cuando utilice una red privada virtual, deberá tener en cuenta los siguientes requisitos:

- La aplicación que usa la conexión VPN se debe permitir en la configuración del firewall.
- La configuración de la red privada virtual definida en la directiva no puede aplicarse a las aplicaciones del sistema. En el caso de las aplicaciones del sistema, es preciso configurar manualmente la conexión de VPN.
- Algunas aplicaciones que utilizan la conexión VPN requieren definir configuraciones adicionales la primera vez que se ejecutan. Para definir la configuración, es preciso permitir la conexión VPN en la configuración de la aplicación.

Para configurar VPN en el dispositivo móvil de un usuario:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al que pertenecen los dispositivos de Android.
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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Gestionar Samsung KNOX → Gestionar 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 la red**, introduzca el nombre del túnel VPN.
8. En el campo **Dirección del servidor**, introduzca el nombre de red o a la dirección IP del servidor VPN.

9. En la lista **Dominios de búsqueda de DNS** introduzca el dominio de búsqueda DNS que se agregará automáticamente al nombre de servidor DNS.

   Puede especificar varios dominios DNS separándolos con espacios en blanco.

10. En el campo **Servidores de DNS**, introduzca el nombre de dominio completo o la dirección IP del servidor DNS.

    Puede especificar varios servidores DNS separándolos con espacios en blanco.

11. En el campo **Enrutamiento**, introduzca el intervalo de direcciones IP de red con las que se intercambian datos a través de la conexión VPN.

    Si el rango de direcciones IP no se especifica en el campo **Enrutamiento**, todo el tráfico de Internet pasará por la conexión de VPN.

12. Además, establezca la siguiente configuración para redes de los tipos **IPSec Xauth PSK** y **L2TP IPSec PSK**:

    a. En el campo **Clave compartida de IPSec**, introduzca la contraseña para la clave de seguridad IPSec predefinida.

    b. En el campo **ID de IPSec**, introduzca el nombre del usuario del dispositivo móvil.

13. Si la red es **L2TP IPSec PSK**, especifique la contraseña para la clave L2TP en el campo **Clave L2TP**.

14. Si la red es **PPTP**, seleccione la casilla **Utilizar conexión SSL** para que la aplicación utilice el método de cifrado de datos MPPE (cifrado punto a punto de Microsoft) para proteger la transmisión de datos cuando el dispositivo móvil se conecte 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.

Configuring VPN on iOS MDM devices

Para conectar un dispositivo MDM de iOS a una red privada virtual y proteger los datos durante la conexión VPN, defina la configuración de conexión VPN.

Para configurar la conexión VPN en el dispositivo MDM de iOS de un usuario:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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** de la sección **Redes VPN**.

   Esto abre la ventana **Red VPN**.

6. En el campo **Nombre de la red**, introduzca 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 la autenticación del usuario del dispositivo móvil de MDM de iOS que utiliza contraseñas MS-CHAP v2, la autenticación de dos factores y la autenticación automática mediante una clave pública.

- **PPTP** (Protocolo de túnel punto a punto). La conexión admite la autenticación del usuario del dispositivo móvil MDM de iOS que utiliza contraseñas MS-CHAP v2 y la autenticación de dos factores.

- **IPSec (Cisco)**. La conexión admite la autenticación de usuario basada en contraseñas, la autenticación de dos factores y la autenticación automática mediante una clave pública y certificados.

- **Cisco AnyConnect**. La conexión admite el firewall Cisco Adaptive Security Appliance (ASA) de la versión 8.0(3).1 o posterior. Para configurar la conexión VPN, instale la aplicación Cisco AnyConnect de la App Store en el dispositivo móvil de MDM de iOS.

- **Juniper SSL**. La conexión admite la puerta de enlace Juniper Networks SSL VPN, SA Series de la versión 6.4 o posterior con el paquete Juniper Networks IVE de la versión 7.0 o posterior. Para configurar la conexión VPN, instale la aplicación de JUNOS desde el App Store en el dispositivo móvil de MDM de iOS.

- **F5 SSL**. La conexión admite las soluciones F5 BIG-IP Edge Gateway, Access Policy Manager y Fire SSL VPN. Para configurar la conexión VPN, instale la aplicación del cliente F5 BIG-IP Edge de la App Store en el dispositivo móvil de MDM de iOS.

- **SonicWALL Mobile Connect**. La conexión admite los dispositivos SonicWALL Aventail E-Class Secure Remote Access de la versión 10.5.4 o posterior, los dispositivos SonicWALL SRA de la versión 5.5 o posterior, así como los dispositivos SonicWALL Next-Generation Firewall, incluidos TZ, NSA, E-Class NSA with SonicOS de la versión 5.8.1.0 o posterior. Para configurar la conexión VPN, instale la aplicación SonicWALL Mobile Connect de la App Store en el dispositivo móvil de MDM de iOS.

- **Aruba VIA**. La conexión admite los controladores de acceso móvil Aruba Networks. Para configurarlos, instale la aplicación Aruba Networks VIA de la App Store en el dispositivo móvil de MDM de iOS.

- **SSL personalizado**. La conexión admite la autenticación del usuario del dispositivo móvil MDM de iOS que utiliza contraseñas y certificados, y la autenticación de dos factores.

8. En el campo **Dirección del servidor**, introduzca el nombre de red o a la dirección IP del servidor VPN.

9. En el campo **Nombre de la cuenta**, introduzca el nombre de la cuenta para su autorización en el servidor VPN. Puede utilizar macros en la lista desplegable **Macros disponibles**.

10. Defina la configuración de seguridad de la conexión VPN según el tipo de red privada virtual seleccionado.

11. Si fuera necesario, defina la configuración de conexión VPN mediante un servidor proxy:

    a. Seleccione la pestaña **Configuración del servidor proxy**.

    b. Seleccione el modo de configuración del servidor proxy y especifique la configuración de conexión.

    c. Haga clic en **Aceptar**.

    Al hacerlo, la configuración de conexión del dispositivo a una red VPN a través de un servidor proxy quedará definida en el dispositivo MDM de iOS.

12. Haga clic en **Aceptar**.

    Aparecerá la nuevo VPN en la lista.

13. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Al hacerlo, la configuración de conexión VPN quedará definida en el dispositivo MDM de iOS del usuario una vez aplicada la directiva.

Configuración de firewall en dispositivos Android (solo Samsung)

Defina la configuración del firewall para supervisar conexiones de 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 que pertenecen los dispositivos de Android.
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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Gestionar Samsung KNOX → Gestionar dispositivos Samsung**.
5. En la ventana **Firewall**, haga clic en **Configurar**.

   Se abrirá la ventana **Firewall**.
6. Seleccione el modo Firewall:
   - Para permitir todas las conexiones entrantes y salientes en el dispositivo móvil, baje el control deslizante a **Permitir todo**.
   - Para bloquear toda la actividad de red salvo la de las aplicaciones de la lista de exclusiones, suba el control deslizante hasta **Bloquear todo salvo excepciones**.
7. Si ha establecido el modo Firewall en **Bloquear todo salvo excepciones**, cree una lista de exclusiones:
   a. Haga clic en **Agregar**.

      Esto abre la ventana **Exclusión de firewall**.
   b. En el campo **Nombre de la aplicación**, escriba el nombre de la aplicación móvil.
   c. En el campo **Nombre de paquete**, introduzca el nombre de sistema del paquete de aplicaciones móviles (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 for Android contra eliminación

Para protección del dispositivo móvil y cumplimiento normativo con los requisitos corporativos de seguridad, puede activar la protección contra la eliminación de Kaspersky Endpoint Security for Android. En este caso, el usuario no puede eliminar la aplicación usando la interfaz Kaspersky Endpoint Security for Android. Al eliminar la aplicación usando las herramientas del sistema operativo de Android, se le indicará que desactive los derechos del administrador para Kaspersky Endpoint Security for Android. Después de desactivar los derechos, el dispositivo móvil se bloqueará.

En ciertos dispositivos de Samsung que ejecutan Android 7.0 o posterior, cuando el usuario intenta configurar métodos no admitidos para desbloquear el dispositivo (por ejemplo, una contraseña gráfica), el dispositivo se puede bloquear si las condiciones siguientes se cumplen: la protección de eliminación de Kaspersky Endpoint Security for Android está activada y se cumplen los requisitos de seguridad de la contraseña de desbloqueo de pantalla. Para desbloquear el dispositivo, debe enviar un comando especial al dispositivo.

Para activar la protección contra eliminación de Kaspersky Endpoint Security for Android:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al que pertenecen los dispositivos de Android.
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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Avanzado**.
5. En la sección **Eliminación de Kaspersky Endpoint Security for Android**, seleccione la casilla **Permitir eliminación de Kaspersky Endpoint Security for Android**.

   Para proteger la aplicación contra la eliminación en dispositivos con Android 7.0 o versiones posteriores, Kaspersky Endpoint Security for Android debe estar configurado como función de accesibilidad. Cuando el Asistente de configuración inicial se está ejecutando, Kaspersky Endpoint Security for 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 intenta eliminar la aplicación, el dispositivo móvil se bloqueará.

Detección de pirateos del dispositivo (acceso root)

Kaspersky Security for Mobile le permite detectar pirateos del dispositivo (acceso root). Los archivos de sistema están desprotegidos en un dispositivo pirateado y, por lo tanto, se pueden modificar. Además, las apps de terceros de fuentes desconocidas podrían instalarse en dispositivos pirateados. Después de detectar un intento de pirateo, recomendamos que restaure inmediatamente el funcionamiento normal del dispositivo.

Para detectar cuándo un usuario obtiene privilegios root, Kaspersky Endpoint Security for Android utiliza los siguientes servicios:

- *Servicio integrado de Kaspersky Endpoint Security for Android* es un servicio de Kaspersky que comprueba si un usuario del dispositivo móvil ha obtenido privilegios root (Kaspersky Mobile Security SDK).

- *Certificación de SafetyNet* es un servicio de Google que comprueba la integridad del sistema operativo, analiza el hardware y el software del dispositivo 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 es pirateado, recibirá una notificación. Puede ver notificaciones de pirateo en el espacio de trabajo del Servidor de administración en la ficha **Supervisión**. También puede desactivar las notificaciones sobre pirateos en la configuración de notificación de eventos.

En dispositivos con Android, puede imponer restricciones a la actividad del usuario en el dispositivo si está pirateado (por ejemplo, bloquear el dispositivo). Puede imponer restricciones usando el componente Control de cumplimiento (consulte la siguiente figura). Para hacer esto, en la configuración de la regla de análisis, seleccione el criterio **El dispositivo ha sido rooteado**.

Configuración de un proxy HTTP global en dispositivos de MDM de iOS

Para proteger el tráfico de Internet del usuario, configure la conexión a Internet del dispositivo iOS con MDM mediante un servidor proxy.

La conexión automática a Internet a través de un servidor proxy solo está disponible para los dispositivos controlados.

Para definir la configuración de proxy HTTP global en el dispositivo MDM de iOS del usuario:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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 del proxy HTTP global**, seleccione la casilla de verificación **Aplicar configuración en el dispositivo**.
6. Seleccione el tipo de configuración de proxy HTTP global.

   De forma predeterminada, la configuración de proxy HTTP global de tipo manual está seleccionada y no se permite al usuario conectarse a redes cautivas sin haberse conectado primero a un servidor proxy. Las *redes cautivas* son redes inalámbricas que requieren realizar una autenticación preliminar en el dispositivo móvil sin conectarse al servidor proxy.

   - Para especificar la configuración de conexión del servidor proxy manualmente:

     a. En la lista desplegable **Tipo de configuración del proxy**, seleccione **Manual**.

     b. En el campo **Dirección y puerto del servidor proxy**, introduzca el nombre de un host o la dirección IP de un servidor proxy y el número de puerto del servidor proxy.

     c. En el campo **Nombre de usuario**, establezca el nombre de cuenta de usuario para la autorización del servidor proxy. Puede utilizar macros en 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, seleccione la casilla de verificación **Permitir el acceso a redes cautivas sin conectarse al proxy**.

- Para definir la configuración de la conexión del servidor proxy mediante un archivo PAC (de configuración de proxy automática) predefinido:

a. En la lista desplegable **Tipo de configuración del proxy**, seleccione **Automático**.

b. En el campo **URL del archivo PAC**, introduzca 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 pueda acceder al archivo PAC, seleccione la casilla de verificación **Permitir conexión directa si no se puede acceder al archivo PAC**.

d. Para permitir al usuario acceder a redes cautivas, seleccione la casilla de verificación **Permitir el acceso a redes cautivas sin conectarse al proxy**.

7. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Al hacerlo, una vez aplicada la directiva, el usuario del dispositivo móvil se conectará a Internet a través de un servidor proxy.

Adición de certificados de seguridad de dispositivos de MDM de iOS

Para simplificar la autenticación de usuarios y garantizar la seguridad de los datos, agregue certificados al dispositivo MDM de iOS del usuario. Los datos firmados con un certificado están protegidos contra su modificación durante el intercambio de red. El cifrado de datos con certificado proporciona un nivel de seguridad adicional para los datos. El certificado también se puede utilizar para comprobar la identidad del usuario.

Kaspersky Device Management for iOS admite los estándares del certificado siguientes:

- **PKCS#1**: Cifrado con una clave pública basada en algoritmos RSA.
- **PKCS#12**: Almacenamiento y transmisión de un certificado y una clave privada.

Para agregar un certificado de seguridad al dispositivo MDM de iOS de un usuario:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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**, seleccione la sección **Certificados**.
5. Haga clic en el botón **Agregar** de la sección **Certificados**.

   Se abrirá la ventana **Certificado**.
6. En el campo **Nombre de archivo**, especifique la ruta del certificado:

Los archivos de los certificados PKCS#1 tienen las extensiones cer, crt o der. Los archivos de los certificados PKCS#12 tienen las extensiones p12 o pfx.

7. Haga clic en **Abrir**.

   Si el certificado está protegido con contraseña, especifíquela. Aparecerá el nuevo certificado en la lista.

8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Al hacerlo, una vez aplicada la directiva, se solicitará al usuario que instale certificados de la lista que se ha creado.

Adición de un perfil de SCEP a dispositivos de MDM de iOS

Debe agregar un perfil de SCEP para permitir al usuario del dispositivo iOS con MDM recibir automáticamente certificados del Centro de certificación a través de Internet. El perfil de SCEP permite la compatibilidad con el protocolo de inscripción de certificados simple.

De forma predeterminada, se agrega un perfil de SCEP con la siguiente configuración:

- El nombre de sujeto alternativo no se utiliza para registrar certificados.
- Tres intentos con 10 segundos de diferencia hacen que se sondee el servidor SCEP. Si todos los intentos de firmar el certificado han fallado, tiene que generar una nueva solicitud de firma de certificado.
- El certificado recibido no se puede utilizar para la firma ni el cifrado de datos.

Puede modificar la configuración especificada al agregar el perfil de SCEP.

Para agregar un perfil de SCEP:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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** de la sección **Perfiles de SCEP**.

   Se abrirá la ventana **Perfil de SCEP**.

6. En el campo **Dirección web del servidor**, introduzca la dirección web del servidor SCEP en la que está implementado 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/servidorcert/scepempresa.

7. En el campo **Nombre**, introduzca el nombre del centro de certificación implementado en el servidor SCEP.
8. En el campo **Firmante**, introduzca una cadena con los atributos del usuario del dispositivo MDM de iOS contenidos en el certificado X.500.

Los atributos pueden contener detalles del país (C), la organización (O) y el nombre de usuario común (CN). Por ejemplo: /C=RU/O=MiEmpresa/CN=Usuario/. También puede utilizar otros atributos especificados en RFC 5280.

9. En la lista desplegable **Tipo de nombre alternativo del sujeto**, seleccione el tipo de nombre alternativo del sujeto del servidor SCEP:

   - **No**: No se utiliza una identificación del nombre alternativa.
   - **Nombre de RFC 822**: La identificación que utiliza la dirección de correo electrónico. La dirección de correo electrónico debe especificarse conforme a RFC 822.
   - **Nombre DNS**: La identificación que utiliza el nombre de dominio.
   - **URI**: La identificación que utiliza la dirección IP o la dirección con formato FQDN.

   Puede utilizar un nombre alternativo del sujeto para identificar al usuario del dispositivo móvil de MDM de iOS.

10. En el campo **Nombre alternativo del firmante**, introduzca el nombre alternativo del sujeto del certificado X.500. El valor del nombre alternativo del asunto depende del tipo de asunto: dirección de correo electrónico del usuario, dominio o dirección web.

11. En el campo **Nombre del sujeto NT**, introduzca el nombre DNS del usuario del dispositivo móvil MDM de iOS de la red de Windows NT.

    El nombre del sujeto NT se incluye en la solicitud de certificado enviada al servidor SCEP.

12. En el campo **Número de intentos de sondeo del servidor SCEP**, especifique el número máximo de intentos de sondeo del servidor SCEP para firmar el certificado.

13. En el campo **Frecuencia de los intentos (s)**, especifique el tiempo en segundos entre los intentos de sondear el servidor SCEP para firmar el certificado.

14. En el campo **Solicitud de registro**, introduzca una clave de registro prepublicada.

    Antes de firmar un certificado, el servidor SCEP solicita al usuario del dispositivo móvil proporcionar la clave. Si se deja este campo vacío, el SCEP no solicita la clave.

15. En la lista desplegable **Tamaño de la clave**, seleccione el tamaño de la clave del registro en bits: 1024 o 2048.

16. Si desea permitir al usuario utilizar un certificado recibido del servidor SCEP como certificado de firma, seleccione la casilla de verificación **Utilizar para firmar**.

17. Si desea permitir al usuario utilizar un certificado recibido del servidor SCEP para el cifrado de datos, seleccione la casilla de verificación **Utilizar para el cifrado**.

    Se prohíbe utilizar el certificado del servidor SCEP como certificado de firma de datos y un certificado de cifrado de datos al mismo tiempo.

18. En el campo **Huella digital del certificado**, introduzca una huella digital de certificado única para comprobar la autenticidad de la respuesta del centro de certificación. Puede utilizar huellas digitales del certificado con el algoritmo de hash MD5 o SHA-1. Puede copiar la huella digital del certificado manualmente o seleccionar un certificado usando el botón **Crear a partir de un certificado**. Cuando se crea la huella con el botón **Crear a partir de un certificado**, esta se agrega al campo automáticamente.

La huella del certificado debe especificarse si el intercambio de datos entre el dispositivo móvil y el centro de certificación se produce a través del protocolo HTTP.

19. Haga clic en **Aceptar**.

    Aparecerá el nuevo perfil de SCEP en la lista.

20. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Al hacerlo, una vez aplicada la directiva, el dispositivo móvil del usuario quedará configurado para recibir un certificado del Centro de certificación automáticamente a través de Internet.

Control

Esta sección contiene información sobre cómo supervisar de forma remota dispositivos móviles en la Consola de administración de Kaspersky Security Center.

Configuración de restricciones

Esta sección proporciona instrucciones sobre cómo configurar el acceso de los usuarios a las funciones de los 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 añadir, 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 escoge 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 sistema operativo de 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 versión 10 o posterior, las redes que se habían añadido anteriormente a través de Kaspersky Security Center no pueden modificarse o eliminarse a través de las directivas de Kaspersky Security Center. En estos casos, 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 para 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 terceros 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 app 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 app 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.
- 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 protegido un dispositivo Android, establezca la configuración del uso del Wi-Fi, la cámara y el Bluetooth en el dispositivo.

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

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

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al que pertenecen los dispositivos de Android.
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 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 desactivar el módulo Wi-Fi en el dispositivo móvil del usuario, seleccione la casilla de verificación **Uso prohibido de Wi-Fi**.

     En dispositivos con Android 10.0 o versiones posteriores, no se admite la prohibición del uso de redes Wi-Fi.

   - Para desactivar la cámara en el dispositivo móvil del usuario, seleccione la casilla de verificación **Uso prohibido de la cámara**.

     En dispositivos con Android 10.0 o versiones posteriores, el uso de la cámara no se puede prohibir completamente.

     En los dispositivos con Android 11 o posterior, Kaspersky Endpoint Security for Android debe estar configurado como función de accesibilidad. Kaspersky Endpoint Security for Android solicita al usuario que configure la app como una función de Accesibilidad a través del Asistente de configuración inicial. El usuario puede omitir este paso o desactivar este servicio en la configuración del dispositivo más adelante. Si este es el caso, no podrá restringir el uso de la cámara.

   - Para desactivar el Bluetooth en el dispositivo móvil del usuario, seleccione la casilla de verificación **Uso prohibido de Bluetooth**.

     En Android 12 o versiones posteriores, puede desactivarse el uso de Bluetooth 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 las restricciones de las funciones del dispositivo iOS con MDM

Para garantizar el cumplimiento de los requisitos de seguridad corporativa, configure las restricciones de funcionamiento del dispositivo MDM de iOS.

Para configurar las restricciones de las funciones del dispositivo MDM de iOS:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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 **Restricción de las funciones**.
5. En la sección **Configuración de restricciones de las funciones**, seleccione la casilla de verificación **Aplicar configuración en el dispositivo**.
6. Configure las restricciones de las funciones del dispositivo MDM de iOS.
7. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.
8. Seleccione la sección **Restricciones de las aplicaciones**.
9. En la sección **Configuración de restricciones de las aplicaciones**, seleccione la casilla de verificación **Aplicar configuración en el dispositivo**.
10. Configure las restricciones de las aplicaciones del dispositivo MDM de iOS.
11. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.
12. Seleccione la sección **Restricciones del contenido multimedia**.
13. En la sección **Configuración de restricciones del contenido multimedia**, seleccione la casilla de verificación **Aplicar configuración en el dispositivo**.
14. Configure las restricciones del contenido multimedia del dispositivo MDM de iOS.
15. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Al hacerlo, una vez aplicada la directiva, las restricciones de las funciones, las aplicaciones y el contenido multimedia se configurarán en el dispositivo móvil del usuario.

Configuración de las restricciones de las funciones del dispositivo EAS

Configure las restricciones de las funciones del dispositivo para mantener protegido el dispositivo EAS.

De forma predeterminada, el usuario puede utilizar funciones de un dispositivo EAS sin restricciones.

Para configurar restricciones en funciones de dispositivos EAS:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al que pertenecen los dispositivos de EAS.
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 las Funciones**.
5. En la sección **Configuración de restricciones de las funciones**, permita o bloquee el uso de funciones de dispositivos EAS:
   - Para permitir al usuario conectar tarjetas de memoria y otras unidades extraíbles al dispositivo, seleccione la casilla de verificación **Permitir unidades extraíbles**.
   - Para permitir el uso de la cámara, seleccione la casilla de verificación **Permitir el uso de la cámara**.
   - Para permitir las conexiones Wi-Fi, seleccione la casilla de verificación **Permitir el uso de Wi-Fi**.
   - Para permitir el uso del puerto de conexión por infrarrojos, seleccione la casilla de verificación **Permitir conexión de infrarrojos**.
   - Para permitir que el usuario utilice el dispositivo como punto de acceso Wi-Fi para crear una red inalámbrica, seleccione la casilla de verificación **Permitir el uso del dispositivo como punto de acceso Wi-Fi**.
   - Para permitir que el usuario se conecte a un escritorio remoto, seleccione la casilla de verificación **Permitir conexión de escritorio remoto**.
   - Para permitir el uso del cliente de escritorio de ActiveSync en el dispositivo, seleccione la casilla de verificación **Permitir sincronización de escritorios**.
   - En la lista desplegable **Uso de Bluetooth**, permita o bloquee el uso del Bluetooth en el dispositivo EAS:
     - **Permitir**. Se permite el uso de Bluetooth en el dispositivo móvil.
     - **Cuando se utilice el manos libres**. El uso del Bluetooth está disponible cuando hay conectados unos auriculares inalámbricos al dispositivo móvil.
     - **Denegar**. El uso de Bluetooth en el dispositivo móvil está bloqueado.
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 del acceso del usuario a sitios web

Esta sección contiene instrucciones sobre cómo configurar el acceso a sitios web en dispositivos iOS y Android.

