ESET Endpoint Security for Android

Manual de usuario

Haga clic aquí para ver la versión de la Ayuda de este documento

Digital Security
Progress. Protected.

Copyright ©2023 de ESET, spol. s r.o.

ESET Endpoint Security for Android está desarrollado por ESET, spol. s r.o.

Para obtener más información, visite https://www.eset.com.

Todos los derechos reservados. Ninguna parte de esta documentación podrá reproducirse, almacenarse en un sistema de recuperación ni transmitirse en forma o modo alguno, ya sea por medios electrónicos, mecánicos, fotocopia, grabación, escaneo o cualquier otro medio sin la autorización por escrito del autor.

ESET, spol. s r.o. se reserva el derecho de modificar cualquier parte del software de aplicación descrito sin previo aviso.

Soporte técnico: https://support.eset.com

REV. 31/03/2023

Introducción

La nueva generación de ESET Endpoint Security for Android (EESA) está diseñada para funcionar con ESET PROTECT y ESET PROTECT Cloud, la nueva consola de administración que permite la administración remota de todas las soluciones de seguridad de ESET.

La versión 3 de ESET Endpoint Security for Android es compatible con:

- ESET Security Management Center 7,
- ESET PROTECT y ESET PROTECT Cloud

ESET Endpoint Security for Android se ha diseñado para proteger los dispositivos móviles corporativos de las amenazas de malware más recientes, y para proteger sus datos hasta si pierde su dispositivo o se lo roban. Además, ayuda a los administradores del sistema a mantener sus dispositivos de conformidad con las políticas de seguridad de la empresa.

ESET Endpoint Security for Android también puede aplicarse en pymes sin necesidad de administración remota a través de ESET PROTECT. El técnico informático, el administrador del sistema o el propio usuario de puede simplemente compartir su configuración de ESET Endpoint Security for Android con otros compañeros de trabajo. Este proceso reduce al mínimo la necesidad de activar el producto y configurar cada uno de los módulos del mismo manualmente, tareas que de otro modo serían necesarias justo después de la instalación de ESET Endpoint Security for Android.

Novedades de la versión 3

Seguridad del dispositivo - Administración de actualizaciones del sistema

En la versión 3 de ESET Endpoint Security for Android puede administrar las actualizaciones de Android desde ESET PROTECT Cloud.

Control de acceso web

En la versión 3 de ESET Endpoint Security for Android puede regular el acceso a sitios web de sus empleados desde ESET PROTECT Cloud.

Requisitos mínimos del sistema

Para poder instalar ESET Endpoint Security for Android, su dispositivo Android debe cumplir con los siguientes requisitos mínimos del sistema:

- Sistema operativo: Android 5 (Lollipop) y posterior
- Resolución de la pantalla táctil: 480 × 800 píxeles
- CPU: ARM con conjunto de instrucciones ARMv7 e x86 Intel Atom
- Espacio de almacenamiento libre: 20 MB

- Conexión a Internet

Android Go no admitido

No es compatible con dispositivos con doble SIM o acceso raíz. Algunas funciones (por ejemplo, Antirrobo y Filtro de llamadas) no están disponibles en tabletas que no permiten realizar llamadas ni enviar mensajes.

Registro de cambios

Conexión de usuarios a ESET PROTECT y ESET PROTECT Cloud

ESET PROTECT y ESET PROTECT Cloud son aplicaciones que le permiten administrar los productos de ESET en un entorno de red desde una ubicación central. El sistema de administración de tareas de ESET PROTECT y ESET PROTECT Cloud le permite instalar soluciones de seguridad de ESET en ordenadores remotos y responder rápidamente a nuevos problemas y amenazas. ESET PROTECT no proporciona protección frente a código malicioso por sí solo. Sino que confía en la