Configuración del acceso a sitios web en dispositivos Android

Puede usar la Protección web para configurar el acceso de usuarios de dispositivos de Android a sitios web. La Protección web permite filtrar sitios web por categorías definidas en el servicio en la nube de Kaspersky Security Network. El filtrado le permite restringir el acceso de los usuarios a determinados sitios web o categorías de sitios web (por ejemplo, páginas web con las categorías "Apuestas, loterías, sorteo" o "comunicación por Internet"). La Protección web también protege los datos personales de los usuarios en Internet.

Kaspersky Endpoint Security for Android debe estar configurada como una función de accesibilidad. Kaspersky Endpoint Security for Android solicita al usuario que configure la app como una función de Accesibilidad a través del Asistente de configuración inicial. El usuario puede omitir este paso o desactivar este servicio en la configuración del dispositivo más adelante. Si hace esto, no se ejecutará la Protección Web.

La Protección web en 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 activada solo para el perfil de trabajo.

De forma predeterminada, la Protección web está activada: el acceso de los usuarios a los sitios web de las categorías **Suplantación de identidad** y **Software malintencionado** está bloqueado.

Para definir la configuración de acceso del usuario del dispositivo a los sitios web:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al que pertenecen los dispositivos de Android.
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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione **Protección web**.
5. Seleccione la casilla de verificación **Activar Protección web**.
6. Para usar la Protección web, usted o el usuario del dispositivo deben leer y aceptar la Declaración relativa al procesamiento de datos para el uso de Protección web (Declaración de Protección web):
   a. Haga clic en el enlace **Declaración de Protección web**.

      Esto abre la ventana **Declaración sobre el procesamiento de datos para el uso de Protección web**. Para aceptar la Declaración de Protección web, debe leer y aceptar la Política de privacidad.

   b. Haga clic en el enlace de la Política de privacidad. Lea y acepte la Política de privacidad.

      Si no acepta la Política 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** → **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**, Protección web no bloquea los sitios en un dispositivo móvil. El usuario del dispositivo móvil no puede activar la Protección web en Kaspersky Endpoint Security.

7. Si desea que la aplicación restrinja el acceso del usuario a los 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 categorías seleccionadas están prohibidos**.

   b. Cree una lista de categorías bloqueadas seleccionando casillas junto a las categorías de sitios web a los que la app bloqueará el acceso.

8. Si desea que la aplicación permita el acceso de los usuarios únicamente a los 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 añadiendo direcciones de sitios web a los que la app no bloqueará el acceso. Kaspersky Endpoint Security for Android solo admite expresiones regulares. Al escribir la dirección de un sitio web permitido, utilice las siguientes plantillas:

      - `http:\/\/www\.example\.com.*`: Se permiten todas las páginas secundarias del sitio web (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 anular restricciones basadas en contenido sobre el acceso de los usuarios a sitios web, desactive la casilla **Activar 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 del acceso a sitios web en dispositivos MDM de iOS

Configure los ajustes de Protección web para controlar el acceso a sitios web para los usuarios de dispositivos iOS con MDM. Protección web controla el acceso del usuario a los sitios web en función de listas de sitios web permitidos y bloqueados. Protección web también permite agregar marcadores de sitios web al panel de marcadores de Safari.

De forma predeterminada, el acceso a sitios web no está restringido.

La configuración de Protección web solo está disponible en los dispositivos supervisados.

Para configurar el acceso a los sitios web en el dispositivo iOS con MDM del usuario:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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**, seleccione la casilla de verificación **Aplicar configuración en el dispositivo**.

6. Para bloquear el acceso a los sitios web bloqueados y permitirlo para los sitios web permitidos:

   a. En la lista desplegable **Modo de filtrado web**, seleccione el modo **Limitar 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 for iOS permite el acceso a todos los sitios web con ese dominio. Por ejemplo, si ha agregado http://www.example.com a la lista de sitios web permitidos, se permite el acceso a http://pictures.example.com y a http://example.com/movies. Si la lista de sitios web permitidos está vacía, la aplicación permite el acceso a todos los sitios web no 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 for iOS bloquea el acceso a todos los sitios web de ese dominio.

7. Para bloquear el acceso a todos los sitios web distintos a los permitidos en la lista de la pestaña:

   a. En la lista desplegable **Modo de filtrado web**, seleccione el modo **Permitir solo los sitios web en marcadores**.

   b. En la sección **Favoritos**, cree una lista de marcadores de sitios web permitidos.

   La dirección del sitio web debe comenzar con `"http://"` o `"https://"`. Kaspersky Device Management for iOS permite el acceso a todos los sitios web con ese dominio. Si la lista de marcadores está vacía, la aplicación permite el acceso a todos los sitios web. Kaspersky Device Management for iOS agrega sitios web de la lista de marcadores de la pestaña de marcadores de Safari al dispositivo móvil del usuario.

8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Al hacerlo, una vez aplicada la directiva, se configurará la Protección Web en el dispositivo móvil del usuario según el modo seleccionado y las listas creadas.

Control de cumplimiento de dispositivos Android con requisitos de seguridad corporativa

Puede controlar dispositivos Android para verificar que cumplen los requisitos corporativos de seguridad. Los requisitos corporativos de seguridad regulan la utilización del dispositivo por parte del usuario. 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 suficientemente segura. El control de cumplimiento se basa en una lista de reglas. Una regla de cumplimiento incluye los componentes siguientes:

- Criterio de comprobación de dispositivo (por ejemplo, ausencia de aplicaciones bloqueadas en el dispositivo).

- Período de tiempo asignado para que el usuario resuelva el incumplimiento (por ejemplo, 24 horas).
- La acción que se tomará en el dispositivo si el usuario no resuelve el incumplimiento en el período de tiempo asignado (por ejemplo, bloqueo del dispositivo).

  En Android 12 o versiones posteriores, 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 en el plazo especificado, se podrán realizar las siguientes acciones:

- **Bloquear todas las aplicaciones salvo 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 el motivo para bloquear el dispositivo no se rectifica después de desbloquear el dispositivo, este se bloqueará de nuevo después del plazo especificado.
- **Eliminar datos corporativos**. Se borran datos de contenedor, cuenta de correo electrónico corporativa, configuración para conectar a la red Wi-Fi corporativa y VPN, nombre de punto de acceso (APN), perfil de trabajo de Android, contenedor KNOX y clave del gestor de licencias de KNOX.
- **Restablecimiento completo**. Se eliminan todos los datos del dispositivo móvil y se restablecen los valores de fábrica de la configuración. Después de realizar esta acción, el dispositivo dejará de ser un dispositivo administrado. Para conectar el dispositivo a Kaspersky Security Center, debe instalar de nuevo Kaspersky Endpoint Security for Android.

Para crear una regla de análisis del cumplimiento de una directiva de grupo por parte de los dispositivos, siga estos pasos:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al que pertenecen los dispositivos de Android.
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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Control de cumplimiento**.
5. Para recibir notificaciones sobre dispositivos que no cumplen la directiva, seleccione en la sección **Notificación de incumplimiento normativo** la casilla de verificación **Notificar al administrador**.

   Si el dispositivo no cumple con una directiva durante la sincronización del dispositivo con el Servidor de administración, Kaspersky Endpoint Security for Android escribe una entrada para **Violación detectada: <name of the criterion checked>** en el registro de eventos. Puede ver el registro de eventos en la ficha **Eventos** de las propiedades del Servidor de Administración o en las propiedades locales de la aplicación.
6. Para informar al usuario del dispositivo de que su dispositivo no cumple con la directiva, seleccione en la sección **Notificación de incumplimiento normativo** la casilla de verificación **Notificar al usuario**.

   Si se detecta que el dispositivo no cumple con la directiva durante su sincronización con el Servidor de Administración, Kaspersky Endpoint Security for Android notifica al usuario en la sección **Estado**.
7. En la sección **Reglas de cumplimiento**, elabore una lista de reglas para comprobar el cumplimiento de la directiva por parte del dispositivo. 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 nueva regla se muestra en la sección **Reglas de cumplimiento** en la lista de reglas de análisis.

8. Para desactivar temporalmente una regla de análisis que haya creado, active la opción que hay 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, se aplican las limitaciones que ha especificado en la lista de reglas de análisis al dispositivo.

Control de inicio de la aplicación

Esta sección contiene instrucciones sobre cómo configurar el acceso de los usuario a aplicaciones en un dispositivo móvil.

Control de inicio de la aplicación en dispositivos Android

Para mantener protegido el dispositivo móvil del usuario, debe configurar los ajustes de inicio de apps en el dispositivo.

Puede imponer restricciones a la actividad del usuario en un dispositivo en el que hay instaladas aplicaciones bloqueadas o no hay instaladas aplicaciones requeridas (por ejemplo, bloquear el dispositivo). Puede imponer restricciones usando el componente Control de cumplimiento. Para ello, en la configuración de reglas de análisis, debe seleccionar el criterio **Hay aplicaciones bloqueadas instaladas**, **Hay aplicaciones de categorías bloqueadas instaladas** o **No se han instalado todas las aplicaciones necesarias**.

Kaspersky Endpoint Security for Android debe estar configurado como función de accesibilidad para garantizar el correcto funcionamiento del Control de aplicaciones. Kaspersky Endpoint Security for Android solicita al usuario que configure la app como una función de Accesibilidad a través del Asistente de configuración inicial. El usuario puede omitir este paso o desactivar este servicio en la configuración del dispositivo más adelante. Si hace esto, no se ejecutará el Control de aplicaciones.

Para definir la configuración de 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 que pertenecen los dispositivos de Android.

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 cualquier columna.

4. En la ventana **Propiedades** de la directiva, seleccione la sección **Control de aplicaciones**.

5. En la sección **Modo de funcionamiento**, seleccione el modo de inicio de aplicaciones en el dispositivo móvil del usuario:

   - Para permitir que el usuario inicie todas las aplicaciones excepto las especificadas en la lista de categorías y aplicaciones como aplicaciones bloqueadas, seleccione el modo **Aplicaciones bloqueadas**.

- Para permitir que el usuario pueda iniciar solamente las aplicaciones especificadas en la lista de categorías y aplicaciones como aplicaciones permitidas, recomendadas o necesarias, seleccione el modo **Aplicaciones permitidas**.

6. Si desea que Kaspersky Endpoint Security for 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 for Android escribe una entrada para **Se ha instalado una aplicación bloqueada**. Puede ver el registro de eventos en la ficha **Eventos** de las propiedades del Servidor de Administración o en las propiedades locales de la aplicación.

7. Si desea que Kaspersky Endpoint Security for Android bloquee el inicio de las aplicaciones del sistema en el dispositivo móvil del usuario (como Calendario, Cámara y Ajustes), en el modo **Aplicaciones permitidas**, seleccione la casilla de verificación **Bloquear aplicaciones del sistema**.

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

8. Cree una lista de categorías y aplicaciones para configurar el inicio de aplicaciones.

   Para obtener más información sobre categorías de aplicación, consulte los Apéndices.

   Para ver 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 del dispositivo EAS para aplicaciones

Para mantener protegido el dispositivo EAS, configure las restricciones de actividad de la aplicación (explorador, aplicaciones sin firmar).

De forma predeterminada, el usuario puede utilizar aplicaciones en el dispositivo EAS sin restricciones.

Para configurar restricciones de actividad de la aplicación en el dispositivo EAS:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al que pertenecen los dispositivos de EAS.

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 de las Aplicaciones**.

5. En la sección **Configuración de restricciones de las aplicaciones**, defina las restricciones de actividad de la aplicación:

   - Para permitir al usuario utilizar el explorador, seleccione la casilla de verificación **Permitir el uso del navegador**.

- Para permitir al usuario crear cuentas de correo electrónico personales (POP3 o IMAP4), seleccione la casilla de verificación **Permitir correo personal**.
- Para permitir al usuario iniciar aplicaciones que no se han firmado con un certificado de autenticación, seleccione la casilla de verificación **Permitir aplicaciones sin firmar**.
- Para permitir al usuario instalar aplicaciones que no se han firmado con un certificado de autenticación, seleccione la casilla de verificación **Permitir paquetes de instalación sin firmar**.

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 del software en dispositivos Android

Puede realizar un inventario de aplicaciones en dispositivos de Android conectados a Kaspersky Security Center. Kaspersky Endpoint Security for Android recibe la información sobre todas las aplicaciones instaladas en dispositivos móviles. La información recopilada durante el inventario se muestra en las propiedades del dispositivo en la sección **Eventos**. Puede consultar la información detallada de cada aplicación instalada, incluyendo su versión y editor.

Para activar el inventario del software:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al que pertenecen los dispositivos de Android.
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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Control de aplicaciones**.
5. En la sección **Inventario del software**, seleccione la casilla de verificación **Enviar datos a las 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 for Android envía datos al registro de eventos cada vez que se instala o se elimina una aplicación del dispositivo.

Configuración de la visualización de dispositivos Android en Kaspersky Security Center

Para operaciones cómodas 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 consola **Avanzado → 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 añaden 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 for Android podrían no ser operativos por las siguientes razones:

- El usuario desactivó el componente en la configuración del dispositivo.
- El usuario no concedió a la aplicación los permisos necesarios para que el componente funcione (por ejemplo, no hay permiso para determinar la ubicación del dispositivo para el comando Antirrobo correspondiente).

Para mostrar el estado del dispositivo, debe activar la condición **Determinado por la aplicación** en las propiedades del grupo de administración (**Propiedades** → **Estado del dispositivo** → **Establecer estado del dispositivo a crítico si** y **Establecer estado del dispositivo a 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 que pertenecen los dispositivos de Android.
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 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 en la Consola de administración:
   - Modelo del dispositivo [correo electrónico, ID de dispositivo]
   - Modelo del dispositivo [correo electrónico (si existe) o ID de dispositivo]

   Un *ID de dispositivo* es un ID único que genera Kaspersky Endpoint Security for Android a partir de los datos que recibe de un dispositivo. Para los dispositivos móviles con Android 10 o versiones posteriores, Kaspersky Endpoint Security for Android utiliza el SSAID (ID de Android) o la suma de comprobación de otros datos que recibe del dispositivo. Para las versiones anteriores de Android, la aplicación utiliza el IMEI.
6. Configure el atributo "bloquear" en la posición bloqueada ( ).
7. En la sección **Estado del dispositivo en Kaspersky Security Center**, seleccione el estado del dispositivo apropiado si un componente de Kaspersky Endpoint Security for Android no funciona: (**Crítico**), (**Advertencia**) o (**Aceptar**).

   En la lista de dispositivos móviles, el estado del dispositivo se cambiará según el estado seleccionado.
8. Configure el atributo "bloquear" en la posición bloqueada.
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 la configuración de dispositivos móviles en la Consola de administración de Kaspersky Security Center.

Configuración de conexión a una red Wi-Fi

Esta sección proporciona instrucciones sobre cómo configurar la conexión automática a una red Wi-Fi corporativa en dispositivos Android y MDM de iOS.

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 que pertenecen los dispositivos de Android.
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 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 servicios de red (SSID)**, introduzca el nombre de la red inalámbrica que incluye el punto de acceso (SSID).
7. En la sección **Protección de red**, seleccione el tipo de seguridad de la red Wi-Fi (red pública o segura protegida con el protocolo WEP o WPA/WPA2 PSK).
8. En el campo **Contraseña**, establezca una contraseña de acceso de red si seleccionó una red segura en el paso anterior.
9. En el campo **Dirección y puerto del servidor proxy**, introduzca la dirección IP o el nombre DNS del servidor proxy y el número de puerto si es necesario.

   En dispositivos que ejecutan Android versión 8.0 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 directiva para configurar los ajustes para conectarse a la red. En los dispositivos que ejecutan Android 8.0 o versiones posteriores, debe configurar manualmente la configuración del servidor proxy. En los dispositivos que ejecutan Android 8.0 o versiones posteriores, no puede usar una directiva para cambiar la configuración de la conexión de red wifi, excepto la contraseña de acceso a la red.

Si no está utilizando un servidor proxy para conectarse a una red wifi, no hay limitaciones en el uso de directivas para administrar una conexión de red wifi.

10. En el campo **No utilizar el servidor proxy para direcciones**, genere una lista de direcciones web a las que pueda accederse sin utilizar el servidor proxy.

    Por ejemplo, puede introducir la dirección `example.com`. En este caso, no se utilizará el servidor proxy para las direcciones `pictures.example.com`, `example.com/movies`, etc. Puede omitirse el protocolo (por ejemplo, `http://`).

    En dispositivos de Android 8.0 o posterior, la exclusión del servidor proxy para direcciones web no funciona.

11. Haga clic en **Aceptar**.

    La red Wi-Fi añadida se muestra en la lista de **Redes Wi-Fi**.

    Puede modificar o eliminar las redes Wi-Fi de la lista de redes con los botones **Editar** y **Eliminar** de 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. Una vez que se aplique la directiva en el dispositivo móvil, el usuario podrá conectarse a la red Wi-Fi agregada 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 dispositivos MDM de iOS a una red Wi-Fi

Para que un dispositivo MDM de iOS se conecte automáticamente a una red Wi-Fi disponible y proteja los datos durante la conexión, defina la configuración de conexión.

Para configurar la conexión de un dispositivo MDM de iOS a una red Wi-Fi:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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** de la sección **Redes Wi-Fi**.

Esto abre la ventana **Red Wi-Fi**.

6. En el campo **Identificador de servicios de red (SSID)**, introduzca el nombre de la red inalámbrica que incluye el punto de acceso (SSID).

7. Si desea que el dispositivo MDM de iOS se conecte automáticamente a la red Wi-Fi, seleccione la casilla de verificación **Conexión automática**.

8. Para impedir conectar dispositivos MDM de iOS a una red Wi-Fi que requiera la autenticación preliminar (red cautiva), seleccione la casilla **Desactivar detección de redes cautivas**.

   Para usar una red cautiva, debe tener una suscripción, aceptar un acuerdo o realizar un pago. Las redes cautivas se pueden desplegar en ubicaciones como cafeterías y hoteles, por ejemplo.

9. Si desea que una red Wi-Fi se oculte en la lista de redes disponibles en el dispositivo MDM de iOS, seleccione la casilla de verificación **Red oculta**.

   En este caso, para conectarse a la red el usuario debe introducir manualmente el Identificador de servicios de red (SSID) especificado en la configuración del enrutador Wi-Fi del dispositivo móvil.

10. En la lista desplegable **Protección de red**, seleccione el tipo de protección de la conexión de red inalámbrica:

    - **Desactivada**. No se requiere la autenticación del usuario.
    - **WEP**. La red está protegida por el protocolo de cifrado inalámbrico (WEP).
    - **WPA / WPA2 (Personal)**. La red está protegida por el protocolo de acceso protegido inalámbrico (WPA / WPA2).
    - **WPA2 (Personal)**. La red está protegida por el protocolo de acceso protegido inalámbrico WPA2 (Wi-Fi Protected Access 2.0). La protección WPA2 está disponible en dispositivos con iOS de la versión 8 o posterior. WPA2 no está disponible en dispositivos de Apple TV.
    - **Cualquiera (personal)**. La red está protegida mediante los protocolos de cifrado WEP, WPA o WPA2 según el tipo de enrutador wifi. Se utiliza para la autenticación una clave de cifrado única para cada usuario.
    - **WEP (dinámico)**. La red está protegida por el protocolo WEP con el uso de una clave dinámica.
    - **WPA/WPA2 (Empresa)**. La red está protegida mediante los protocolos de cifrado WPA/WPA2 con el uso del protocolo 802.1X.
    - **WPA2 (Empresa)**. La red está protegida mediante el protocolo de cifrado WPA2 con el uso de una clave compartida por todos los usuarios (802.1X). La protección WPA2 está disponible en dispositivos con iOS de la versión 8 o posterior. WPA2 no está disponible en dispositivos de Apple TV.
    - **Cualquiera (Empresa)**. La red está protegida por los protocolos WEP o WPA/WPA2 según el tipo de enrutador wifi. Se utiliza para la autenticación una clave de cifrado compartida por todos los usuarios.

    Si ha seleccionado **WEP (Dinámico)**, **WPA / WPA2 (Empresa)**, **WPA2 (Empresa)** o **Cualquiera (Empresa)**, en la lista **Protección de red**, en la sección **Protocolos**, puede seleccionar el tipo de protocolo EAP (protocolo de autenticación extensible) para la autenticación de usuarios en la red Wi-Fi.

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

11. Defina la configuración de la cuenta para la autenticación de usuarios cuando se conecte el dispositivo MDM de iOS a una red Wi-Fi:

    a. En la sección **Autenticación**, haga clic en el botón **Configurar**.

Se abrirá la ventana **Autenticación**.

b. En el campo **Nombre de usuario**, introduzca el nombre de la cuenta para la autenticación de usuarios cuando se conecten a una red Wi-Fi.

c. Para que el usuario introduzca la contraseña manualmente cada vez que se conecte a una red Wi-Fi, seleccione la casilla de verificación **Solicitar contraseña en cada conexión**.

d. En el campo **Contraseña**, introduzca 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 de usuarios en la red Wi-Fi. Si la lista no contiene certificados, **puede agregarlos en la sección** Certificados.

f. En el campo **ID de usuario**, introduzca el ID de usuario mostrado durante la transmisión de datos al realizar la autenticación, y no el nombre real del usuario.

El ID de usuario está diseñado para hacer que el proceso de autenticación sea más seguro, ya que el nombre de usuario no se muestra públicamente, sino que se transmite a través de un túnel TLS cifrado.

g. Haga clic en **Aceptar**.

Al hacerlo, la configuración de la cuenta para la autenticación de usuarios al conectarse a una red Wi-Fi quedará definida en el dispositivo MDM de iOS.

12. Si fuera necesario, defina la configuración de conexión de red Wi-Fi mediante 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 del servidor proxy y especifique la configuración de conexión.

c. Haga clic en **Aceptar**.

Al hacerlo, la configuración de conexión del dispositivo a una red Wi-Fi a través de un servidor proxy quedará definida en el dispositivo MDM de iOS.

13. Haga clic en **Aceptar**.

Aparecerá la nueva red Wi-Fi en la lista.

14. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Al hacerlo, la configuración de conexión de la red Wi-Fi quedará definida en el dispositivo MDM de iOS del usuario una vez aplicada la directiva. El dispositivo móvil del usuario se conectará automáticamente a las redes Wi-Fi disponibles. La seguridad de los datos durante la conexión a una red Wi-Fi la garantiza la tecnología de autenticación.

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 MDM de iOS

Para permitir al usuario del dispositivo MDM de iOS utilizar el correo electrónico, agregue la cuenta de correo electrónico del usuario a la lista de cuentas en el dispositivo iOS con MDM.

De forma predeterminada, la cuenta de correo electrónico se agrega con la siguiente configuración:

- Protocolo de correo electrónico: IMAP.
- El usuario puede mover mensajes de correo electrónico entre las cuentas de usuario y sincronizar direcciones de cuentas.
- El usuario puede utilizar cualquier cliente de correo electrónico (aparte de Mail) para utilizar el correo electrónico.
- Durante la transmisión de mensajes no se utiliza la conexión SSL.

Puede modificar la configuración especificada al agregar la cuenta.

Para agregar una cuenta de correo electrónico del usuario del dispositivo MDM de iOS:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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** de la sección **Cuenta de correo electrónico**.

   Se abrirá la ventana **Cuenta de correo electrónico**.
6. En el campo **Descripción**, introduzca una descripción de la cuenta de correo electrónico del usuario.
7. Seleccione el protocolo de correo electrónico:
   - **POP**
   - **IMAP**
8. Si fuera necesario, especifique prefijo de la ruta IMAP en el campo **Prefijo de la ruta IMAP**.

   El prefijo de la ruta IMAP debe introducirse en letras mayúsculas (por ejemplo, GMAIL para Google Mail). Este campo está disponible si el protocolo de la cuenta IMAP está seleccionado.
9. En el campo **Nombre del usuario tal y como aparece en los mensajes**, introduzca el nombre de usuario que se mostrará en el campo **De:** para todos los mensajes salientes.
10. En el campo **Dirección de correo electrónico**, especifique la dirección de correo electrónico del usuario del dispositivo MDM de iOS.
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, seleccione la casilla de verificación **Permitir el movimiento de mensajes entre cuentas**.
    - Para permitir la sincronización de las direcciones de correo electrónico utilizadas entre las cuentas de usuario, seleccione la casilla de verificación **Permitir la sincronización de las direcciones recientes**.

- Para permitir que un usuario utilice el servicio de buzón de correo para reenviar adjuntos de gran tamaño, seleccione la casilla **Permitir buzón de correo**.

- Para permitir que el usuario solo utilice el cliente de correo estándar de iOS, seleccione la casilla de verificación **Permitir solo el uso de la aplicación Correo**.

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 el correo saliente, seleccione la casilla **Firmar mensajes** y 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. Una firma del mensaje está disponible en dispositivos con la versión 10.3 de iOS o posterior.

    - Para usar el protocolo S/MIME para firmar correo saliente, seleccione la casilla **Cifrar mensajes de forma predeterminada** y seleccione un certificado para el cifrado (clave pública). El cifrado de mensajes está disponible para dispositivos con iOS de la versión 10.3 o posterior.

    - Para permitir que un usuario cifre mensajes particulares, seleccione la casilla **Mostrar botón para cifrar mensajes**. Para enviar mensajes cifrados, el usuario debe hacer clic en el icono en la aplicación de 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 definir la configuración de conexión del servidor:

    - **Dirección y puerto del servidor**: Nombres de hosts o direcciones IP de servidores de correo entrante y servidores de correo saliente, así como 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 los servidores de correo saliente.

    - **Contraseña**: Contraseña de la cuenta para la autenticación en el servidor de correo saliente protegido con el método de autenticación seleccionado.

    - **Utilizar una contraseña para servidores de correo entrante y saliente**: use una contraseña para la autenticación de usuarios en servidores de correo entrante y saliente.

    - **Utilizar conexión SSL**: Uso del protocolo de transferencia de datos SSL (capa de sockets seguros) que utiliza el cifrado y la autenticación basada en certificados para proteger la transmisión de datos.

14. Haga clic en **Aceptar**.

    Aparecerá la nueva cuenta de correo electrónico en la lista.

15. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Al hacerlo, una vez aplicada la directiva, las cuentas de correo electrónico de la lista compilada se agregarán al dispositivo móvil del usuario.

Configuración de un buzón de correo de Exchange en dispositivos MDM de iOS

Para que el usuario del dispositivo MDM de iOS pueda utilizar el correo electrónico corporativo, el calendario, los contactos, las notas y las tareas, agregue la cuenta de Exchange ActiveSync del usuario a Microsoft Exchange Server.

De forma predeterminada, se agrega a Microsoft Exchange Server una cuenta con la siguiente configuración:

- El correo electrónico se sincroniza una vez por semana.
- El usuario puede mover mensajes entre las cuentas de usuario y sincronizar direcciones de cuentas.
- El usuario puede utilizar cualquier cliente de correo electrónico (aparte de Mail) para utilizar el correo electrónico.
- Durante la transmisión de mensajes no se utiliza la conexión SSL.

Puede modificar la configuración especificada cuando agregue la cuenta de Exchange ActiveSync.

Para agregar una cuenta de Exchange ActiveSync del usuario del dispositivo MDM de iOS:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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** de la sección **Cuentas de Exchange ActiveSync**.

   Se abrirá la ventana **Cuenta de Exchange ActiveSync** en la pestaña **General**.
6. En el campo **Nombre de la cuenta**, introduzca el nombre de la cuenta para su autorización en Microsoft Exchange Server. Puede utilizar macros en la lista desplegable **Macros disponibles**.
7. En el campo **Dirección del servidor**, introduzca el nombre de red o a la dirección IP de Microsoft Exchange Server.
8. Para utilizar el protocolo de transferencia de datos SSL (capa de sockets seguros) para proteger la transmisión de datos, seleccione la casilla de verificación **Utilizar conexión SSL**.
9. En el campo **Dominio**, introduzca el nombre del dominio del dispositivo MDM de iOS del usuario. Puede utilizar macros en la lista desplegable **Macros disponibles**.
10. En el campo **Nombre de usuario de la cuenta**, introduzca el nombre del usuario del dispositivo MDM de iOS.

    Si deja este campo en blanco, Kaspersky Device Management for iOS solicitará al usuario que introduzca el nombre de usuario al aplicar la directiva en el dispositivo MDM de iOS. Puede utilizar macros en la lista desplegable **Macros disponibles**.
11. En el campo **Dirección de correo electrónico**, especifique la dirección de correo electrónico del usuario del dispositivo MDM de iOS. Puede utilizar macros en la lista desplegable **Macros disponibles**.
12. En el campo **Contraseña**, introduzca la contraseña de la cuenta de Exchange ActiveSync para su autorización en Microsoft Exchange Server.
13. Seleccione la ficha **Avanzado** y configure las opciones adicionales de la cuenta Exchange ActiveSync:
    - **Número de días para sincronizar el correo electrónico para <time period>**.
    - **Tipo de autenticación**.

- **Permitir el movimiento de mensajes entre cuentas**.
- **Permitir la sincronización de las direcciones recientes**.
- **Permitir solo el uso de la aplicación Correo**.

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 el correo saliente, seleccione la casilla **Firmar mensajes** y 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. Una firma del mensaje está disponible en dispositivos con la versión 10.3 de iOS o posterior.
    - Para usar el protocolo S/MIME para firmar correo saliente, seleccione la casilla **Cifrar mensajes de forma predeterminada** y seleccione un certificado para el cifrado (clave pública). El cifrado de mensajes está disponible para dispositivos con iOS de la versión 10.3 o posterior.
    - Para permitir que un usuario cifre mensajes particulares, seleccione la casilla **Mostrar botón para cifrar mensajes**. Para enviar mensajes cifrados, el usuario debe hacer clic en el icono en la aplicación de Correo en el campo **Para**.
15. Haga clic en **Aceptar**.

    Aparecerá la nueva cuenta de Exchange ActiveSync en la lista.
16. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Al hacerlo, una vez aplicada la directiva, las cuentas de Exchange ActiveSync de la lista compilada se agregarán al dispositivo móvil del usuario.

Configuración de un buzón de correo de Exchange en dispositivos Android (solo Samsung)

Para usar correo corporativo, contactos y el calendario en el dispositivo móvil, debería configurar los ajustes 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 que pertenecen los dispositivos de Android.
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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Gestionar Samsung KNOX → Gestionar dispositivos Samsung**.
5. En la ventana **Exchange ActiveSync**, haga clic en el botón **Configurar**.

   Se abrirá la ventana **Intercambiar configuración de servidor de correo electrónico**.
6. En el campo **Dirección del servidor**, introduzca la dirección IP o el nombre DNS del servidor que aloja el servidor de correo.

7. En el campo **Dominio**, introduzca el nombre de dominio del usuario del dispositivo móvil de la red corporativa.

8. En la lista desplegable **Intervalo de sincronización**, seleccione el intervalo deseado para la sincronización del dispositivo móvil con el servidor Microsoft Exchange Server.

9. Para utilizar el protocolo SSL (capa de sockets seguros) de transferencia de datos, seleccione la casilla de verificación **Utilizar conexión SSL**.

10. Para utilizar certificados digitales con el fin de proteger la transferencia de datos entre el dispositivo móvil y Microsoft Exchange Server, seleccione la casilla de verificación **Verificar certificado de 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 utilizar contenedores para supervisar la actividad de las aplicaciones iniciadas en el dispositivo móvil del usuario. *Un contenedor* es un depósito especial para aplicaciones móviles que posibilita el control de la actividad de la aplicación contenida, protegiendo así los datos personales y corporativos del usuario en el dispositivo.

En Kaspersky Security for Mobile Service Pack 3 Maintenance Release 2 no se puede crear contenedores para aplicaciones móviles. Sin embargo, los contenedores que se crearon en versiones anteriores de la aplicación se pueden añadir a dispositivos de Android.

Puede instalar una aplicación de un contenedor en el dispositivo del usuario de cualquiera de estas formas:

- Enviando al usuario un mensaje de correo electrónico con un vínculo al paquete de instalación de la aplicación en contenedor.

- Especificando una aplicación incluida en un contenedor como una aplicación necesaria o permitida en la sección **Control de aplicaciones** de la ventana de propiedades de la directiva. Cuando el dispositivo móvil se sincroniza con Kaspersky Security Center, el paquete de distribución de la aplicación en 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 su dispositivo y sus datos, después de instalar aplicaciones en contenedores, se recomienda prohibir la instalación de aplicaciones de orígenes desconocidos. Para obtener información sobre la instalación de aplicaciones sin Google Play, consulte la *Guía de ayuda de Android*.

Configurar notificaciones de Kaspersky Endpoint Security for Android

Si no desea que las notificaciones de Kaspersky Endpoint Security for Android distraigan al usuario del dispositivo móvil, puede desactivar 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 hay. 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, acciones a tomar cuando se detecta una amenaza).

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

Un usuario del dispositivo Android puede desactivar todas las notificaciones desde Kaspersky Endpoint Security for Android en la configuración de la barra de notificaciones. Si las notificaciones se desactivan, el usuario no supervisa el funcionamiento de la aplicación y puede perderse información importante (por ejemplo, información sobre fallos durante la sincronización del dispositivo con Kaspersky Security Center). En este caso, para comprobar el estado de funcionamiento de la aplicación, el usuario debe abrir Kaspersky Endpoint Security for Android.

Para configurar la visualización de notificaciones sobre el funcionamiento de Kaspersky Endpoint Security for Android:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al que pertenecen los dispositivos de Android.
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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Avanzado**.
5. En la sección **Notificaciones de la app**, haga clic en el botón **Configurar**.

   Se abre 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 for Android no mostrará problemas en la notificación de estado de protección ni en la sección **Estado** de la app. Kaspersky Endpoint Security for Android continuará mostrando las notificaciones de estado de protección y las notificaciones de la app.

   Algunos problemas de Kaspersky Endpoint Security for Android son obligatorios y no es posible desactivarlos (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 está en segundo plano**.

   Kaspersky Endpoint Security for 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 app (por ejemplo, cuando el usuario actualiza las bases de datos antivirus manualmente).

Los expertos de Kaspersky recomiendan activar las notificaciones y los mensajes emergentes. Si desactiva las notificaciones y los mensajes emergentes cuando la app está en segundo plano, la app 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 app.

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 de MDM de iOS a AirPlay

Configure la conexión a los dispositivos AirPlay para activar la transferencia de música, fotos y vídeos por streaming desde el dispositivo MDM de iOS a los dispositivos AirPlay. Para poder utilizar la tecnología AirPlay, el dispositivo móvil y el dispositivo AirPlay deben estar conectados a la misma red inalámbrica. Los dispositivos AirPlay incluyen dispositivos de Apple TV (de segunda y tercera generación), dispositivos AirPort Express, altavoces o equipos de radio compatibles con AirPlay.

La conexión automática a dispositivos AirPlay solo está disponible para los dispositivos controlados.

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

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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 de verificación **Aplicar configuración en el dispositivo**.
6. Haga clic en el botón **Agregar** de la sección **Contraseñas**.

   Se agregará una fila vacía a la tabla de contraseñas.
7. En la columna **Nombre del dispositivo**, introduzca el nombre del dispositivo AirPlay de la red inalámbrica.
8. En la columna **Contraseña**, introduzca la contraseña del dispositivo AirPlay.
9. Para restringir el acceso de los dispositivos MDM de iOS 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.

   No se permite el acceso a los dispositivos AirPlay que no están incluidos en la lista de dispositivos permitidos. Si se deja vacía la lista de dispositivos permitidos, Kaspersky Device Management for iOS permitirá el acceso a todos los dispositivos AirPlay.
10. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Al hacerlo, una vez aplicada la directiva, el dispositivo móvil del usuario se conectará automáticamente a dispositivos AirPlay para transmitir contenido multimedia por streaming.

Conexión de dispositivos de MDM de iOS a AirPrint

Para activar la impresión de documentos en el dispositivo MDM de iOS de forma inalámbrica mediante 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 de AirPrint.

Para configurar la conexión de un dispositivo MDM de iOS a una impresora AirPrint:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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** de la sección **Impresoras AirPrint**.

   Se abrirá la ventana **Impresora**.
6. En el campo **Dirección IP**, introduzca la dirección IP de la impresora AirPrint.
7. En el campo **Ruta de acceso del recurso**, introduzca la ruta de la impresora AirPrint.

   La ruta de acceso a la impresora corresponde a la clave "rp" (ruta de acceso del recurso) del protocolo Bonjour. Por ejemplo:

   - printers/Canon_MG5300_series
   - ipp/print
   - Epson_IPP_Printer
8. Haga clic en **Aceptar**.

   Aparecerá en la lista la impresora AirPrint recién agregada.
9. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Al hacerlo, una vez aplicada la directiva, el usuario del dispositivo móvil puede imprimir documentos de forma inalámbrica 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 las opciones 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.

Para configurar el Nombre de punto de acceso (APN):

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al que pertenecen los dispositivos de Android.
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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Gestionar Samsung KNOX → APN**.
5. En la sección **APN**, haga clic en el botón **Configurar**.

   Se abrirá la ventana **Configuración de APN**.
6. En la pestaña **General**, especifique la siguiente configuración de 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**, introduzca el código de país de telefonía móvil (MCC).
   d. En el campo **MNC**, introduzca el código de red de telefonía móvil (MNC).
   e. Si ha seleccionado **MMS** o **Internet y MMS** como tipo de punto de acceso, especifique la siguiente configuración adicional de MMS:
      - En el campo **Servidor de MMS**, especifique el nombre de dominio completo del servidor del operador de telefonía móvil utilizado para el intercambio de MMS.
      - En el campo **Servidor proxy de MMS**, especifique el nombre de red o la dirección IP del servidor proxy y número de puerto del servidor del operador de telefonía móvil usado para el intercambio de MMS.
7. En la pestaña **Avanzado**, configure las opciones avanzadas 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 del operador de telefonía móvil utilizado para el acceso a la red.
   b. En el campo **Dirección del servidor**, especifique el nombre de red del servidor del operador de telefonía móvil a través del cual se accede a los servicios de transmisión de datos.
   c. En el campo **Dirección del servidor proxy**, especifique el nombre de red o la dirección IP y el número de puerto del servidor proxy del operador de telefonía móvil utilizado para el acceso a la red.
   d. En el campo **Nombre de usuario**, introduzca el nombre de usuario para la autorización en la red de telefonía móvil.

e. En el campo **Contraseña**, introduzca la contraseña para la autorización del usuario en la red de telefonía 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 MDM de iOS

Es preciso configurar el Nombre de punto de acceso (APN) para activar el servicio de transmisión de datos de red móvil en el dispositivo MDM de iOS del usuario.

La sección **APN** está desfasada. Se recomienda configurar los ajustes de APN en la sección **Comunicaciones celulares**. Antes de configurar los ajustes de comunicaciones celulares, asegúrese de que la configuración de la sección **APN** no se haya aplicado en el dispositivo (la casilla **Aplicar configuración en el dispositivo** no debe estar seleccionada). La configuración de las secciones **APN** y **Comunicaciones celulares** no se puede utilizar simultáneamente.

Para configurar un punto de acceso en el dispositivo MDM de iOS de un usuario:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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 celulares**.

5. En la sección **Configuración de comunicaciones celulares**, seleccione la casilla de verificación **Aplicar configuración en el dispositivo**.

6. En la lista de **tipo de APN**, seleccione el tipo del punto del acceso para la transferencia de datos en una red móvil GPRS/3G/4G:

   - **APN integrado**: configuración de ajustes de comunicaciones celulares para la transferencia de datos a través de un operador de red móvil que admite la operación con la 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 ajustes de comunicaciones celulares para transferencia de datos a través del operador de red móvil de la tarjeta SIM insertada.

   - **APN integrado y APN**: configuración de ajustes de comunicaciones celulares para transferencia de datos a través del operador de red móvil de la tarjeta SIM insertada y la SIM de Apple integrada. Para obtener más información sobre dispositivos con SIM de Apple integrada y una ranura de tarjeta SIM, visite el sitio web 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 de usuario del dispositivo en el servidor del operador utilizado para acceder a la red (Internet y MMS):

9. En el campo **Nombre de usuario**, introduzca el nombre de usuario para la autorización en la red de telefonía móvil.

10. En el campo **Contraseña**, introduzca la contraseña para la autorización del usuario en la red de telefonía móvil.

11. En el campo **Dirección y puerto del servidor proxy**, introduzca el nombre de un host o la dirección IP de un servidor proxy y el número de puerto del servidor proxy.

12. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Al hacerlo, el nombre de punto de acceso (APN) quedará configurado en el dispositivo móvil del usuario una vez que se aplique la directiva.

Configuración del perfil de trabajo de Android

Esta sección contiene información sobre cómo trabajar con un perfil de trabajo de Android.

Acerca del 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 detalles sobre el uso de Android Enterprise, visite el sitio web de soporte técnico de Google.

Puede crear el perfil de trabajo de Android (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 apps 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 apps corporativas: Google Play Market, Google Chrome, Descargas, Kaspersky Endpoint Security for Android, entre otras. Las apps corporativas instaladas en el perfil de trabajo y las notificaciones de estas apps se marcan con el icono . Debe crear una cuenta corporativa de Google separada para la app Google Play Market. Las apps instaladas en el perfil de trabajo aparecen en la lista común de apps.

Configuración del perfil de trabajo

Para establecer la configuración del perfil de trabajo de Android:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccione el grupo de administración al que pertenecen los dispositivos de Android.

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 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. Especifique la configuración del perfil de trabajo:

- Para activar el Control de aplicaciones en el perfil de trabajo de Android y desactivarlo en el perfil personal, seleccione la casilla de verificación **Activar control de aplicaciones solo en perfil de trabajo**.

  En la sección **Usuarios**, puede seleccionar **Control de aplicaciones** 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 activar la Protección web para Google Chrome en el perfil de trabajo y desactivarla en el perfil personal, en el espacio de trabajo de la sección **Perfil de trabajo de Android**, seleccione la casilla **Activar Protección web solo en perfil de trabajo**.

  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, desactive la opción **Activar Protección web solo en perfil de trabajo**. Si esta opción está activada, la Protección web para el Navegador de Samsung no se ejecuta. La Protección web en el perfil de trabajo está desactivada de forma predeterminada.

  > La Protección Web en dispositivos de Android solo funciona en el navegador Google Chrome y en el Navegador de Samsung.

  Puede definir la configuración de acceso a sitios web (cree 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 a través del portapapeles de aplicaciones del perfil de trabajo en aplicaciones personales, seleccione la casilla **Prohibir transferencia de datos de perfil de trabajo a perfil personal**.

- Para impedir que el usuario utilice el modo de depuración de USB en el dispositivo móvil con el perfil de trabajo, seleccione la casilla **Prohibir la activación del modo de depuración de 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 de todos los orígenes excepto Google Play, seleccione la casilla de verificación **Prohibir la instalación de aplicaciones en el perfil de trabajo de orígenes desconocidos**.

- Para prohibir al usuario eliminar aplicaciones desde el perfil de trabajo de Android, seleccione la casilla de verificación **Prohibir la eliminación de aplicaciones del perfil de trabajo**.

7. Para establecer la configuración del perfil de trabajo 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. El espacio del dispositivo móvil del usuario se divide en un perfil de trabajo y un perfil personal.

Adición de una cuenta de LDAP

Para permitir al usuario del dispositivo MDM de iOS acceder a los contactos corporativos en el servidor LDAP, agregue la cuenta de LDAP.

Para agregar una cuenta de LDAP del usuario del dispositivo MDM de iOS:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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 de LDAP**.

   Se abrirá la ventana **Cuenta LDAP**.

6. En el campo **Descripción**, introduzca una descripción de la cuenta de LDAP del usuario. Puede utilizar macros en la lista desplegable **Macros disponibles**.

7. En el campo **Nombre de la cuenta**, introduzca el nombre de la cuenta para su autorización en el servidor LDAP. Puede utilizar macros en la lista desplegable **Macros disponibles**.

8. En el campo **Contraseña**, introduzca la contraseña de la cuenta de LDAP para su autorización en el servidor LDAP.

9. En el campo **Dirección del servidor**, introduzca el nombre de dominio del servidor LDAP. Puede utilizar macros en la lista desplegable **Macros disponibles**.

10. Para utilizar el protocolo de transferencia de datos SSL (capa de sockets seguros) para proteger la transmisión de mensajes, seleccione la casilla de verificación **Utilizar conexión SSL**.

11. Compile una lista de consultas de búsqueda para el acceso del usuario del dispositivo móvil MDM de iOS a los datos corporativos en el servidor LDAP:

    a. Haga clic en el botón **Agregar** de la sección **Buscar configuración**.

       Aparecerá una fila en blanco en la tabla con consultas de búsqueda.

    b. En la columna **Nombre**, introduzca el nombre de una consulta de búsqueda.

    c. En la columna **Alcance de la 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 a partir de la carpeta base.
       - **Árbol secundario**: búsqueda en las carpetas de todos los niveles de anidamiento a partir de la carpeta base.

    d. En la columna **Base de la búsqueda**, introduzca la ruta de la carpeta en el servidor LDAP con que comience la búsqueda (por ejemplo: "ou=personas", "o=ejemplo corporativo").

    e. Repita los pasos a-d con todas las consultas de búsqueda que desee agregar al dispositivo MDM de iOS.

12. Haga clic en **Aceptar**.

    Aparecerá la nueva cuenta de LDAP en la lista.

13. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Al hacerlo, una vez aplicada la directiva, las cuentas de LDAP de la lista compilada se agregarán al dispositivo móvil del usuario. El usuario puede acceder a los contactos corporativos en las aplicaciones de iOS estándares: Contactos, Mensajes y Mail.

Adición de una cuenta de calendario

Para permitir al usuario del dispositivo MDM de iOS acceder a sus eventos de calendario del servidor CalDAV, agregue la cuenta de CalDAV. La sincronización con el servidor de CalDAV permite al usuario crear y recibir invitaciones, recibir actualizaciones de eventos y sincronizar tareas con la aplicación Recordatorios.

Para agregar una cuenta de CalDAV del usuario del dispositivo MDM de iOS:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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**, seleccione la sección **Calendario**.
5. Haga clic en el botón **Agregar** de la sección **Cuentas de CalDAV**.

   Se abrirá la ventana **Cuenta de CalDAV**.
6. En el campo **Descripción**, introduzca una descripción de la cuenta de CalDAV del usuario.
7. En el campo **Dirección y puerto del servidor**, introduzca el nombre de un host o la dirección IP de un servidor CalDAV y el número de puerto del servidor CalDAV.
8. En el campo **URL principal**, especifique la URL de la cuenta de CalDAV del usuario del dispositivo MDM de iOS en el servidor CalDAV (por ejemplo: http://ejemplo.com/caldav/usuarios/miempresa/usuario).

   La URL debe comenzar con `"http://"` o `"https://"`.
9. En el campo **Nombre de la cuenta**, introduzca el nombre de la cuenta para su autorización en el servidor CalDAV.
10. En el campo **Contraseña**, configure la contraseña de la cuenta de CalDAV para su autorización en el servidor CalDAV.
11. Para utilizar el protocolo de transferencia de datos SSL (capa de sockets seguros) para proteger la transmisión de datos de eventos entre el servidor CalDAV y el dispositivo móvil, seleccione la casilla de verificación **Utilizar conexión SSL**.
12. Haga clic en **Aceptar**.

    Aparecerá la nueva cuenta de CalDAV en la lista.
13. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Al hacerlo, una vez aplicada la directiva, las cuentas de CalDAV de la lista compilada se agregarán al dispositivo móvil del usuario.

Adición de una cuenta de un contacto

Para permitir al usuario del dispositivo MDM de iOS sincronizar datos con el servidor CardDAV, agregue la cuenta de CardDAV. La sincronización con el servidor CardDAV permite al usuario acceder a los detalles de contactos de cualquier dispositivo.

Para agregar una cuenta de CardDAV del usuario del dispositivo MDM de iOS:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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**, seleccione la sección **Contactos**.
5. Haga clic en el botón **Agregar** de la sección **Cuentas de CardDAV**.

   Se abrirá la ventana **Cuenta de CardDAV**.
6. En el campo **Descripción**, introduzca una descripción de la cuenta de CardDAV del usuario. Puede utilizar macros en la lista desplegable **Macros disponibles**.
7. En el campo **Dirección y puerto del servidor**, introduzca el nombre de un host o la dirección IP de un servidor CardDAV y el número de puerto del servidor CardDAV.
8. En el campo **URL principal**, especifique la URL de la cuenta de CardDAV del usuario del dispositivo MDM de iOS en el servidor CardDAV (por ejemplo: http://ejemplo.com/carddav/usuarios/miempresa/usuario).

   La URL debe comenzar con `"http://"` o `"https://"`.
9. En el campo **Nombre de la cuenta**, introduzca el nombre de la cuenta para su autorización en el servidor CardDAV. Puede utilizar macros en la lista desplegable **Macros disponibles**.
10. En el campo **Contraseña**, configure la contraseña de la cuenta de CardDAV para su autorización en el servidor CardDAV.
11. Para utilizar el protocolo de transferencia de datos SSL (capa de sockets seguros) para proteger la transmisión de contactos entre el servidor CardDAV y el dispositivo móvil, seleccione la casilla de verificación **Utilizar conexión SSL**.
12. Haga clic en **Aceptar**.

    Aparecerá la nueva cuenta de CardDAV en la lista.
13. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Al hacerlo, una vez aplicada la directiva, las cuentas de CardDAV de la lista compilada se agregarán al dispositivo móvil del usuario.

Configuración de la suscripción al calendario

Para permitir al usuario del dispositivo MDM de iOS agregar eventos de calendarios compartidos (como el calendario corporativo) al calendario del usuario, agregue la suscripción a dicho calendario. Los *calendarios compartidos* son calendarios de otros usuarios que tienen una cuenta de CalDAV, calendarios iCal y otros calendarios abiertamente publicados.

Para agregar la suscripción al calendario:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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**, seleccione la sección **Suscripción al calendario**.

5. Haga clic en el botón **Agregar** de la sección **Suscripciones a calendarios**.

   Se abrirá la ventana **Suscripción al calendario**.

6. En el campo **Descripción**, introduzca una descripción de la suscripción al calendario.

7. En el campo **Dirección web del servidor**, especifique la URL de un calendario de terceros.

   En este campo, puede introducir la URL del correo de la cuenta de CalDAV del usuario a cuyo calendario se está suscribiendo. También puede especificar la URL de un calendario iCal u otro calendario abiertamente publicado.

8. En el campo **Nombre de usuario**, indique el nombre de la cuenta de usuario para autenticarse en el servidor del calendario de terceros.

9. En el campo **Contraseña**, introduzca la contraseña de la suscripción al calendario para autenticarse en el servidor del calendario de terceros.

10. Para utilizar el protocolo de transferencia de datos SSL (capa de sockets seguros) para proteger la transmisión de datos de eventos entre el servidor CalDAV y el dispositivo móvil, seleccione la casilla de verificación **Utilizar conexión SSL**.

11. Haga clic en **Aceptar**.

12. Aparecerá la nueva suscripción al calendario en la lista.

13. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

    Al hacerlo, una vez aplicada la directiva, los eventos del calendario compartido de la lista se agregarán al calendario del dispositivo móvil del usuario.

Adición de clips web

Un *clip web* es una aplicación que abre un sitio web en la pantalla principal del dispositivo móvil MDM de iOS. Al hacer clic en los iconos de clips web de la pantalla principal del dispositivo, el usuario puede abrir sitios web rápidamente (como el sitio web corporativo). Puede agregar clips web a dispositivos de usuario y configurar el aspecto de los iconos de los clips web mostrados en pantalla.

De forma predeterminada, se aplican las siguientes restricciones de uso de clips web:

- El usuario no puede eliminar clips web manualmente del dispositivo móvil.
- Los sitios web que se abren cuando el usuario hace clic en un icono de clip web no se abren en el modo de pantalla completa.
- A los iconos de clip web de la pantalla se les aplican efectos visuales como el redondeo de esquinas, sombras y brillo.

Para agregar un clip web al dispositivo MDM de iOS de un usuario:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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 **Clips web**.
5. Haga clic en el botón **Agregar** de la sección **Clip web**.

   Se abrirá la ventana **Clip web**.
6. En el campo **Nombre**, introduzca el nombre del clip web que desee mostrar en la pantalla principal del dispositivo MDM de iOS.
7. En el campo **URL**, introduzca la dirección web del sitio web que se abrirá al hacer clic en el icono del clip web. La dirección debe comenzar con `"http://"` o `"https://"`.
8. Para permitir al usuario desinstalar un clip web en el dispositivo MDM de iOS, seleccione la casilla de verificación **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 mostrará en la pantalla principal del dispositivo móvil MDM de iOS. La imagen debe cumplir los siguientes requisitos:

   - Tamaño de la imagen no superior a 400 × 400 píxeles.
   - Formato de archivo: GIF, JPEG o PNG.
   - Tamaño de archivo no superior a 1 MB.

   El icono del clip web está disponible para su previsualización en el campo **Icono**. SI no selecciona una imagen para el clip web, el icono será un cuadrado en blanco.

   Si desea que el icono del clip web se muestre sin efectos visuales especiales (redondeo de esquinas del icono y efecto brillo), seleccione la casilla de verificación **Icono precompuesto**.
10. Si desea que el sitio web se abra en el modo de pantalla completa en el dispositivo MDM de iOS al hacer clic en el icono, seleccione la casilla de verificación **Clip web en pantalla completa**.
11. Haga clic en **Aceptar**.

    Aparecerá el nuevo clip web en la lista.
12. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Al hacerlo, una vez aplicada la directiva, los iconos de clips web de la lista que ha creado se agregarán a la pantalla principal del dispositivo móvil del usuario.

Adición de fuentes

Para agregar una fuente al dispositivo MDM de iOS de un usuario:

1. En el árbol de la consola, en la carpeta **Dispositivos administrados**, seleccionan el grupo de administración al cual los dispositivos 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**, seleccione la sección **Fuentes**.
5. Haga clic en el botón **Agregar** de la sección **Fuentes**.

   Se abrirá la ventana **Fuente**.
6. En el campo **Nombre de archivo**, especifique la ruta del archivo de fuente (un archivo con la extensión .ttf o .otf).

   Las fuentes con la extensión "ttc" u "otc" no son compatibles.

   Las fuentes se identifican mediante el nombre PostScript. No instale fuentes con el mismo nombre PostScript, incluso si su contenido es distinto. La instalación de fuentes con el mismo nombre PostScript generará un error no definido.
7. Haga clic en **Abrir**.

   Aparecerá la nueva fuente en la lista.
8. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

Al hacerlo, una vez aplicada la directiva, se solicitará al usuario que instale fuentes de la lista que se ha creado.

Administración de la aplicación mediante el uso de los sistemas EMM de terceros (solo Android)

Puede utilizar la aplicación Kaspersky Endpoint Security for Android sin sistemas de administración de Kaspersky. Utilice soluciones de otros proveedores de servicios de EMM (administración de movilidad empresarial) para instalar y administrar la aplicación Kaspersky Endpoint Security for Android. Kaspersky participa en la Comunidad AppConfig para garantizar que la app funcione con soluciones de EMM de terceros.

Puede administrar la aplicación Kaspersky Endpoint Security for Android a través de soluciones EMM de terceros solo en dispositivos con Android.

Puede utilizar soluciones de EMM de terceros para instalar la aplicación Kaspersky Endpoint Security for Android solamente. Conecte el dispositivo a Kaspersky Security Center y administre la aplicación en la Consola de administración. En este caso, la administración de la aplicación Kaspersky Endpoint Security for Android en la consola de EMM no estará disponible.

Si ha instalado la aplicación Kaspersky Endpoint Security for Android con un sistema de EMM de terceros, es imposible administrar la aplicación en Kaspersky Endpoint Security Cloud. Puede administrar la aplicación Kaspersky Endpoint Security for Android en la consola de EMM.

Las siguientes soluciones de EMM son compatibles con el uso de la aplicación Kaspersky Endpoint Security for Android:

- VMware AirWatch
- MobileIron
- IBM Maas360
- Microsoft Intune
- SOTI MobiControl

Puede realizar las siguientes acciones en la consola de EMM:

- Implementar la aplicación a un perfil de trabajo de Android en los dispositivos de los usuarios.
- Activar la aplicación.
- Especificar la configuración adicional:
  - Activar protección contra sitios web maliciosos y de phishing en Internet.
  - Configure los parámetros para conectar el dispositivo a Kaspersky Security Center.
  - Ajustar la configuración de Antirrobo.
  - Configurar la planificación para ejecutar un análisis de virus en el dispositivo.
  - Activar la detección de software publicitario y aplicaciones que pueden utilizar los delincuentes para dañar el dispositivo del usuario o sus datos personales.
  - Configurar la programación para actualizaciones de la base de datos de aplicaciones.

Primeros pasos

Para implementar la aplicación en los dispositivos móviles de los usuarios, debe añadir Kaspersky Endpoint Security for Android a la tienda de aplicaciones de EMM. Puede añadir Kaspersky Endpoint Security for Android a la tienda de apps de EMM usando un enlace de Google Play. Para obtener más información sobre el funcionamiento con aplicaciones en la consola de EMM, visite el *sitio web del Soporte Técnico del proveedor de servicios de EMM*.

La aplicación Kaspersky Endpoint Security for Android se implementa en un perfil de trabajo de Android. La aplicación se aísla de los datos personales del usuario y protege únicamente los datos corporativos en el perfil de trabajo. Se recomienda asegurarse de que Kaspersky Endpoint Security for Android esté protegida contra la eliminación por herramientas de la consola EMM.

Cómo instalar la aplicación

Según la consola de EMM, seleccione el método para instalar la aplicación en los dispositivos: instalación silenciosa, enviar un correo electrónico con un enlace 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 está ejecutando el antivirus (solo para Android 6.0 o versiones posteriores).
- Permiso telefónico para identificar el dispositivo, por ejemplo, al activar la aplicación.
- Solicitud de añadir Kaspersky Endpoint Security for Android a la lista de aplicaciones que se inician en el arranque del sistema operativo (en ciertos dispositivos, como Huawei, Meizu y Xiaomi). Si no se muestra la solicitud de añadir, añada manualmente Kaspersky Endpoint Security for Android a la lista de aplicaciones de inicio. Puede que no muestre la solicitud si la aplicación de seguridad no está instalada en el perfil de trabajo.

Puede conceder los permisos requeridos en la consola EMM antes de instalar la aplicación Kaspersky Endpoint Security for Android. Para obtener más información sobre cómo conceder permisos en la consola de EMM, visite *el sitio web del Soporte Técnico del proveedor de servicios de EMM*. También puede conceder los permisos mientras completa el Asistente de Configuración Inicial de Kaspersky Endpoint Security for Android en el dispositivo.

La aplicación Kaspersky Endpoint Security for Android se instalará en el perfil de trabajo de Android.

Para que la Protección Web funcione, debe configurar también un servidor proxy en la configuración Google Chrome:

- Modo de configuración del servidor proxy: manual.
- Dirección y puerto del servidor proxy: 127.0.0.1:3128.
- Soporte del protocolo SPDY: desactivado.
- Compresión de datos a través de servidor proxy: desactivada.

Cómo activar la aplicación

La información sobre la licencia se transmite al dispositivo móvil junto con otros ajustes 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 la evaluación expira. Cuando caduca la licencia de evaluación, se desactivan todas las funciones de la aplicación móvil Kaspersky Endpoint Security for 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 for Android no están disponibles). Para seguir utilizando todas las funciones de la aplicación, es preciso renovar la licencia comercial.

Para activar Kaspersky Endpoint Security for Android:

1. En la consola de EMM, abra la configuración de la aplicación Kaspersky Endpoint Security for Android.
2. En el campo `LicenseActivationCode`, introduzca el código de activación de la aplicación.

   Para activar la aplicación en un dispositivo, debe tener acceso a los servidores de activación de Kaspersky.

Cómo conectar un dispositivo a Kaspersky Security Center

Una vez que se ha instalado Kaspersky Endpoint Security for Android en un dispositivo móvil, el dispositivo puede conectarse a Kaspersky Security Center. Los datos necesarios para la conexión del dispositivo a Kaspersky Security Center se transmiten al dispositivo móvil junto con los otros ajustes mencionados en el archivo de configuración. Tras conectar el dispositivo a Kaspersky Security Center, pueden utilizarse directivas de grupo para configurar la aplicación de forma centralizada. También es posible recibir informes y estadísticas de rendimiento de Kaspersky Endpoint Security for Android.

Antes de conectar un dispositivo a Kaspersky Security Center, asegúrese de que estén dadas las siguientes condiciones:

- El complemento de administración de Kaspersky Endpoint Security for Android está instalado en la estación de trabajo del administrador.
- El puerto para la conexión de dispositivos móviles esté abierto en las propiedades del servidor de administración.
- La visualización de la carpeta **Administración del dispositivo móvil** está activada en la consola de administración.
- Se haya creado en el almacenamiento de certificados de Kaspersky Security Center un certificado general para identificar al usuario del dispositivo móvil.

Antes de conectar un dispositivo a Kaspersky Security Center, se recomienda hacer lo siguiente:

- Si desea crear tareas y directivas 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 for Android de manera centralizada, cree una directiva de grupo.

Para conectar un dispositivo a Kaspersky Security Center:

1. En la consola de EMM, abra la configuración de la aplicación Kaspersky Endpoint Security for Android.
2. En el campo `KscServer`, introduzca 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 el usuario se distraiga con las notificaciones de Kaspersky Endpoint Security for Android, desactive las notificaciones de la aplicación. Para hacerlo, establezca la configuración `DisableNotification = True`.

   Después de conectarse, la aplicación muestra todas las notificaciones. Es posible desactivar determinadas notificaciones de la aplicación en la configuración de la directiva.

   No desactive las notificaciones de la aplicación si no utiliza Kaspersky Security Center. Esto podría hacer que un usuario no reciba notificaciones sobre la caducidad de la licencia. En consecuencia, la aplicación dejará de realizar sus funciones.

Una vez que las opciones de conexión estén configuradas, Kaspersky Endpoint Security for Android mostrará una notificación que solicitará 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.

Dadas las características específicas de un perfil de trabajo de Android (ausencia del servicio de accesibilidad), las funciones de Control de aplicaciones 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 ha creado una regla para mover dispositivos automáticamente a un grupo de administración, el dispositivo se añadirá automáticamente a la carpeta **Dispositivos no asignados**. Si se ha creado una regla para mover dispositivos automáticamente a un grupo de administración, el dispositivo se añadirá 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 existe) o ID de dispositivo]

Un ID de dispositivo es un ID único que genera Kaspersky Endpoint Security for Android a partir de los datos que recibe de un dispositivo. Para los dispositivos móviles con Android 10 o versiones posteriores, Kaspersky Endpoint Security for Android utiliza el SSAID (ID de Android) o la suma de comprobación de otros datos que recibe del dispositivo. Para las versiones anteriores de Android, la aplicación utiliza el IMEI. Puede configurar el formato de nombre de dispositivo en la política de grupos. También puede añadir 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 añadir la etiqueta al nombre del dispositivo:

1. En la consola de EMM, abra la configuración de la aplicación Kaspersky Endpoint Security for 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 añadir algunos valores (por ejemplo, `{DeviceSerialNumber} {DeviceUid}`). La etiqueta se añadirá 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 se conecta a Kaspersky Security Center, la configuración de la aplicación se modifica según la directiva de grupo. Kaspersky Endpoint Security for Android ignora la configuración de la aplicación del archivo de configuración de la Consola EMM. Es posible configurar todas las secciones de la directiva excepto las siguientes:

- **Antirrobo** (Bloqueo del dispositivo)
- **Contenedores**
- **Administración del dispositivo** (Bloqueo de pantalla)
- **Control de aplicaciones** (Bloqueo de aplicaciones bloqueadas)
- **Perfil de trabajo de Android**
- **Gestionar Samsung KNOX**

Como consecuencia del método utilizado para desplegar un perfil de trabajo, no es posible aplicar la configuración de la directiva de grupo desde la sección **Perfil de trabajo de Android**. Esta configuración puede aplicarse únicamente 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.

Ajustes del archivo de configuración

Clave de configuración	Descripción	Tipo	Value
`LicenseActivationCode`	Código de activación de la aplicación	String	Código de activación de la app formadc por 20 letras latinas y números. Para activar la aplicación con un código de activación, se necesita contar con acceso 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 evaluación. La licencia de evaluación es válida durante 30 días. Cuando caduca l licencia de evaluación, se desactivan todas las funciones de la aplicación móv Kaspersky Endpoint Security for 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 contar co acceso a Internet para conectarse a los servidores de Kaspersky. Si selecciona `Declined`, la aplicación le pedirá al usuario que acepte los términc y las condiciones del EULA. Los usuarios del dispositivo móvil pueden aceptar las condiciones en el Asistente de configuración inicial.
`EulaAcceptanceCodeV1`	Código del Contrato de licencia	String	Esta configuración solo está disponible para VMware AirWatch. 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 enlace del Contrato de licencia (`EulaAcceptanceConfirmationV1` de la Consola de EMM. 2. Pegue el enlace 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
`EulaAcceptanceCodesV2`	Códigos del Contrato de licencia	String	

			Contrato de licencia. Para aceptar los términos y las condiciones de los EULA para todos los dispositivos móviles, debe contar con acceso a Internet para 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. Introduzca la dirección como se indica a continuación: `<server address>:<port>`. Si ingresa la dirección del servidor, pero no especifica el puerto, la aplicación utilizará el puerto predeterminado 13292.
`DisableNotification`	Desactive las notificaciones de la aplicación antes de conectarse a Kaspersky Security Center	Boolean	`True`: Kaspersky Endpoint Security for Android oculta todas las notificaciones de la aplicación. Kaspersky Endpoint Security for Android oculta las notificaciones hasta que el dispositivo s conecta a Kaspersky Security Center. Después de conectarse, la aplicación muestra todas las notificaciones. Es posible desactivar determinadas notificaciones de la aplicación en la configuración de la directiva. No desactive las notificaciones de la aplicación si no utiliza Kaspersky Security Center. Esto podría hacer que un usuario no vea las notificaciones sobre la caducidad de la licencia. En este caso, la aplicación dejaría de funcionar. `False` - Kaspersky Endpoint Security for 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 la hora de inicio de análisis (`ScanScheduleTime`). `Weekly` – Inicia un análisis antivirus una vez por semana. Seleccione el día de la semana para iniciar un análisis antivirus (`ScanScheduleDay`) y configure la hora (`ScanScheduleTime`). `Off` – Se deshabilita el inicio automático de un análisis antivirus. Independientemente del valor configurado, el usuario del dispositivo puede iniciar manualmente un análisis antivirus.
`ScanScheduleDay`	Día de análisis	Choice	`Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday` Puede seleccionar un solo valor para este parámetro.
`ScanScheduleTime`	Hora del análisis	String	La hora se puede indicar en formato de 24 horas (por ejemplo, 13:00) o formato de 12 horas (por ejemplo, 10:30 P.M.).
`ScanScheduleLock`	Bloquear la configuración del modo de ejecución de análisis	Boolean	`True` – El usuario no puede acceder a la configuración del modo de ejecución de análisis antivirus en la configuración de la aplicación. `False` – El usuario puede configurar el modo de ejecución del análisis antivirus y, por ejemplo, deshabilitar el inicio automático de un análisis antivirus.
`ScanOnlyExecutableFiles`	Tipos de archivos para analizar (Análisis antivirus)	Choice	`AllFiles` – Analiza todos los archivos. `OnlyExecutables` – Solo analiza archivos ejecutables. Los archivos ejecutables son archivos con las extensiones .apk (.zip), .dex o .so. En Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 1, no puede habilitar el análisis de archivos ejecutables únicamente.
`ScanArchives`	Analizar archivos comprimidos y descomprimirlos	Boolean	`True` – La aplicación descomprime archivos comprimidos y analiza su contenido. `False` – La aplicación solo analiza los archivos comprimidos. La aplicación solo analiza archivos comprimidos con extensión .zip (.apk).

			En Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 1, no puede deshabilitar el análisis del contenido de los archivos comprimidos.
`ScanActionOnThreatFound`	Acción al detectar amenazas (Análisis antivirus)	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 los objetos detectados. `Skip` – La aplicación deja los objetos detectados sin alterar. Si los objetos detectados se han omitido, Kaspersky Endpoint Security for Android advierte 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 abrir), la aplicación bloquea el acceso al objeto. `AskUser` – La aplicación solicita al usuario seleccionar una acción para cada objeto detectado: omitir, poner en cuarentena o eliminar. Cuando se detectan varios objetos, el usuario puede aplicar una acción seleccionada a todos los objetos. La información sobre amenazas detectadas y las acciones realizadas en ellos se registra en los informes de la aplicación.
`ScanLock`	Bloquear los ajustes de la configuración del 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 comprimidos y la acción a tomar 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 software publicitario, marcadores automáticos y aplicaciones que los delincuentes pueden utilizar para dañar el	Boolean	`True`: la aplicación detecta el software publicitario y otras aplicaciones que los delincuentes pueden utilizar para dañar el dispositivo y los datos del usuario. `False`: la aplicación omite el software publicitario y otras aplicaciones que los delincuentes pueden utilizar para dañar el dispositivo y los datos del usuario.

	dispositivo y los datos del usuario		
`ProtectionMode`	Modo de protección en tiempo real	Choice	`Recommended` – La aplicación analiza solo nuevas aplicaciones una vez inmediatamente después de que se han instalado, así como archivos desde la carpeta Descargas. `Extended` – La aplicación analiza todos los archivos que el usuario abre, modifica, copia, ejecuta y guarda en el dispositivo. La aplicación también analiz nuevas aplicaciones y archivos desde la carpeta Descargas. `Disabled`: la protección en tiempo real está desactivada.
`UseKsnMode`	Modo Kaspersky Security Network	Choice	`Recommended` – La aplicación cambia datos con Kaspersky Security Network (KSN). Kaspersky Endpoint Security for Android usa KSN para la protección en tiempo real del dispositivo contra amenazas (Protección en la nube) y para el funcionamiento de la 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 for Android. Esta información hace posible llevar un seguimiento de amenazas en tiempo real. No se recopila, se procesa r almacena ningún dato personal por part de los servicios de KSN. `Disabled` – La aplicación no usa datos de Kaspersky Security Network. No puede activar la Protección Web (`EnableWebFilter`). El componente de 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 las extensiones .apk (.zip), .dex o .so. En Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 1, no puede habilitar el análisis d archivos ejecutables únicamente.
`ProtectionActionOnThreatFound`	Acción al detectar amenazas	Choice	`Quarantine` – La aplicación pone objetos detectados en cuarentena. La cuarentena almacena los archivos como

	(Protección en tiempo real)		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 objetos detectados. `Skip` – La aplicación deja los objetos detectados sin alterar. Si los objetos detectados se han omitido, Kaspersky Endpoint Security for Android advierte 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. La información sobre amenazas detectadas y las acciones realizadas en ellos se registra en los informes de la aplicación.
`ProtectionLock`	Bloquear el ajuste de la configuración de la protección en tiempo real	Boolean	`True` – El usuario no puede acceder a la siguiente configuración de la protección en tiempo real en la configuración de la aplicación: modo de protección en tiempo real, tipos de archivos para analizar, y la acción que se tomará cuando se detecte 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 la actualización de bases de datos	Choice	`Daily` – Comprueba nuevas bases de datos antivirus y la descarga a los dispositivos una vez al día. Configure la hora de inicio de la actualización de la base de datos `(UpdateScheduleTime)`. `Weekly` – Comprueba nuevas bases de datos antivirus y la descarga a dispositivos una vez por semana. Seleccione el día de la semana para iniciar la actualización de la base de datos `(UpdateScheduleDay)` y configure la hora (`UpdateScheduleTime`). `Off` – Se deshabilita la actualización automática de bases de datos del antivirus. Sea cual sea el valor establecido, el usuario puede actualizar manualmente las bases de datos antivirus.
`UpdateScheduleDay`	Día para iniciar actualización de la base de datos	Choice	`Monday / Tuesday / Wednesday / Thursday / Friday / Saturday /`

			`Sunday` Puede seleccionar un solo valor para este parámetro.
`UpdateScheduleTime`	Hora de inicio de la actualización de la base de datos	String	La hora se puede indicar en formato de 24 horas (por ejemplo, 13:00) o formato de 12 horas (por ejemplo, 10:30 P.M.).
`UpdateScheduleLock`	Bloquear la configuración del modo de ejecución de la 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, deshabilita el inicio automático de las actualizaciones de la base de datos de antivirus.
`AllowUpdateInRoaming`	Actualizar bases de datos en itinerancia	Boolean	`True` – La aplicación descarga bases de datos antivirus si el dispositivo está en la zona de 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 web maliciosos y de phishing en Internet. Protección web solo es compatible con Google Chrome. Se permite que los sitios web maliciosos y de phishing que utilizan el protocolo HTTPS permanezcan desbloqueados si el dominio es de confianza. Si el dominio no es de confianza, 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 de Protección Web funcione, deben cumplirse las siguientes condiciones: • Los usuarios del dispositivo aceptan la Política de privacidad y la Declaración de protección web en el Asistente de configuración inicial o en la configuración de la aplicación.

			• Hay configurado un servidor proxy e 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 eliminar la aplicación Kaspersky Endpoint Security for Android del dispositivo móvil, restablezca la configuración del servidor proxy. • El uso de KSN se activa en la configuración de la aplicación: `UseKsnMode = Recommended` o `UseKsnMode = Extended`. • Se recomienda seleccionar Google Chrome como navegador predeterminado en la configuración del sistema operativo.
`EnableWebFilterLock`	Bloquear configuración de la 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, desactivar la protección contra sitios web maliciosos y de phishing en Internet.
`UpdateServer`	Dirección del servidor del origen 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 for Android utilizará los servidores de actualizaciones 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 for Android a los servicios de Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics. Estos datos son necesarios para mejora 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 acces a los datos y su protección están regulados por las correspondientes condiciones de uso de los servicios de Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics. `False`: se desactiva el envío de datos a 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 añadirá 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 del dispositivo (UDID). • `{DeviceAssetNumber}` – Número de activo del dispositivo. Este núme se crea internamente dentro de su organización. Puede añadir 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. Luego, 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 serán ignorados.

Carga de la 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
Implementación inicial de la aplicación, MB	0,08	17,76	17,84
Actualización inicial de las bases de datos antivirus (el volumen de tráfico puede variar 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 regular de las bases de datos antivirus (el volumen de tráfico puede variar debido al tamaño de las bases de datos antivirus), MB	0,08	3,06	3,14
Ejecución de comandos Antirrobo. Localizar el dispositivo (el volumen de tráfico puede variar debido a las especificaciones de la cámara integrada y a 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 diario medio, MB	0,22	6,96	7,18

Participación en Kaspersky Security Network

Para proteger dispositivos móviles con mayor eficacia, Kaspersky Endpoint Security for Android utiliza datos recopilados de usuarios de todo el mundo. *Kaspersky Security Network* se ha diseñado para procesar dichos datos.

Kaspersky Security Network (KSN) es una infraestructura de servicios en la nube que proporciona acceso a la base de conocimiento en línea de Kaspersky con información sobre la reputación de los archivos, los recursos web y el 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 de Kaspersky Endpoint Security for Android. La participación 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 hace posible llevar un seguimiento de amenazas en tiempo real. Los archivos o las partes de archivos que pueden ser aprovechados por intrusos para dañar el equipo o el contenido del usuario también se pueden enviar a Kaspersky para ser examinados.

Se requiere Kaspersky Security Network para el uso de Kaspersky Endpoint Security for Android. KSN se utiliza en los componentes principales de la aplicación: Antivirus, Protección Web y Control de aplicaciones. Si se rechaza la participación en KSN, se reduce el nivel de protección, con riesgo de infección del dispositivo y pérdida de datos. Para empezar a usar Kaspersky Security Network, debe aceptar los términos del Contrato de licencia de usuario final al instalar la aplicación. En el Contrato de licencia de usuario final, se indica qué datos se transmiten a Kaspersky Security Network mediante Kaspersky Endpoint Security for Android.

Para mejorar el rendimiento de la aplicación, también puede proporcionar datos estadísticos a Kaspersky Security Network. Proporcionar la información anterior a la KSN es un acto voluntario. Para empezar a utilizar 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 for Android transmite a Kaspersky Security Network.

Intercambio de información con Kaspersky Security Network

Para mejorar la protección en tiempo real, Kaspersky Security for Mobile 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 en línea de Kaspersky para comprobar la reputación de 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 usar todas las funciones 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 los usuarios según listas de categorías permitidas y bloqueadas (por ejemplo, la categoría "Comunicación por Internet").

- **Control de aplicaciones.** La aplicación determina la categoría de la aplicación para restringir el inicio de aplicaciones que no cumplan con los requisitos corporativos de seguridad 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 aplicaciones está disponible en el Contrato de licencia de usuario final. Al aceptar los términos y las condiciones del Contrato de licencia, acepta transferir esta información.

La información sobre los tipos de datos enviados a Kaspersky cuando se usa KSN durante el funcionamiento de Protección web está disponible en la Declaración sobre el procesamiento de datos para Protección web. Al aceptar los términos y las condiciones de la Declaración, acepta transferir esta información.

Con el objetivo de detectar 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, puede ampliar su participación en Kaspersky Security Network.

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

- 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 solicitará que acepten los términos mediante una notificación en la pantalla principal de la aplicación. Los usuarios también pueden aceptar las declaraciones en la sección **Acerca de la aplicación** en la configuración de Kaspersky Endpoint Security for Android.

  Si elige aceptar las declaraciones de forma global, las versiones de las declaraciones aceptadas mediante Kaspersky Security Center deben coincidir con las versiones ya aceptadas por los usuarios. De lo contrario, se 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 las opciones de la directiva de grupo para permitir que las estadísticas se envíen a KSN.

Puede dejar de 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 Kaspersky Endpoint Security for Android.

Para obtener más información sobre la provisión de datos a KSN, consulte la sección "Provisión de datos".

La provisión de datos a KSN es voluntaria. Si lo desea, puede desactivar el intercambio de datos con KSN.

Activación y desactivación del uso de Kaspersky Security Network

Para el funcionamiento de los componentes de Kaspersky Endpoint Security for Android que usan Kaspersky Security Network, la aplicación envía solicitudes a servicios en la nube. Las solicitudes contienen los datos descritos en la sección "Provisión de datos".

Si se desactiva el uso de Kaspersky Security Network en el dispositivo, los componentes Protección en la nube, Protección web y Control de aplicaciones se desactivan automáticamente.

Activar o desactivar el uso de Kaspersky Security Network:

1. Abra la ventana con la configuración de la directiva de administración para dispositivos móviles en los cuales se instaló Kaspersky Endpoint Security for Android.

2. En la ventana **Propiedades** de la directiva, seleccione la sección **Avanzado**.

3. En la sección **Configuración de Kaspersky Security Network (KSN)**, ajuste la configuración para utilizar Kaspersky Security Network:

- Seleccione la **Utilizar Kaspersky Security Network** para utilizar los componentes siguientes: Antivirus (Protección en la nube), Protección Web y Control de aplicaciones (Categorías aplicaciones).

- Seleccione la casilla **Permitir el envío de estadísticas a KSN** para remitir datos a Kaspersky. Estos datos ayudarán a la aplicación de Kaspersky Endpoint Security for Android responder a amenazas con mayor rapidez, mejorar el rendimiento de los componentes de protección y disminuir la probabilidad 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 desactivan 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 **Abrir**.

6. Si definió la configuración del servidor proxy en las propiedades del Servidor de administración, pero la arquitectura de su red requiere que use una KSN privada directamente, active 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 aplicaciones 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 for 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 for Android utiliza el servicio Firebase Cloud Messaging (FCM) para garantizar la entrega oportuna de comandos a los dispositivos móviles y la sincronización forzada cuando se cambia la configuración de la directiva. Kaspersky Endpoint Security for 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 for Android utiliza el servicio Firebase Cloud Messaging (FCM) para garantizar la entrega oportuna de comandos a los dispositivos móviles y la sincronización forzada cuando se cambia la configuración de la directiva. La aplicación también emplea notificaciones de inserción.

Para utilizar el servicio Firebase Cloud Messaging, debe ajustar la configuración del servicio en Kaspersky Security Center. Para obtener más detalles sobre cómo configurar Firebase Cloud Messaging en Kaspersky Security Center, consulte la *ayuda de Kaspersky Security Center*. Si la configuración de Firebase Cloud Messaging no se ajusta, los comandos del dispositivo móvil y la configuración de directiva se entregarán cuando el dispositivo se sincronice con Kaspersky Security Center según la planificación establecida en la directiva (por ejemplo, cada 24 horas). En otras palabras, los comandos y la configuración de directiva se entregarán con retraso.

Con el fin de admitir la funcionalidad principal del producto, usted acepta proporcionar automáticamente al servicio Firebase Cloud Messaging el ID único de la instalación de la aplicación (ID de instancia) y los siguientes datos:

- Información sobre el software instalado: versión de la aplicación, ID de la aplicación, versión de compilación de la aplicación, nombre del paquete de la aplicación.
- Información sobre el equipo en el que está instalado el software: versión del sistema operativo, ID del dispositivo, versión de los servicios de Google.
- Información sobre FCM: ID de la aplicación en FCM, ID de usuario en FCM, versión de protocolo.

Los datos se transmiten a los servicios de Firebase a través de 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 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 la 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 componente de administración de una versión anterior y tiene habilitado el intercambio de datos con el servicio de Google Analytics, Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 3 llevará a cabo el intercambio de datos con el servicio de Google Analytics para Firebase. La asistencia de Google Analytics se ha interrumpido.

Kaspersky Security for Mobile intercambia datos con los servicios de Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics para los siguientes fines:

- Para actualizar 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 solicitará que acepten los términos mediante una notificación en la pantalla principal de la aplicación. Los usuarios también pueden aceptar las declaraciones en la sección **Acerca de la aplicación** en la configuración de Kaspersky Endpoint Security for Android.

    Si elige aceptar las declaraciones de forma global, las versiones de las declaraciones aceptadas mediante Kaspersky Security Center deben coincidir con las versiones ya aceptadas por los usuarios. De lo contrario, se 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 ajustar la configuración de la directiva del grupo para permitir que las estadísticas se envíen a KSN (ver 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 debe leer y aceptar los términos de la Declaración en cuanto al procesamiento de la información para fines de marketing. Si elige que los usuarios acepten la Declaración, pueden aceptar los términos de la Declaración al instalar la aplicación o en la sección **Acerca de la aplicación** en la configuración de Kaspersky Endpoint Security for 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 a continuación).

Provisión de datos a Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics en virtud de la Declaración relativa al procesamiento de la información con fines de marketing

El Titular de los derechos utiliza sistemas de información de terceros para procesar la información. Su procesamiento de datos se rige por las declaraciones de privacidad de dichos sistemas de información de terceros. Los siguientes servicios son los que utiliza el titular de los derechos utiliza y los datos que se procesan:

Google Analytics para Firebase

Durante el uso del Software, se enviarán los siguientes datos a Google Analytics para Firebase de forma automática y periódica con el fin de alcanzar el objetivo declarado:

- información de la aplicación (versión, ID de la aplicación, ID de la aplicación de servicios de Firebase, ID de instancia de servicio de Firebase, nombre del establecimiento en el que se obtuvo la aplicación, fecha y hora del primer lanzamiento del Software)
- El ID de instalación de la aplicación en el dispositivo y el método de instalación en el dispositivo
- información sobre la región y el idioma de localización
- información de la resolución de la pantalla del dispositivo
- información sobre la obtención de root del usuario
- la información de diagnóstico sobre el dispositivo desde el servicio SafetyNet Attestation
- la información sobre la configuración de Kaspersky Endpoint Security for Android como herramienta de Accesibilidad
- información sobre las transiciones entre pantallas de aplicaciones, duración de las sesiones, comienzo y final de las sesiones en pantalla, nombre de la pantalla
- información sobre el protocolo utilizado para enviar datos al servicio de Firebase, su versión y el número de identificación del método utilizado para el envío de datos
- los datos sobre el tipo y los parámetros del evento para el que se presentan los datos
- información sobre la licencia de la aplicación, su disponibilidad y el número de dispositivos
- información sobre la frecuencia de las actualizaciones de la base de datos de antivirus y la sincronización con el Servidor de administración
- información sobre la Consola de administración (Kaspersky Security Center o sistemas EMM de terceros)
- ID de Android
- ID de publicidad
- información sobre el Usuario: la categoría de edad y el género, el identificador del país de residencia y la lista de intereses
- información sobre el equipo del Usuario en el que se ha instalado el Software: el nombre del fabricante del ordenador, el tipo de ordenador, la versión y el idioma (configuración regional) del sistema operativo, la información sobre la aplicación abierta por primera vez en los últimos 7 días y la aplicación abierta por primera vez hace más de 7 días

  La transmisión de datos al servicio Firebase se realiza a través de un canal seguro. La información sobre cómo se tratan los datos en Firebase está publicada en: https://firebase.google.com/support/privacy.

SafetyNet Attestation

Durante el uso del Software, se enviarán los siguientes datos a SafetyNet Attestation de forma automática y periódica con el fin de alcanzar el objetivo declarado:

- el tiempo de comprobación del dispositivo
- la información sobre el software, nombre y datos sobre los certificados del software
- los resultados de comprobación del dispositivo
- las comprobaciones al azar de los números de identificación para verificar los resultados de comprobación del dispositivo

  La transmisión de datos a SafetyNet Attestation se realiza a través de un canal seguro. La información sobre cómo se tratan los datos en SafetyNet Attestation está publicada en: https://policies.google.com/privacy.

Firebase Performance Monitoring

Durante el uso del Software, se enviarán los siguientes datos al Firebase Performance Monitoring de forma automática y periódica con el fin de alcanzar el objetivo 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
- aviso para indicar si el dispositivo está comprometido
- fuerza de la señal
- duración de los rastros automatizados
- red y la información correspondiente a continuación: código de respuesta, tamaño de la carga útil en bytes, tiempo de respuesta
- descripción del dispositivo

La transmisión de datos al servicio de Firebase Performance Monitoring se realiza a través de un canal seguro. La información sobre cómo se procesan los datos en Firebase Performance Monitoring está publicada en: https://firebase.google.com/support/privacy.

Crashlytics

Durante el uso del Software, se enviarán los siguientes datos a Crashlytics de forma automática y periódica con el fin de alcanzar el objetivo declarado:

- ID del Software
- versión del Software instalado
- mensaje que indica si el software estaba en ejecución en segundo plano
- arquitectura del 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
- aviso para indicar si el dispositivo está comprometido
- orientación de la pantalla al momento del evento
- fabricante del producto o hardware
- ID de instalación único
- versión de las estadísticas que se envían
- tipo de excepción de software
- texto del mensaje de error
- mensaje que indica que la excepción de software fue provocada por una excepción anidada
- ID de subproceso
- mensaje que indica si el marco fue el motivo del error de software
- mensaje 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 del evento, fecha y hora del evento, tipo y valor del evento
- valores de registro del CPU
- el tipo y el valor del evento

  La transmisión de datos a Crashlytics se realiza a través de un canal seguro. La información sobre cómo se tratan los datos en Crashlytics está publicada en: https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

El envío de la información anterior para su procesamiento con fines de comercialización es voluntario.

Para desactivar el intercambio de datos con los servicios de Google Analytics para Firebase, SafetyNet Attestation, Firebase Performance Monitoring y Crashlytics:

1. Abra la ventana de la configuración de la directiva de gestión de dispositivos móviles en que se ha instalado la aplicación Kaspersky Endpoint Security for Android.
2. En la ventana **Propiedades** de la directiva, seleccione la sección **Avanzado**.
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 for Android, se deben aceptar los términos del Contrato de licencia de usuario final, así como las Declaraciones adicionales (ver más abajo). Se configura una política para aceptar las Declaraciones que se indican a continuación de forma global, para todos los usuarios. No se 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 relativa al procesamiento de datos para Protección web
- Declaración relativa al procesamiento de la información para fines de marketing

Si elige aceptar las declaraciones de forma global, las versiones de las declaraciones aceptadas mediante Kaspersky Security Center deben coincidir con las versiones ya aceptadas por los usuarios. De lo contrario, se 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 por 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 que pertenecen los dispositivos de Android.
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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Avanzado**.
5. En la sección **Transferencia de datos**, elija si la Declaración sobre el procesamiento de datos con fines de marketing se aceptará globalmente o por los usuarios.
6. En la sección **Configuración de Kaspersky Security Network (KSN)**, elija si la Declaración de Kaspersky Security Network se aceptará globalmente o por los usuarios.
7. Haga clic en el botón **Aplicar** para guardar los cambios que ha realizado.

El usuario puede aceptar los términos de una declaración o rechazarlos en cualquier momento en la sección **Información de la aplicación** en la configuración de Kaspersky Endpoint Security for 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 for Android mediante la inscripción móvil de KNOX

La inscripción móvil KNOX (KME) forma parte de la solución móvil de Samsung KNOX. Se utiliza para la instalación por lotes y la configuración inicial de las aplicaciones en nuevos dispositivos Samsung que se compran en los proveedores oficiales.

La instalación de la aplicación de Kaspersky Endpoint Security for Android mediante inscripción móvil de KNOX requiere los pasos siguientes:

1. Crear un perfil MDM de KNOX con la aplicación de Kaspersky Endpoint Security for Android.
2. Añadir dispositivos a la inscripción móvil de KNOX.
3. Instalar la aplicación Kaspersky Endpoint Security for Android en los dispositivos móviles del usuario.

Para obtener más información sobre cómo trabajar con la inscripción móvil de KNOX, consulte la *Guía del usuario de inscripción móvil de KNOX*.

La implementación a través de KNOX Mobile Enrollment solo es posible para dispositivos Samsung. Para consultar la lista de dispositivos admitidos, visite el *sitio web del Soporte Técnico de Samsung*.

Crear un perfil MDM de KNOX

Un perfil *MDM de KNOX* es un perfil que contiene enlaces a aplicaciones para su rápida implementación y configuración inicial en dispositivos móviles.

Para crear un perfil MDM de KNOX:

1. Inicie sesión en la Consola de Samsung KNOX → **Inscripción móvil de KNOX**.
2. Seleccione la sección **Perfiles MDM**.
3. Haga clic en **Agregar**.

   Se inicia el Asistente del nuevo Perfil MDM de KNOX.
4. En el paso **Conexión del servidor de MDM**, seleccione **URI del servidor no se requiere para mi servicio de MDM** y haga clic en **Siguiente**.
5. En el paso **Información del perfil MDM**:
   a. Introduzca la información general sobre el perfil MDM de KNOX: **Nombre de Perfil** y **Descripción**.
   b. Haga clic en el botón **Añadir aplicaciones de MDM** e introduzca la ruta al archivo de instalación APK.

      El archivo de instalación para Kaspersky Endpoint Security for Android se incluye en el kit de distribución de Kaspersky Security for Mobile. De antemano, coloque el archivo de instalación APK en el Web Server de Kaspersky Security Center o en otro servidor que ofrezca acceso para descargas desde el dispositivo.
   c. Introduzca la configuración para conectar el dispositivo a Kaspersky Security Center en el campo **Datos del usuario de JSON** en el formato siguiente:
      `{"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 **Añadir acuerdos de Knox**.

      Para instalar Kaspersky Endpoint Security for Android mediante el registro de KNOX Mobile, 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 **los Acuerdos de licencia para el usuario final, Condiciones del Servicio y Condiciones de uso**. También puede añadir otros documentos oficiales de su empresa que son necesarios para desplegar un perfil MDM de KNOX haciendo clic en el botón **Añadir Contrato de usuario**.
   e. Desmarque la casilla **Asociar licencia de Knox a este perfil**.

      Se proporciona información sobre la licencia de Samsung KNOX al dispositivo móvil junto con la directiva cuando el dispositivo se sincroniza con Kaspersky Security Center.
6. Haga clic en el botón **Guardar**.

Como resultado, el nuevo perfil MDM de KNOX con la aplicación de Kaspersky Endpoint Security for Android se añadirá a la lista en la consola de KME.

Añadir dispositivos a la inscripción móvil de KNOX

Los dispositivos se pueden añadir en la consola de inscripción móvil de KNOX (KME) de las siguientes formas:

- El proveedor añade automáticamente dispositivos en la consola de KME después de comprar los dispositivos.

  Seleccione este método si su organización trabaja con un proveedor oficial de dispositivos Samsung.

- El administrador instala la app de implementación de KNOX desde Google Play en su dispositivo móvil y migra el perfil MDM de KNOX a los dispositivos de los usuarios a través de Bluetooth o NFC (Comunicación de Campo Cercano). Después de implementar el perfil MDM de KNOX, el dispositivo se añadirá automáticamente a la consola de KME.

  Seleccione este método si los dispositivos Samsung no se compran a un proveedor oficial.

Añadir un dispositivo a través del proveedor

Un proveedor oficial de dispositivos Samsung está registrado en Samsung KNOX. Para consultar la lista de proveedores oficiales, visite el *sitio web del Soporte Técnico de Samsung*. El proveedor añade automáticamente los dispositivos a la consola de KME para su cuenta Samsung inmediatamente después de comprar los dispositivos. Para que el proveedor añada los dispositivos, debe registrar al proveedor en la consola de KME con su cuenta de Samsung. Necesitará un ID del distribuidor para añadir al proveedor de dispositivos Samsung a la consola de KME. Para recibir el ID del distribuidor, debe enviar una solicitud al proveedor. En la solicitud, especifique su ID de cliente de KNOX.

Para ver su ID del cliente de KNOX:

1. Inicie sesión en la consola de Samsung KNOX → **Inscripción móvil de KNOX**.
2. Seleccione la sección **Distribuidores**.
3. Su ID se muestra en el campo **ID de cliente de KNOX**.

Después de recibir una respuesta del proveedor con el ID de distribuidor, registre al proveedor en la consola de KME. Antes registrar al proveedor, puede crear un perfil MDM de KNOX para que el perfil pueda implementarse automáticamente al añadir nuevos dispositivos.

Para registrar a un proveedor oficial en la consola de KME:

1. Inicie sesión en la consola de Samsung KNOX → **Inscripción móvil de KNOX**.
2. Seleccione la sección **Distribuidores**.
3. Haga clic en el botón **Registrar distribuidor**.

   Esto abrirá una ventana para registrar al proveedor del dispositivo.
4. En el campo **ID del distribuidor**, introduzca el ID recibido del proveedor oficial de dispositivos Samsung.
5. Si ha creado un perfil MDM de KNOX, seleccione el perfil MDM de KNOX en la ventana de registro del proveedor.

   Cuando añada nuevos dispositivos, el perfil MDM de KNOX se instalará automáticamente.

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 añade un dispositivo, tendrá que confirmar la operación.

   - **Confirmar automáticamente todas las descargas de este distribuidor**. Los dispositivos del proveedor se añadirán automáticamente a la consola de KME.

7. Haga clic en **Aceptar**.

El proveedor de dispositivos Samsung se añadirá a la lista de proveedores de la consola de KME.

Después de comprar los nuevos dispositivos al proveedor oficial, la aplicación Kaspersky Endpoint Security for Android se instalará automáticamente en los dispositivos al conectarlos a Internet. Para obtener más información sobre cómo trabajar con la inscripción móvil de KNOX, consulte la *Guía del usuario de inscripción móvil de KNOX*. Si ya tiene una lista de dispositivos en la consola de KME, añada el perfil MDM de KNOX con la app de MDM de KNOX al dispositivo.

Para enviar un perfil MDM de KNOX a dispositivos:

1. Inicie sesión en la Consola de Samsung KNOX → **Inscripción móvil de KNOX**.

2. Seleccione **Dispositivos** → **Todos los dispositivos**.

3. Seleccione los dispositivos en los que desea instalar el perfil MDM de KNOX.

4. Haga clic en el botón **Configurar**.

   Se abrirá la ventana **Información del dispositivo**.

5. En la lista **Perfil MDM**, seleccione el perfil MDM de KNOX con la app de Kaspersky Endpoint Security for Android.

6. En el campo **Etiquetas**, introduzca etiquetas para agrupar y etiquetar dispositivos, y para optimizar la búsqueda en la consola de KME.

7. Introduzca las credenciales de la cuenta de usuario del dispositivo en los campos **ID de usuario** y **Contraseña**.

   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 de KNOX para los dispositivos restantes.

9. Haga clic en el botón **Guardar**.

Después de conectar el dispositivo a Internet, se le solicitará al usuario instalar el perfil MDM de KNOX.

Añadir un dispositivo mediante la app de implementación de KNOX

Si no ha comprado su dispositivo Samsung a un proveedor oficial, puede añadir el dispositivo a la inscripción móvil de KNOX a través de Bluetooth o NFC. Esto requerirá el dispositivo móvil del administrador que será utilizado para enviar los perfiles MDM de KNOX a los dispositivos móviles de los usuarios.

Para añadir dispositivos utilizando la app de implementación de KNOX, deben cumplirse las condiciones siguientes:

- Según el modo de entrega seleccionado, Bluetooth o los módulos NFC se deben activar en los dispositivos móviles.
- Los dispositivos móviles deben estar conectados a Internet.

Para enviar un perfil MDM de KNOX utilizando la app de implementación de KNOX:

1. Instale la app de implementación de KNOX desde Google Play en el dispositivo móvil del administrador.
2. Inicie la app de implementación de KNOX.
3. Introduzca sus credenciales de la cuenta de Samsung.
4. En la ventana **Implementación de KNOX**, ajuste la configuración para implementar un perfil MDM de KNOX:
   - Seleccione el perfil MDM de KNOX.
   - Seleccione el modo de implementación: **Bluetooth** o **NFC**.

     Al utilizar Bluetooth, puede añadir un perfil MDM de KNOX a varios dispositivos al mismo tiempo.
5. Haga clic en **Iniciar implementación**:
   - **Bluetooth**. En el dispositivo móvil del usuario, abra el sitio web https://configure.samsungknox.com.

     Esto iniciará el Asistente de Registro del Dispositivo de Samsung KNOX. Siga las instrucciones en pantalla.

     Después de instalar el perfil MDM de KNOX, el nuevo dispositivo con la etiqueta **Bluetooth** se añadirá a la consola de 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 nuevo dispositivo con la etiqueta **NFC** se añadirá a la consola de KME.

Instalación de la aplicación

Antes de instalar la aplicación de Kaspersky Endpoint Security for 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 implementación del perfil MDM de KNOX, el archivo de instalación APK se descargará automáticamente en el dispositivo móvil. La Instalación de la aplicación de Kaspersky Endpoint Security for Android se inicia automáticamente. El usuario debe aceptar el Contrato de licencia de Samsung KNOX y el Contrato de licencia de Kaspersky Endpoint Security for Android. No se requiere ninguna configuración adicional de la aplicación. Después de instalar la aplicación, 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 de KNOX (`groupName`).

Configuración de los contenedores KNOX

Esta sección contiene información sobre el uso de contenedores KNOX en dispositivos Samsung con Android.

El uso de contenedores KNOX solo está disponible en dispositivos Samsung con Android 6.0 o posterior.

Acerca de los 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 situado en un contenedor KNOX. Se recomienda implementar un contenedor KNOX si los dispositivos móviles personales de empleados se utilizan para trabajar con datos corporativos.

Para usar contenedores KNOX, debe activar Samsung KNOX. Después de sincronizar un dispositivo con Kaspersky Security Center, se solicitará al usuario del dispositivo móvil que instale el contenedor KNOX. Antes de instalar el contenedor KNOX, el usuario debe aceptar las condiciones del Contrato de licencia de usuario final de Samsung.

Después de instalar el contenedor KNOX, el icono de KNOX se añadirá al escritorio del dispositivo móvil. O bien la estación de trabajo se añadirá a la lista de aplicaciones del dispositivo móvil. Para utilizar datos corporativos, el usuario tiene que iniciar la aplicación desde el contenedor KNOX.

Kaspersky Endpoint Security for Android no está instalado en el contenedor KNOX y no protege datos corporativos. Kaspersky Endpoint Security for Android no detecta la descarga de archivos maliciosos ni bloquea sitios maliciosos en el contenedor KNOX. No puede controlar el inicio de aplicaciones ni prohibir el uso de la cámara en el contenedor KNOX. Kaspersky Endpoint Security for Android protege solo datos privados. Puede proteger 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 utilizar 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 for Android instalada en los dispositivos de sus usuarios:

- Si hay una versión actual de Kaspersky Endpoint Security for Android instalada en los dispositivos, no necesita ninguna clave para activar Samsung KNOX.
- Si hay una versión anterior de Kaspersky Endpoint Security for Android (10.8.3.174 o anterior) instalada en los dispositivos, debe obtener una clave del gestor de licencias de KNOX (en lo sucesivo, clave KLM) de Samsung. Una *clave del gestor de licencias de KNOX* es un código exclusivo 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 que pertenecen los dispositivos de Android.
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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Gestionar Samsung KNOX → Contenedores KNOX**.
5. En el campo **Clave del gestor de licencias de KNOX**, especifique lo siguiente:
   - Si hay una versión actual de Kaspersky Endpoint Security for Android instalada en los dispositivos, escriba cualquier carácter.
   - Si hay una versión anterior de Kaspersky Endpoint Security for Android (10.8.3.174 o anterior) instalada en los dispositivos, introduzca la clave KLM de Samsung.
6. Configure el atributo "bloquear" en la posición bloqueada .
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. Se indicará al usuario que acepte los términos del Contrato de licencia de usuario final de Samsung e instale 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 que pertenecen los dispositivos de Android.
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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Gestionar Samsung KNOX → Contenedores KNOX**.
5. Elimine el valor del campo **Clave del gestor de licencias de 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. Se bloqueará el acceso al contenedor KNOX.

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 aplicaciones no funcionan en un contenedor KNOX. Este problema se debe a la falta de permisos en el contenedor KNOX (servicio de accesibilidad). En dispositivos compatibles con KNOX 2.8 o posterior, todos los componentes de la aplicación funcionan sin limitaciones.

- Las versiones de Kaspersky Endpoint Security for Android anteriores a Service Pack 4 Maintenance Release 3 Update 2 pueden no funcionar correctamente en dispositivos Samsung con Android 10 debido a las actualizaciones de Samsung KNOX. Se recomienda actualizar Kaspersky Endpoint Security for Android a la versión Service Pack 4 Maintenance Release 3 Update 2.

Configuración de firewall en KNOX

Debería configurar el 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 que pertenecen los dispositivos de Android.

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 cualquier columna.

4. En la ventana **Propiedades** de la directiva, seleccione la sección **Gestionar Samsung KNOX → Contenedores KNOX**.

5. En la ventana **Firewall**, haga clic en **Configurar**.

   Se abrirá la ventana **Firewall**.

6. Seleccione el modo Firewall:

   - Para permitir todas las conexiones entrantes y salientes en el dispositivo móvil, baje el control deslizante a **Permitir todo**.

   - Para bloquear toda la actividad de red salvo la de las aplicaciones de la lista de exclusiones, suba el control deslizante hasta **Bloquear todo salvo excepciones**.

7. Si ha establecido el modo Firewall en **Bloquear todo salvo excepciones**, cree una lista de exclusiones:

   a. Haga clic en **Agregar**.

      Esto abre la ventana **Exclusión de firewall**.

   b. En el campo **Nombre de la aplicación**, escriba el nombre de la aplicación móvil.

   c. En el campo **Nombre de paquete**, introduzca el nombre de sistema del paquete de aplicaciones móviles (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 usar correo corporativo, contactos y el calendario en un contenedor KNOX, debería configurar los ajustes 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 que pertenecen los dispositivos de Android.
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 cualquier columna.
4. En la ventana **Propiedades** de la directiva, seleccione la sección **Gestionar Samsung KNOX → Contenedores KNOX**.
5. En la ventana **Exchange ActiveSync**, haga clic en el botón **Configurar**.

   Se abrirá la ventana **Intercambiar configuración de servidor de correo electrónico**.
6. En el campo **Dirección del servidor**, introduzca la dirección IP o el nombre DNS del servidor que aloja el servidor de correo.
7. En el campo **Dominio**, introduzca el nombre de dominio del usuario del dispositivo móvil de la red corporativa.
8. En la lista desplegable **Intervalo de sincronización**, seleccione el intervalo deseado para la sincronización del dispositivo móvil con el servidor Microsoft Exchange Server.
9. Para utilizar el protocolo SSL (capa de sockets seguros) de transferencia de datos, seleccione la casilla de verificación **Utilizar conexión SSL**.
10. Para utilizar certificados digitales con el fin de proteger la transferencia de datos entre el dispositivo móvil y Microsoft Exchange Server, seleccione la casilla de verificación **Verificar certificado de 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 complementaria al 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 para diferentes funciones de la aplicación, dependiendo de las funciones del puesto de cada usuario.

Para cada área funcional, el administrador puede asignar los siguientes permisos:

- **Permitir editar**. El usuario de la Consola de administración tiene permiso para cambiar la configuración de directiva en la ventana de propiedades.

- **Bloquear editar**. Se prohíbe al usuario de la Consola de administración cambiar la configuración de directiva en la ventana de propiedades. No se muestran en la interfaz las pestañas de directiva pertenecientes al ámbito funcional para la cual se ha asignado este derecho.

Permisos para acceder a las secciones del complemento de administración Kaspersky Endpoint Security

Ámbito funcional	Sección Directivas
Android Enterprise	Perfil de trabajo de Android
Antirrobo	Antirrobo
Control de aplicaciones	Control de aplicaciones
Protección	Protección, Análisis, Actualización
Control de cumplimiento	Control de cumplimiento
Contenedores	Contenedores
Configuración del dispositivo	Control de dispositivos, Sincronización
Administración de dispositivos Samsung	APN, Administración de dispositivos Samsung, contenedores KNOX
Administración del sistema	Avanzado, Wi-Fi
Protección web	Protección web

Permisos para acceder a las secciones del complemento de administración de Kaspersky Device Management for iOS

Ámbito funcional	Sección Directivas
Avanzado	Clips web, Fuentes, AirPlay, AirPrint
Exchange ActiveSync	General, contraseña, sincronización, restricciones de las funciones, restricciones de las aplicaciones
General	General, Inicio de sesión único, Protección web, Wi-Fi, Nombre de punto de acceso (APN), Exchange ActiveSync, Correo electrónico, Cargas personalizadas
LDAP (calendario/contactos)	LDAP, Calendario, Contactos, Suscripciones del calendario
Limitaciones y seguridad	Restricción de las Funciones, Restricciones de Aplicaciones, Restricciones de Contenido multimedia, Contraseña, VPN, proxy de HTTP Global, Certificados, SCEP

Categorías de aplicación

El Control de aplicaciones admite la clasificación de aplicaciones. El modo de funcionamiento configurado para la categoría de 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	Aplicaciones diseñadas para desarrollar software. Depuradores, compiladores, editores

de desarrollo	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 for 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 configura su dispositivo según los requisitos corporativos de seguridad. Es posible que algunas de las funciones y opciones que se describen en esta sección no se apliquen a su experiencia real con la app. Si tiene alguna pregunta sobre la app instalada en un dispositivo específico, comuníquese con su administrador.

Funciones de la aplicación

Kaspersky Endpoint Security ofrece las siguientes funciones clave.

Protección frente a virus y otros tipos de software malintencionado

La aplicación utiliza el componente Antivirus para proteger el dispositivo frente a virus y otros tipos de software malintencionado.

El componente Antivirus incluye las siguientes funciones:

- Análisis en busca de amenazas en todo el dispositivo, las aplicaciones instaladas o las carpetas seleccionadas
- Protección del dispositivo en tiempo real
- Análisis de aplicaciones instaladas recientemente antes de que se inicien por primera vez
- Actualización de las bases de datos antivirus

Si una aplicación que recopila la información y la envía para procesarse se instala en un dispositivo móvil, Kaspersky Endpoint Security for Android puede clasificarla como software malicioso.

Control de aplicaciones

Según los requisitos de seguridad corporativa, el *administrador del sistema de administración remota* (en adelante, también "administrador") crea listas de aplicaciones recomendadas, bloqueadas y necesarias. El componente Control de aplicaciones sirve para instalar las aplicaciones recomendadas y necesarias, actualizarlas y eliminar las que están bloqueadas.

Control de aplicaciones le permite instalar aplicaciones recomendadas y necesarias en el dispositivo por medio de un vínculo directo al paquete de distribución o un vínculo a Google Play. Control de aplicaciones le permite eliminar las aplicaciones bloqueadas que infringen los requisitos corporativos de seguridad.

Kaspersky Endpoint Security debe estar activado como un servicio de Funciones de accesibilidad para garantizar el correcto funcionamiento del Control de aplicaciones. Si no activa este servicio durante el Asistente de configuración inicial para la aplicación, puede activar Kaspersky Endpoint Security como un servicio de Funciones de Accesibilidad en la sección **Estado** seleccionando la notificación apropiada, o bien en la configuración del dispositivo (**Configuración de Android** → **Accesibilidad** → **Servicios**).

Protección de datos de dispositivos robados o extraviados

El componente Antirrobo protege sus datos frente a accesos no autorizados y ayuda a localizar el dispositivo en caso de pérdida o robo.

Antirrobo le permite realizar las siguientes operaciones de forma remota:

- Bloquear el dispositivo.

  Para evitar que un pirata pueda abrir el dispositivo, Kaspersky Endpoint Security se debe activar como un servicio de Funciones de Accesibilidad en dispositivos móviles con Android 7.0 o posterior.

- Activar una alarma fuerte en el dispositivo incluso si el dispositivo está silenciado.
- Obtener las coordenadas del mapa de ubicación del dispositivo.
- Borrar los datos almacenados en el dispositivo.
- Restablecer a la configuración de fábrica.
- Tomar secretamente una foto de identificación de la persona que esté utilizando el dispositivo.

Para activar operaciones Antirrobo, Kaspersky Endpoint Security se debe activar como administrador del dispositivo. Si no concedió derechos de administrador del dispositivo durante la configuración inicial de aplicaciones, puede concederlos a Kaspersky Endpoint Security en la sección **Estado** al seleccionar la notificación apropiada, o bien en la configuración del dispositivo (**Configuración de Android** → **Seguridad** → **Administradores de dispositivo**).

Protección contra amenazas en línea

El componente Protección web ofrece protección contra amenazas en línea.

Protección web bloquea los sitios web maliciosos que distribuyen un código malicioso y los sitios web de phishing diseñados para robar datos confidenciales y obtener acceso a sus cuentas bancarias. Protección web utiliza el servicio en la nube de Kaspersky Security Network para analizar sitios web antes de abrirlos.

Para activar Protección web:

- Kaspersky Endpoint Security se debe activar como un servicio de Funciones de Accesibilidad.
- Debe aceptar la Declaración relativa al procesamiento de datos para el uso de 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 ha aceptado la Declaración de Protección web y le envió la solicitud para que lo haga, 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 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 activada solo para el perfil de trabajo.

Ventana principal de un vistazo

El aspecto de la ventana principal varía ligeramente de una resolución de pantalla a otra.

El aspecto 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 con la protección de su dispositivo.
- Información sobre si su dispositivo cumple o no con los requisitos corporativos de seguridad.
- Información sobre el estado de la protección de su dispositivo.

Puede abrir la sección **Estado** pulsando la parte superior de la ventana principal de Kaspersky Endpoint Security.

Problemas de protección del dispositivo

Los problemas de protección se agrupan por categorías. Cada problema viene acompañado de las medidas que pueden seguirse para solucionarlo.

La sección **Estado** también muestra una lista de objetos omitidos detectados por la aplicación. La lista de objetos omitidos puede cambiar, por ejemplo, si un archivo malicioso se elimina o se mueve. Para recibir una lista actualizada de amenazas, ejecute un análisis del dispositivo completo. Para asegurarse de que sus datos siguen estando protegidos, elimine todos los objetos detectados.

Existen dos tipos de problemas de protección:

- *Problemas de notificación*. Están resaltados en amarillo. Los problemas de notificación informan al usuario de eventos que pueden afectar a la seguridad del dispositivo (por ejemplo, si el último análisis se ha realizado hace más de 14 días o si no se ha analizado una aplicación instalada recientemente). Puede ocultar un problema de notificación. Posteriormente, podrá consultar la información del problema a través del menú **Problemas ocultos**.
- *Críticos*. Están resaltados en rojo. Los problemas críticos informan al usuario de eventos de vital importancia para la seguridad del dispositivo (como, por ejemplo, el hecho de que las bases de datos antivirus lleven mucho

tiempo sin actualizarse, o sobre la instalación de una aplicación bloqueada en el dispositivo). No es posible ocultar los problemas críticos.

Control de cumplimiento

La aplicación comprueba automáticamente si el dispositivo se ajusta a los requisitos de seguridad corporativa. En la sección **Estado**, se muestra información sobre si el dispositivo cumple los requisitos de seguridad corporativa.

- La razón por la que el dispositivo no cumple con los requisitos de seguridad corporativa (por ejemplo, se han detectado aplicaciones bloqueadas en el dispositivo).
- El período de tiempo en que debe resolver el incumplimiento (por ejemplo, 24 horas).
- La 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).
- La acción adoptada para resolver el incumplimiento con los requisitos de la seguridad corporativa del dispositivo.

Icono de la barra de estado

Una vez que termine el primer asistente de inicio, aparecerá el icono de Kaspersky Endpoint Security en la barra de estado.

Este icono refleja el funcionamiento de la aplicación y permite acceder a la ventana principal de Kaspersky Endpoint Security.

Este icono señala el funcionamiento de Kaspersky Endpoint Security y refleja el estado de protección de su 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 un icono de maletín, Configuración del perfil de trabajo de Android). Kaspersky Endpoint Security for Android no tiene acceso a la memoria externa en el perfil de trabajo. La información sobre los objetos detectados se muestra en la sección **Estado** de la app. 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 for 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, siga estos pasos:

1. Pulse **Analizar** en el panel de inicio rápido de la ventana principal de Kaspersky Endpoint Security.

2. Seleccione la cobertura del análisis del dispositivo:

   - **Analizar todo el dispositivo**. La aplicación analiza todo el sistema de archivos del dispositivo.
   - **Analizar aplicaciones instaladas**. La aplicación analiza solo las aplicaciones instaladas.
   - **Análisis personalizado**. La aplicación analiza las carpetas o archivos individuales seleccionados. Puede seleccionar un objeto particular (carpeta o archivo) o una de las siguientes particiones de la memoria del dispositivo:
     - **Memoria del dispositivo**. Memoria con acceso de lectura de todo el dispositivo. Aquí también se incluye la partición de memoria del sistema que almacena los archivos del sistema operativo.
     - **Memoria interna**. Partición de la memoria del dispositivo pensada para la instalación de aplicaciones y el almacenamiento de contenido 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 acceso a la configuración del análisis de virus puede estar restringido por su administrador.

Para configurar el análisis de virus:

1. En el panel de inicio rápido de la ventana principal de Kaspersky Endpoint Security, pulse → **Configuración** → **Antivirus** → **Analizar**.
2. Si desea que la aplicación detecte adware y aplicaciones que podrían utilizar los piratas informáticos para causar daños a su dispositivo o sus datos mientras la aplicación realiza un análisis, active el botón **Software publicitario, marcadores y otros**.
3. Haga clic en **Acción al detectar una amenaza** y seleccione la acción predeterminada que realizará la aplicación:

   - **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 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 eliminarse un objeto, Kaspersky Endpoint Security mostrará una notificación temporal sobre la detección del objeto.

   - **Omitir**

     Si los objetos detectados se han omitido, Kaspersky Endpoint Security le advierte sobre problemas en la protección del dispositivo. Puede ver más información sobre los objetos omitidos en la sección **Estado** de la aplicación. Para cada amenaza omitida, la aplicación proporciona acciones que puede realizar para eliminar la amenaza. La lista de objetos omitidos puede cambiar, por ejemplo, si un archivo malicioso se elimina o se mueve. Para recibir una lista actualizada de amenazas, ejecute un análisis completo del dispositivo. Para asegurarse de que sus datos siguen estando protegidos, elimine todos los objetos detectados.

La información sobre las amenazas detectadas y las acciones realizadas respecto de ellas se registra en los informes de la app (→ **Informes**). Puede optar por mostrar informes sobre operaciones antivirus.

Ejecución de 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 un icono de maletín, Configuración del perfil de trabajo de Android). Kaspersky Endpoint Security for Android no tiene acceso a la memoria externa en el perfil de trabajo. La información sobre los objetos detectados se muestra en la sección **Estado** de la app. 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 for 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 planificación del análisis completo para un dispositivo:

1. En el panel de inicio rápido de la ventana principal de Kaspersky Endpoint Security, pulse → **Configuración** → **Antivirus** → **Analizar**.
2. Pulse **Planificación** y seleccione la frecuencia del análisis completo:
   - **Semanalmente**
   - **Diariamente**
   - **Desactivada**
   - **Tras la actualización de la base de datos**
3. Haga clic en **Día de inicio** y seleccione el día de la semana en que desea iniciar el análisis completo.
4. Haga clic en **Hora de inicio** y seleccione la hora de inicio del análisis completo.

El análisis completo del dispositivo se iniciará según la planificación.

> En Android 12 o versiones posteriores, 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

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 automáticamente.

Para cambiar el modo de protección del dispositivo, siga estos pasos:

1. En el panel de inicio rápido de la ventana principal de Kaspersky Endpoint Security, pulse → **Configuración** → **Antivirus** → **Modo de protección en tiempo real**.

2. Seleccione el modo de protección del dispositivo:

   - **Desactivada**. La protección está desactivada.
   - **Recomendado**. El antivirus analiza solo aplicaciones y archivos instalados desde la carpeta Descargas. El antivirus analiza las aplicaciones nuevas inmediatamente después de su instalación.
   - **Ampliado**. El antivirus analiza todos los archivos del dispositivo en busca de objetos maliciosos cuando se realiza cualquier operación con ellos (por ejemplo, cuando se guardan, mueven o modifican). El antivirus también analiza las aplicaciones nuevas inmediatamente después de su instalación.

La información sobre el modo de protección actual aparece debajo de 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. Pulse → **Configuración** → **Antivirus** en el panel de inicio rápido de la ventana principal de Kaspersky Endpoint Security.

2. Active el botón **Protección en la nube (KSN)**.

   El botón 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 de verificación está desactivada, Kaspersky Endpoint Security continúa utilizando KSN para el funcionamiento de otros componentes de la aplicación.

Como resultado, la aplicación obtiene acceso a la base de conocimientos en línea de Kaspersky para comprobar la reputación de 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 usar todas las funciones del Antivirus y reduce la posibilidad de falsas alarmas. Solo su administrador puede deshabilitar completamente el uso de Kaspersky Security Network.

Para configurar la Protección en tiempo real:

1. En el panel de inicio rápido de la ventana principal de Kaspersky Endpoint Security, pulse → **Configuración** → **Antivirus** → **Modo de protección en tiempo real**.

2. Si desea que la aplicación detecte adware y aplicaciones que podrían utilizar los piratas informáticos para causar daños a su dispositivo o sus datos mientras la aplicación realiza un análisis, active el botón **Software publicitario, marcadores y otros**.

3. Haga clic en **Acción al detectar una amenaza** y seleccione la acción predeterminada que realizará la aplicación:

   - **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.

   - **Eliminar**

     Los objetos detectados se eliminarán automáticamente. No se requieren más acciones. Antes de eliminarse un objeto, Kaspersky Endpoint Security mostrará una notificación temporal sobre la detección del objeto.

- **Omitir**

  Si los objetos detectados se han omitido, Kaspersky Endpoint Security le advierte sobre problemas en la protección del dispositivo. Puede ver más información sobre los objetos omitidos en la sección **Estado** de la aplicación. Para cada amenaza omitida, la aplicación proporciona acciones que puede realizar para eliminar la amenaza. La lista de objetos omitidos puede cambiar, por ejemplo, si un archivo malicioso se elimina o se mueve. Para recibir una lista actualizada de amenazas, ejecute un análisis completo del dispositivo. Para asegurarse de que sus datos siguen estando protegidos, elimine todos los objetos detectados.

La información sobre amenazas detectadas y las acciones realizadas en ellos se registra en los informes de la app (→ **Configuración** → **Informes**). Puede optar por mostrar informes sobre operaciones antivirus.

Actualizaciones de bases de datos antivirus

Para actualizar las bases de datos antivirus de la aplicación, siga estos pasos:

Pulse **Actualizar base de datos** en el panel de inicio rápido de la ventana principal de Kaspersky Endpoint Security.

Actualización de la base de datos planificada

La aplicación puede actualizar automáticamente las bases de datos antivirus según la planificación que especifique.

Para configurar la planificación de la actualización, siga estos pasos:

1. En el panel de inicio rápido de la ventana principal de Kaspersky Endpoint Security, pulse → **Configuración** → **Antivirus** → **Actualizar base de datos**.
2. Haga clic en **Planificación** y seleccione la frecuencia de actualización:
   - **Semanalmente**
   - **Diariamente**
   - **Desactivada**
3. Haga clic en **Día de inicio** y seleccione el día de la semana en que desea ejecutar la actualización.
4. Haga clic en **Hora de inicio** y seleccione la hora de inicio de la actualización.

Las actualizaciones de la base de datos antivirus se iniciarán según la planificación.

En Android 12 o versiones posteriores, 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

Si se pierde o le roban el dispositivo, comuníquese con el administrador del sistema. El administrador puede ejecutar comandos de Antirrobo en su dispositivo de forma remota según los requisitos corporativos de seguridad.

Si se envía un comando de reinicio completo al dispositivo, se perderá el control sobre este y los comandos antirrobo restantes no funcionarán.

Protección web

Para activar Protección web:

- Kaspersky Endpoint Security se debe activar como un servicio de Funciones de Accesibilidad.
- Debe aceptar la Declaración relativa al procesamiento de datos para el uso de 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 ha aceptado la Declaración de Protección web y le envió la solicitud para que lo haga, 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 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 activada solo para el perfil de trabajo.

Para utilizar Protección web en todo momento mientras navega por Internet, establezca Google Chrome o Samsung Internet Browser como navegador predeterminado.

Para definir un navegador compatible como navegador predeterminado y utilizar Protección web para el análisis de sitios web en todo momento:

1. Pulse → **Configuración** → **Protección web** en el panel de inicio rápido de la ventana principal de Kaspersky Endpoint Security.
2. Active el botón **Protección web**.
3. Pulse **Establecer navegador predeterminado**.

   Este botón se muestra cuando la Protección web está activada y no se ha establecido un navegador compatible como navegador predeterminado.

   Se iniciará el asistente de selección del navegador predeterminado.
4. Siga las instrucciones del asistente.

El asistente establece Google Chrome o los navegadores de Samsung o Huawei como navegador predeterminado. Protección web analiza constantemente los sitios web mientras navega por Internet.

Control de aplicaciones

Control de aplicaciones 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 aplicaciones permitidas, bloqueadas, obligatorias y recomendadas según los requisitos corporativos de seguridad. Debido al Control de aplicaciones, Kaspersky Endpoint Security le solicita instalar las aplicaciones obligatorias y recomendadas, y eliminar 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 aplicaciones.
3. Realice las acciones recomendadas.

Obtener certificado

Para obtener un certificado de acceso a los recursos de red corporativos:

1. Pulse → **Configuración** → **Avanzado** → **Obtener certificado** en el panel de inicio rápido de la ventana principal de Kaspersky Endpoint Security.
2. Especifique sus credenciales de la cuenta de red corporativa.
3. Si el administrador le ha proporcionado una contraseña de un solo uso, seleccione la casilla **Contraseña de un solo uso** y proporciónela.

   Se inicia el asistente de instalación de certificados.
4. Siga las instrucciones del Asistente.

Sincronizando con Kaspersky Security Center

Se requiere la sincronización del dispositivo móvil con el sistema de administración remota de Kaspersky Security Center para proteger su dispositivo y configurarlo según los requisitos de seguridad corporativa. El dispositivo se sincroniza con Kaspersky Security Center automáticamente, y también puede iniciar la sincronización manualmente. Después de la primera sincronización, su dispositivo se añade a la lista de dispositivos móviles administrados mediante Kaspersky Security Center. A continuación, el administrador puede configurar su dispositivo de acuerdo con los requisitos de seguridad corporativa.

Puede configurar la sincronización durante la ejecución del Asistente de configuración inicial o en la configuración de Kaspersky Endpoint Security. La configuración de sincronización debe estar definida si ha instalado Kaspersky Endpoint Security mediante Google Play. Solicite los valores de la configuración de sincronización al administrador del sistema.

Modifique la configuración de sincronización con el sistema de administración remota de Kaspersky Security Center solo cuando se lo indique el administrador.

Para sincronizar el dispositivo con Kaspersky Security Center:

1. Pulse → **Configuración** → **Sincronización** en el panel de inicio rápido de la ventana principal de Kaspersky Endpoint Security.
2. En la sección **Configuración de sincronización**, especifique los valores de los siguientes ajustes:
   - **Servidor**
   - **Puerto**
   - **Grupo**
   - **Dirección de correo electrónico corporativa**

   El administrador de configuración de la sincronización puede ocultar la configuración.
3. Pulse **Sincronizar**.

Activación de la aplicación Kaspersky Endpoint Security for Android sin Kaspersky Security Center

En la mayoría de los casos, el administrador activa la aplicación Kaspersky Endpoint Security for 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 introducir 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 introducir el código de activación:

1. En el mensaje de error que dice que su licencia caducará pronto o que ha caducado y que su dispositivo no está conectado al Servidor de administración, pulse **Activar**.
2. En la ventana de activación, introduzca el código de activación que le proporcionó el administrador y pulse **Activar**.
3. Si el código de activación es correcto, se muestra una notificación que indica que la aplicación se ha activado, junto con la fecha de caducidad de la licencia.

La aplicación Kaspersky Endpoint Security for Android en su dispositivo está activada.

Actualización de la app

Kaspersky Endpoint Security se puede actualizar de las siguientes maneras:

- Manualmente con Google Play. Puede descargar la nueva versión de la aplicación de Google Play e instalarla en el dispositivo.
- Con ayuda del administrador. El administrador puede actualizar de manera remota la versión de la aplicación en el dispositivo mediante el sistema de administración remota de Kaspersky Security Center.

Actualización de la aplicación desde Google Play

El administrador puede impedir que actualice 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:

- 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, cómo vincular el dispositivo a su cuenta o cómo utilizar la tienda de Google Play, visite el sitio web de soporte técnico 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 la actualización.

   La nueva versión de la aplicación se instalará en su dispositivo. La aplicación no requiere configuración adicional después de la actualización.

Eliminación de la app

El administrador puede impedir que elimine la aplicación usted mismo. Si es así, no puede eliminar Kaspersky Endpoint Security.

Kaspersky Endpoint Security se puede eliminar de los modos siguientes:

- Manualmente en la configuración de la aplicación.
- Manualmente en la configuración del dispositivo.

- Con ayuda del 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 de su dispositivo, siga estos pasos:

1. En el panel de inicio rápido de la ventana principal de Kaspersky Endpoint Security, pulse → **Desinstale la aplicación**.

   Esto inicia el asistente de eliminación de aplicaciones.

2. Siga las instrucciones del Asistente.

Eliminación en la configuración del dispositivo

Esta aplicación se elimina siguiendo el procedimiento estándar para la plataforma Android. Para eliminar la aplicación, se deben desactivar los derechos de administrador de Kaspersky Endpoint Security en la configuración de seguridad del dispositivo.

En dispositivos que ejecutan Android 7.0 o posterior, si el administrador ha bloqueado la eliminación, el dispositivo se bloqueará si se produce un intento de eliminar la aplicación en la configuración de Android. Para desbloquear el dispositivo, póngase en contacto con su administrador.

Eliminación mediante Kaspersky Security Center

Para eliminar una aplicación usando Kaspersky Security Center, se deben seguir estos 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. Confirmación de eliminación de aplicación.

   La aplicación se eliminará de su dispositivo.

Aplicaciones con un icono de maletín

Icono de la aplicación en el perfil de trabajo de Android

Las aplicaciones marcadas con un icono de maletín (aplicaciones corporativas) se almacenan en su dispositivo en el perfil de trabajo de Android (en adelante también llamado "perfil de trabajo"). El *perfil de trabajo de Android* es un entorno seguro en su dispositivo en el que el administrador puede gestionar aplicaciones y cuentas sin restringir sus capacidades de trabajo con datos personales.

El perfil de Work le permite almacenar datos corporativos por separado de los datos personales. Esto mantiene la confidencialidad de los datos corporativos y los protege contra malware. Cuando se crea un perfil de trabajo en su dispositivo, las aplicaciones corporativas siguientes se instalan automáticamente en el perfil de trabajo: Google Play Market, Google Chrome, Descargas, Kaspersky Endpoint Security for Android, entre otras.

Aplicación KNOX

Icono de 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 rápido, aplicaciones y widgets. El administrador puede gestionar aplicaciones y cuentas en un contenedor KNOX sin restringir sus capacidades de trabajar con datos personales.

Un contenedor KNOX le permite almacenar datos corporativos por separado de los datos personales. 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 información de contacto de empleados de la empresa, almacenamiento de archivos y otras aplicaciones.

Para obtener más información sobre el funcionamiento con KNOX, *visite el sitio web del soporte técnico de Samsung*.

Uso de la aplicación Kaspersky Security for iOS

Esta sección de Ayuda describe las funciones y operaciones que están disponibles para los usuarios de la app Kaspersky Security for 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 configura su dispositivo según los requisitos corporativos de seguridad. Es posible que algunas de las funciones y opciones que se describen en esta sección no se apliquen a su experiencia real con la app. Si tiene alguna pregunta sobre la app instalada en un dispositivo específico, comuníquese con su administrador.

Funciones de la aplicación

Kaspersky Security for iOS ofrece las siguientes funciones clave.

Protección contra amenazas en línea

El componente Protección web ofrece protección contra amenazas en línea.

Protección web bloquea los sitios web maliciosos que distribuyen un código malicioso y los sitios web de phishing diseñados para robar datos confidenciales y obtener acceso a sus cuentas bancarias. Protección web utiliza el servicio en la nube de Kaspersky Security Network para analizar sitios web antes de abrirlos. 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 añada una configuración de VPN.

Detección de liberación

Cuando Kaspersky Security for 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

Instalación de la aplicación

Para instalar la aplicación Kaspersky Security for iOS:

1. Busque el mensaje de correo electrónico con la invitación del administrador para instalar la aplicación Kaspersky Security for iOS desde la App Store.
2. Vaya a la App Store de una de las siguientes maneras:
   - Toque el enlace 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 un ordenador.

   El enlace de invitación es válido durante 24 horas. Si no logra instalar la aplicación a tiempo, póngase en contacto 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 for iOS se instala en su dispositivo. Para proteger el dispositivo, active la aplicación.

Activación de la aplicación

Para activar la aplicación Kaspersky Security for iOS, siga estos pasos:

1. Inicie la aplicación en su dispositivo.
2. Acepte los contratos y las declaraciones seleccionando las casillas **Contrato de licencia de usuario final** y **Política de Privacidad de Productos y Servicios**.

   O bien, puede aceptar la **Declaración de Kaspersky Security Network** para permitir el envío de estadísticas a Kaspersky Security Network. Esto mejora el rendimiento de la aplicación y garantiza su funcionamiento ininterrumpido.
3. Pulse **Siguiente**. La aplicación se conecta al sistema de administración remota de Kaspersky Security Center y obtiene la información de la licencia.
4. Permita que la aplicación añada 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 for iOS en su dispositivo está activada.

Activar la aplicación con un código de activación

Cuando instala la aplicación Kaspersky Security for 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 introducir 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 introducir el código de activación:

1. En el mensaje que indica que la aplicación no está activada, pulse **Activar la app**.
2. En la ventana de activación, introduzca el código de activación que le proporcionó el administrador y pulse **Activar**.

   Si el código de activación es correcto, se muestra una notificación que indica que la aplicación se ha activado, junto con la fecha de caducidad de la licencia.

La aplicación Kaspersky Security for iOS en su dispositivo está activada.

Ventana principal de un vistazo

El aspecto de la ventana principal varía ligeramente de una resolución de pantalla a otra.

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 le 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 le informan sobre eventos de importancia crítica para la seguridad del dispositivo.

Puede pulsar un mensaje para ver los detalles.

Actualización de la app

Puede descargar la última versión de la aplicación Kaspersky Security for 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 app

Para eliminar la aplicación Kaspersky Security for iOS, siga el procedimiento estándar en la plataforma iOS:

1. En la pantalla de inicio, mantenga pulsado el icono de la aplicación.
2. Elimine la aplicación.

La aplicación Kaspersky Security for iOS se elimina de su dispositivo.

Licencia de aplicaciones

Esta sección proporciona información sobre los términos generales relacionados con la licencia de Kaspersky Security for Mobile.

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 for Mobile.

Le recomendamos que lea detenidamente los Términos y condiciones del EULA antes de utilizar Kaspersky Security for Mobile.

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

- Durante la instalación de componentes de Kaspersky Security for Mobile.
- 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 for Android.
- En la sección **Información de la aplicación** en Kaspersky Endpoint Security for Android.
- En la sección **Sobre la app** → **Contratos y Declaraciones** en Kaspersky Security for iOS.
- En la sección **Avanzado** → **Contratos de licencia aceptados** de 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 for Mobile, también indica que acepta los Términos y condiciones del Contrato de licencia de usuario final. Si no acepta los términos del Contrato de licencia de usuario final, debe cancelar la instalación de los componentes de Kaspersky Security for Mobile y abstenerse de utilizarlos.

Información sobre la licencia

Una licencia es un derecho de duración limitada para utilizar la solución integrada Kaspersky Security for Mobile 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:

- *Evaluación*.

Licencia gratuita con el fin de probar Kaspersky Security for Mobile.

La licencia de evaluación es válida durante 30 días. Cuando la licencia de la evaluación caduque, las aplicaciones móviles Kaspersky Endpoint Security for Android o Kaspersky Security for 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 for Mobile.

  Cuando la licencia comercial expire, la aplicación móvil continuará funcionando, pero con funcionalidad limitada.

  En el modo de funcionalidad limitada, los siguientes componentes están disponibles según la aplicación.

  - Aplicación Kaspersky Endpoint Security for 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 for Android deja de intercambiar la 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 evaluación caduca o si falta una licencia (el código de activación se elimina de la directiva de grupo).

  - Aplicación Kaspersky Security for iOS:
    - **Sincronización con el Servidor de administración**.

    Kaspersky Security for iOS deja de intercambiar información con Kaspersky Security Network si la licencia de evaluación 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 utilizar directivas del grupo para administrar estos componentes en el modo de funcionalidad limitada. No puede usar directivas 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 período de la licencia o comprar una nueva antes de que caduque la actual.

Acerca de la suscripción

Suscripción para Kaspersky Security for Mobile 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 for Mobile 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 for Mobile 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 for Mobile 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 for Mobile.

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 for Mobile conforme a las condiciones del Contrato de licencia de usuario final. Los especialistas de Kaspersky generan las claves.

Puede añadir una clave para la aplicación móvil mediante un fichero llave o código de activación:

- Si su organización ha implementado 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 for 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 en caso de, por ejemplo, incumplimiento de las condiciones del Contrato de licencia. Cuando la clave esté bloqueada, la aplicación móvil dejará de realizar todas sus funciones excepto la sincronización con el Servidor de administración. Para continuar usando la aplicación, tiene que 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 añadir una clave que activa la aplicación móvil Kaspersky Endpoint Security for Android o Kaspersky Security for 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 for Mobile o bien después de pedir la versión de evaluación de Kaspersky Security for Mobile.

Para activar la aplicación móvil con un código de activación, se necesita contar con acceso 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 añadir una clave que active la aplicación Kaspersky Endpoint Security for Android.

No puede activar la aplicación Kaspersky Security for iOS con un fichero llave.

Se envía el fichero clave a la dirección de correo electrónico que se especificó tras adquirir la solución integrada de Kaspersky Security for Mobile o bien después de pedir la versión de evaluación de Kaspersky Security for Mobile.

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 el vendedor de la licencia.
- Reciba un fichero llave desde el sitio web de Kaspersky utilizando su código de activación disponible.

Provisión de datos en Kaspersky Endpoint Security for Android

Kaspersky Security for Mobile cumple con el Reglamento General de Protección de Datos (RGPD).

Para instalar la aplicación, usted o el usuario del dispositivo deben leer y aceptar los términos del Contrato de licencia de usuario final. Además, puede configurar una política para aceptar las declaraciones enumeradas a continuación de forma global para todos los usuarios. De lo contrario, los usuarios recibirán una notificación en la pantalla principal de la aplicación para aceptar las siguientes declaraciones con respecto al procesamiento de los datos personales del usuario:

- Declaración de Kaspersky Security Network
- Declaración relativa al procesamiento de datos para Protección web
- Declaración relativa al procesamiento de la información para fines de marketing

Si elige aceptar las declaraciones de forma global, las versiones de las declaraciones aceptadas mediante Kaspersky Security Center deben coincidir con las versiones ya aceptadas por los usuarios. De lo contrario, se 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 los términos de una declaración o rechazarlos en cualquier momento en la sección **Información de la aplicación** en la configuración de Kaspersky Endpoint Security for Android.

Intercambio de información con Kaspersky Security Network

Para mejorar la protección en tiempo real, Kaspersky Endpoint Security for 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 en línea de Kaspersky para comprobar la reputación de 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 usar todas las funciones 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 los usuarios según listas de categorías permitidas y bloqueadas (por ejemplo, la categoría "Comunicación por Internet").

- **Control de aplicaciones.** La aplicación determina la categoría de la aplicación para restringir el inicio de aplicaciones que no cumplan con los requisitos corporativos de seguridad 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 aplicaciones está disponible en el Contrato de licencia de usuario final. Al aceptar los términos y las condiciones del Contrato de licencia, acepta transferir esta información.

La información sobre los tipos de datos enviados a Kaspersky cuando se usa KSN durante el funcionamiento de Protección web está disponible en la Declaración sobre el procesamiento de datos para Protección web. Al aceptar los términos y las condiciones de la Declaración, acepta transferir esta información.

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 Kaspersky Endpoint Security for Android. Al aceptar los términos y las condiciones de la Declaración, acepta transferir esta información.

Disposición de datos según el contrato de licencia de usuario final

Cuando se utiliza el Código de activación para activar el Software, con el fin de verificar su uso legítimo, el Usuario final se compromete a proporcionar periódicamente al Titular de los derechos la siguiente información:

- formato de los datos en la solicitud a la infraestructura del titular de los derechos; dirección IPv4 del servicio web a la que se accedió; tamaño del contenido de la solicitud a la infraestructura del titular de los derechos; ID de protocolo; código de activación del Software; tipo de compresión de datos; ID 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 extendida sobre 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 del 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 utilizado para proveer la licencia del Software; fecha y hora de caducidad de la licencia de Software; estado actual de la clave de la licencia del Software; tipo de licencia del Software utilizada; tipo de licencia usada para activar el Software; ID del Software derivado de la licencia.

Con el fin de proteger el Ordenador de las amenazas a la seguridad de la información, el Usuario final acepta proporcionar al Titular de los derechos la siguiente información:

- tipo de suma de comprobación del objeto que se procesa; suma de comprobación del objeto que se procesa; ID del componente del software;
- ID del registro activado en las bases de datos Anti-virus del software; marca de tiempo del registro activado en las bases de datos Anti-virus del software; tipo de registro activado en las bases de datos Anti-virus del software; nombre del software malicioso detectado o del software legítimo que puede usarse para dañar el dispositivo o los datos del usuario;
- nombre de la tienda desde donde se instaló la aplicación; nombre del paquete de la aplicación; clave pública empleada para firmar el archivo APK; suma de comprobación del certificado empleado para firmar el archivo APK; marca de tiempo del certificado digital;
- versión completa del Software; ID de actualización de software; tipo de software instalado; el identificador de configuración; el resultado de la acción del software; código del 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 Usted utiliza los servidores de actualización del Titular de los derechos para descargar las actualizaciones, el Usuario final, con el fin de mejorar la eficacia del procedimiento de actualización, acepta proporcionar al Titular de los derechos la siguiente información de forma periódica:

- ID del Software derivado de la licencia; versión completa del Software; ID de la licencia del Software; tipo de licencia del software utilizada; 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 está protegida por Kaspersky de acuerdo con los requisitos establecidos por ley. La información original recibida se guarda en formato cifrado y se destruye según se acumula (dos veces al año) o a petición del usuario. Las estadísticas generales se almacenan indefinidamente.

Disposición de datos de la declaración de Kaspersky Security Network

El uso de KSN puede aumentar la eficacia de la protección proporcionada por el Software contra las amenazas informáticas y de red.

Si usa una licencia para 5 o más nodos, el Titular de los derechos recibirá y procesará automáticamente los siguientes datos mientras use KSN:

- ID del registro activado en las bases de datos Anti-virus del software; marca de tiempo del registro activado en las bases de datos Anti-virus del software; tipo de registro activado en las bases de datos Anti-virus del software; fecha y hora 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 extendida sobre 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; aviso que muestra 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 de tipo de objeto; la decisión del software sobre el objeto que se procesa; ruta al objeto que se procesa; código de directorio; versión del componente del software; versión de las estadísticas que se envían; 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 objetos analizados (versión de la aplicación desde 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 empleado 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 empleada para firmar el archivo APK; suma de comprobación del certificado empleado para firmar el archivo APK; fecha y hora de caducidad del certificado; fecha y hora de emisión del certificado; versión de las estadísticas que se envían; 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 forma dinámica a la aplicación; versión del software de terceros; mensaje que indica si la aplicación es la mensajería SMS predeterminada; aviso para indicar si la aplicación cuenta con derechos de Administrador del Dispositivo; mensaje que indica si la aplicación está en el catálogo del sistema; aviso para indicar si la aplicación utiliza 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 los fragmentos en el 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; nombre y configuración del titular del certificado; huella digital del certificado del objeto analizado y algoritmo de hash; 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 del 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 completa; ruta al objeto que se procesa; información sobre los resultados de la comprobación de la firma del archivo; clave de sesión de inicio; algoritmo de encriptación para la clave de inicio de sesión; tiempo de almacenamiento para el objeto que se procesa; algoritmo para calcular la huella digital del certificado digital);

- tipo de compilación, por ejemplo "user" o "eng"; nombre completo del producto; fabricante del producto o hardware; si se pueden instalar apps desde fuera de Google Play; estado del servicio en la nube para la verificación de las aplicaciones de Google; estado del servicio en la nube para la verificación de las apps de Google que se instalan por medio de ADB; el nombre en clave del desarrollo actual o "REL" para las 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; aviso para indicar si el dispositivo está comprometido; sistema operativo; nombre del software; tipo de licencia del software utilizada;

- 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 cuando se dejaron de recibir las estadísticas; cantidad de conexiones KSN tomadas desde la caché; cantidad de solicitudes para las que se encontró una respuesta en la base de datos local de solicitudes; cantidad de conexiones de KSN no exitosas; cantidad de transacciones KSN fallidas; distribución temporal de solicitudes canceladas a KSN; distribución temporal de conexiones KSN fallidas; distribución temporal de transacciones KSN fallidas; distribución temporal de conexiones KSN exitosas; distribución temporal de transacciones exitosas de KSN; distribución temporal de solicitudes exitosas a KSN; distribución temporal de las solicitudes KSN expiradas; cantidad de conexiones KSN

nuevas; cantidad de solicitudes fallidas a KSN causadas por errores de enrutamiento; cantidad de solicitudes fallidas causadas por la desactivación de KSN en la configuración del Software; cantidad de solicitudes fallidas a KSN causadas por problemas de red; cantidad de conexiones KSN realizadas con éxito; cantidad de transacciones KSN exitosas; Cantidad total de solicitudes a KSN; fecha y hora en que las estadísticas comenzaron a recibirse);

- ID del dispositivo; versión completa del Software; ID de actualización de software; ID de instalación del software (PCID); tipo de software instalado;

- Alto 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 al archivo APK sin el nombre de archivo; altura de superposición; información sobre el software superpuesto: hash MD5 del archivo APK; información sobre la aplicación superpuesta: hash MD5 del archivo classes.dex; información sobre la aplicación superpuesta: nombre del archivo APK; información sobre la aplicación superpuesta: ruta al archivo APK sin el nombre de archivo; información sobre la aplicación superpuesta: nombre del paquete de la aplicación (para la aplicación superpuesta: si el anuncio se muestra en un escritorio vacío, el valor debe ser "ejecutor"); fecha y hora de la superposición; información sobre la aplicación superpuesta: nombre del paquete de la aplicación; ancho de la superposición;

- configuración del punto de acceso Wi-Fi en uso (tipo de dispositivo detectado; configuración 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 longitud del prefijo de red; suma de comprobación de la dirección local IPv6); 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 red wifi; lista de redes wifi disponibles y su configuración; 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 compatibles con el punto de acceso de wifi; tipo de cifrado de red wifi; hora local de inicio y finalización de la conexión de red wifi; ID de red wifi basada en la dirección MAC del punto de acceso; ID de la red wifi basada en el nombre de la red wifi; ID de red wifi basada en el nombre de la red wifi y la dirección MAC del punto de acceso; fuerza de la señal de Wi-Fi; el nombre de la red wifi; conjunto de protocolos de autenticación que admite esta configuración; protocolo de autenticación usado para una conexión WPA-EAP; protocolo de autenticación interna; conjunto de cifrados de grupo que admite esta configuración; conjunto de protocolos de administración de claves que admite esta configuración; la categoría de privacidad final de la red en el software; la categoría de seguridad final de la red en el software; conjunto de cifrados de bloque para WPA que admite esta configuración; conjunto de protocolos de seguridad compatibles con esta configuración);

- fecha y hora de instalación del software; fecha de activación del software; identificador de la organización asociada a través de la cual se realizó el pedido de licencia 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, para lograr el objetivo declarado de aumentar la eficacia de la protección proporcionada por el Software, el Titular de los derechos puede recibir objetos que los intrusos podrían explotar para dañar el Ordenador y crear amenazas de seguridad de la información.

Proporcionar la información anterior a la KSN es un acto voluntario. Puede dejar de participar en Kaspersky Security Network en cualquier momento.

Disposición de datos conforme a la Declaración relativa al 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 detectar amenazas web y determinar 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 los 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 URL, URL, que hace referencia a la información solicitada.

Disposición de datos en la declaración relativa al procesamiento de la información para fines de marketing

El Titular de los derechos utiliza sistemas de información de terceros para procesar la información. Su procesamiento de datos se rige por las declaraciones de privacidad de dichos sistemas de información de terceros. Los siguientes servicios son los que utiliza el titular de los derechos utiliza y los datos que se procesan:

Google Analytics para Firebase

Durante el uso del Software, se enviarán los siguientes datos a Google Analytics para Firebase de forma automática y periódica con el fin de alcanzar el objetivo declarado:

- información de la aplicación (versión, ID de la aplicación, ID de la aplicación de servicios de Firebase, ID de instancia de servicio de Firebase, nombre del establecimiento en el que se obtuvo la aplicación, fecha y hora del primer lanzamiento del Software)
- El ID de instalación de la aplicación en el dispositivo y el método de instalación en el dispositivo
- información sobre la región y el idioma de localización
- información de la resolución de la pantalla del dispositivo
- información sobre la obtención de root del usuario
- la información de diagnóstico sobre el dispositivo desde el servicio SafetyNet Attestation
- la información sobre la configuración de Kaspersky Endpoint Security for Android como herramienta de Accesibilidad
- información sobre las transiciones entre pantallas de aplicaciones, duración de las sesiones, comienzo y final de las sesiones en pantalla, nombre de la pantalla
- información sobre el protocolo utilizado para enviar datos al servicio de Firebase, su versión y el número de identificación del método utilizado para el envío de datos
- los datos sobre el tipo y los parámetros del evento para el que se presentan los datos
- información sobre la licencia de la aplicación, su disponibilidad y el número de dispositivos
- información sobre la frecuencia de las actualizaciones de la base de datos de antivirus y la sincronización con el Servidor de administración
- información sobre la Consola de administración (Kaspersky Security Center o sistemas EMM de terceros)

- ID de Android
- ID de publicidad
- información sobre el Usuario: la categoría de edad y el género, el identificador del país de residencia y la lista de intereses
- información sobre el equipo del Usuario en el que se ha instalado el Software: el nombre del fabricante del ordenador, el tipo de ordenador, la versión y el idioma (configuración regional) del sistema operativo, la información sobre la aplicación abierta por primera vez en los últimos 7 días y la aplicación abierta por primera vez hace más de 7 días

  La transmisión de datos al servicio Firebase se realiza a través de un canal seguro. La información sobre cómo se tratan los datos en Firebase está publicada en: https://firebase.google.com/support/privacy.

SafetyNet Attestation

Durante el uso del Software, se enviarán los siguientes datos a SafetyNet Attestation de forma automática y periódica con el fin de alcanzar el objetivo declarado:

- el tiempo de comprobación del dispositivo
- la información sobre el software, nombre y datos sobre los certificados del software
- los resultados de comprobación del dispositivo
- las comprobaciones al azar de los números de identificación para verificar los resultados de comprobación del dispositivo

  La transmisión de datos a SafetyNet Attestation se realiza a través de un canal seguro. La información sobre cómo se tratan los datos en SafetyNet Attestation está publicada en: https://policies.google.com/privacy.

Firebase Performance Monitoring

Durante el uso del Software, se enviarán los siguientes datos al Firebase Performance Monitoring de forma automática y periódica con el fin de alcanzar el objetivo 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
- aviso para indicar si el dispositivo está comprometido
- fuerza de la señal
- duración de los rastros automatizados
- red y la información correspondiente a continuación: código de respuesta, tamaño de la carga útil en bytes, tiempo de respuesta
- descripción del dispositivo

  La transmisión de datos al servicio de Firebase Performance Monitoring se realiza a través de un canal seguro. La información sobre cómo se procesan los datos en Firebase Performance Monitoring está publicada en: https://firebase.google.com/support/privacy.

Crashlytics

Durante el uso del Software, se enviarán los siguientes datos a Crashlytics de forma automática y periódica con el fin de alcanzar el objetivo declarado:

- ID del Software
- versión del Software instalado
- mensaje que indica si el software estaba en ejecución en segundo plano
- arquitectura del 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
- aviso para indicar si el dispositivo está comprometido
- orientación de la pantalla al momento del evento
- fabricante del producto o hardware
- ID de instalación único
- versión de las estadísticas que se envían
- tipo de excepción de software
- texto del mensaje de error
- mensaje que indica que la excepción de software fue provocada por una excepción anidada

- ID de subproceso
- mensaje que indica si el marco fue el motivo del error de software
- mensaje 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 del evento, fecha y hora del evento, tipo y valor del evento
- valores de registro del CPU
- el tipo y el valor del evento

  La transmisión de datos a Crashlytics se realiza a través de un canal seguro. La información sobre cómo se tratan los datos en Crashlytics está publicada en: https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

El envío de la información anterior para su procesamiento con fines de comercialización es voluntario.

Provisión de datos en Kaspersky Security for iOS

Kaspersky Security for Mobile cumple con el Reglamento General de Protección de Datos (RGPD).

Para instalar la aplicación, el usuario de un dispositivo debe leer y aceptar los términos de las 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 **Sobre la app** → **Contratos y Declaraciones** dentro de la configuración de Kaspersky Security for 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 for 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.

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 Kaspersky Security for iOS. Al aceptar los términos y las condiciones de la Declaración, acepta transferir esta información.

Disposición de datos según el contrato de licencia de usuario final

Cuando se utiliza el Código de activación para activar el Software, con el fin de verificar su uso legítimo, el Usuario final se compromete a proporcionar periódicamente al Titular de los derechos la siguiente información:

- Formato de los datos en la solicitud a la infraestructura del Titular de los derechos; dirección IPv4 del servicio web a la que se accedió; tamaño del contenido de la solicitud a la infraestructura del titular de los derechos; ID de protocolo; código de activación del Software; tipo de compresión de datos; ID 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 extendida sobre la edición del SO; modelo del dispositivo; código del operador 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 del 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 utilizado para proveer la licencia del Software; fecha y hora de caducidad de la licencia de Software; estado actual de la clave de la licencia del Software; tipo de licencia del Software utilizada; tipo de licencia usada para activar el Software; ID del Software derivado de la licencia.

El Titular de los derechos puede utilizar dicha información también para recopilar información estadística sobre la distribución y el uso del Software del Titular de los derechos.

Con el fin de proteger el Ordenador de las amenazas a la seguridad de la información, el Usuario final acepta proporcionar al Titular de los derechos la siguiente información:

- Formato de los datos en la solicitud a la infraestructura del Titular de los derechos; dirección del servicio web a la que se accedió (URL, IP); número del puerto; dirección web de la fuente de la solicitud del servicio web (árbitro).

- versión completa del Software; ID de actualización de software; tipo de Software instalado; ID del Software; el identificador de la configuración; el resultado de la acción del Software; código del error.

- dirección web que se procesa; dirección IPv4 del servicio web a la que se accedió; huella digital del certificado del objeto analizado y algoritmo de hash; tipo de certificado; contenidos del certificado digital que se procesa.

Disposición de datos de 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 cuando se dejaron de recibir las estadísticas; cantidad de conexiones KSN tomadas desde la caché; cantidad de solicitudes para las que se encontró una respuesta en la base de datos local de solicitudes; cantidad de conexiones de KSN no exitosas; cantidad de transacciones KSN fallidas; distribución temporal de solicitudes canceladas a KSN; distribución temporal de conexiones KSN fallidas; distribución temporal de transacciones KSN fallidas; distribución temporal de conexiones KSN exitosas; distribución temporal de transacciones exitosas de KSN; distribución temporal de solicitudes exitosas a KSN; distribución temporal de las solicitudes KSN expiradas; cantidad de conexiones KSN nuevas; cantidad de solicitudes fallidas a KSN causadas por errores de enrutamiento; cantidad de solicitudes fallidas causadas por la desactivación de KSN en la configuración del Software; cantidad de solicitudes fallidas a KSN causadas por problemas de red; cantidad de conexiones KSN realizadas con éxito; cantidad de transacciones KSN exitosas; cantidad total de solicitudes a KSN; fecha y hora en que las estadísticas comenzaron a recibirse).

- ID del dispositivo; versión completa del Software; ID de actualización de 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 instalado en el equipo del usuario; versión de bits del sistema operativo.

Proporcionar la información anterior a la KSN es un acto voluntario. Puede dejar de participar en Kaspersky Security Network en cualquier momento.

Póngase en contacto con Servicio de soporte técnico

En esta sección se describe cómo 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 for Mobile o las fuentes de información sobre Kaspersky Security for Mobile, 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 for Mobile.

Kaspersky ofrece asistencia técnica para Kaspersky Security for Mobile durante su vida útil (consulte la página de vida útil del soporte técnico del producto). Antes de ponerse en contacto con el Servicio de soporte técnico, lea las reglas de 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 al Servicio de soporte técnico desde el portal Kaspersky CompanyAccount

Soporte técnico a través de Kaspersky CompanyAccount

Kaspersky CompanyAccount es un portal para compañías que utilizan 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 llevar un seguimiento del estado de sus solicitudes en línea y también almacenar un historial de estas.

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 de Soporte técnico.

Fuentes de información sobre la aplicación

Página web de Kaspersky Security for Mobile en el sitio web de Kaspersky

En la página de Kaspersky Security for Mobile encontrará información general sobre la aplicación y sus funciones, así como parámetros de funcionamiento.

En la página web de Kaspersky Security for Mobile encontrará un enlace a la tienda electrónica. Donde podrá comprar la aplicación o hacer la renovación.

Página web de Kaspersky Security for Mobile en la Base de conocimientos

La *Base de conocimientos* es una sección del sitio web de soporte técnico.

En la página de Kaspersky Security for Mobile de la Base de conocimientos, encontrará artículos con información útil, recomendaciones y respuestas a preguntas frecuentes sobre la compra, 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 for Mobile, 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 for Mobile ofrece información sobre las ventanas de Kaspersky Security Center: consisten en una descripción de la configuración de Kaspersky Security for Mobile 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 for Android y Kaspersky Security for iOS proporciona información la configuración y el uso de las aplicaciones móviles.

Debate 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

Cambio de la aplicación al modo completamente funcional. El usuario lleva a cabo la activación de la aplicación durante la instalación de la aplicación o después de esta. Debe tener un código de activación o un fichero llave 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 Administración 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 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 contra la seguridad de los equipos conocidas por Kaspersky en el momento en que se publican las bases de datos antivirus. Las entradas en bases de datos antivirus permiten detectar códigos maliciosos en objetos escaneados. Los autores de estas bases de datos antivirus, actualizadas cada hora, son especialistas de Kaspersky.

Categorías de Kaspersky

Categorías de datos predefinidas desarrolladas por expertos de Kaspersky. Las categorías se pueden actualizar durante las actualizaciones de la base de datos de aplicaciones. Un encargado de 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 es necesario para activar la aplicación.

El código de activación es una secuencia única de veinte letras y números con el formato xxxxx-xxxxx-xxxxx-xxxxx.

Código de desbloqueo

Un código que puede obtener en Kaspersky Security Center. Es necesario desbloquear un dispositivo después de ejecutar los comandos **Bloquear y Localizar**, **Alarma** o **Foto de identificación** y cuando se activa la Autoprotección.

Complemento de administración de la aplicación

Componente especializado que proporciona la interfaz para administrar aplicaciones de Kaspersky a través de 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 se pueden administrar mediante Kaspersky Security Center.

Contrato de licencia de usuario final

El contrato entre usted y AO Kaspersky Lab que estipula los términos bajo los que usted puede usar la aplicación.

Control de cumplimiento

Verificación del cumplimiento de los requisitos de seguridad corporativa por parte de un dispositivo móvil y Kaspersky Endpoint Security for Android. Los requisitos corporativos de seguridad 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 componentes siguientes:

- El criterio de comprobación de dispositivo (por ejemplo, ausencia de aplicaciones prohibidas en el dispositivo)
- El intervalo de tiempo asignado para que el usuario resuelva el 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 que la aplicación de Kaspersky mueve los objetos probablemente infectados que se han detectado. Los objetos se almacenan en Cuarentena en forma cifrada para evitar impactos en el equipo.

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 de iOS.

Dispositivo EAS

Un dispositivo móvil conectado al Servidor de administración a través del protocolo Exchange ActiveSync.

Dispositivo supervisado

Un dispositivo iOS con configuración controlada por Apple Configurator, un programa para la configuración grupal de dispositivos iOS. Los dispositivos supervisado tienen el estado *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. No es posible sincronizar los dispositivos supervisados cuando la aplicación Apple Configurator está instalada en otro equipo.

Cada dispositivo supervisado proporciona más configuraciones a 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 controlar el tráfico de Internet en un dispositivo dentro de la red corporativa. De forma predeterminada, todos los dispositivos móviles son de tipo no supervisado.

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.

Fichero llave

Un archivo con formato de xxxxxxxx.key que permite usar una aplicación de Kaspersky con una licencia de prueba o comercial. La aplicación genera el fichero llave según el código de activación. Solo puede usar la aplicación cuando tenga un fichero llave.

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 a correo electrónico. A diferencia del protocolo POP3, IMAP proporciona funciones adicionales para el uso de buzones de correo, entre ellas la gestión de carpetas y el uso de mensajes sin tener que copiar el contenido desde el 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 actualizada 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 de duración limitada para utilizar la aplicación que se le concede en 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 que se incluyen 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

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 datos personales al usuario. Cuando se crea un perfil de trabajo en el dispositivo móvil del usuario, se instalan automáticamente las siguientes aplicaciones corporativas en el perfil de trabajo: Google Play Market, Google Chrome, Descargas, Kaspersky Endpoint Security for Android, entre 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 app Google Play Market. Las apps instaladas en el perfil de trabajo aparecen en la lista común de apps.

Perfil del aprovisionamiento

Colección de configuraciones para la operación de aplicaciones en dispositivos iOS móviles. Un perfil de aprovisionamiento contiene información sobre la licencia y está vinculado a una aplicación específica.

Phishing

Clase de estafa en Internet destinada a obtener acceso no autorizado a los datos confidenciales de usuarios.

Plazo de la licencia

Un período de tiempo durante el cual el usuario tiene acceso a las funciones de la aplicación y derechos para usar servicios adicionales. Los servicios que puede usar dependen del tipo de licencia.

POP3

Protocolo de red usado por un cliente de correo para recibir mensajes de un servidor de correo.

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 de 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 gestión de esos dispositivos móviles iOS a través del servicio Apple Push Notification (APNs).

Servidor proxy

Un servicio de red de ordenadores que permite a los usuarios realizar solicitudes indirectas a otros servicios de red. Primero, un usuario se conecta a un servidor proxy y solicita un recurso (p. ej., un archivo) ubicado en otro servidor. A continuación, el servidor proxy se conecta al servidor especificado y obtiene el recurso o lo devuelve desde su propia caché (si la tiene). En algunos casos, el servidor proxy puede modificar una solicitud de un usuario o la respuesta de un servidor para un propósito concreto.

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.

Servidores de actualizaciones de Kaspersky

Servidores HTTP(S) de Kaspersky desde los que las aplicaciones de Kaspersky descargan actualizaciones del módulo de la aplicación y base de datos.

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 según los parámetros seleccionados (fecha de caducidad y número de dispositivos). Puede poner en pausa 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.

Virus

Un programa que infecta otros al añadirles su código, con el fin de hacerse con el control cuando se ejecutan los archivos infectados. Esta simple definición permite identificar la acción principal realizada por cualquier virus: infectar.

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 for Android)
- legal_notices_iOS.txt (para la aplicación Kaspersky Security for iOS)

En dispositivos móviles, la información acerca del código de terceros está disponible en la sección **Sobre 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 de 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 está 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 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.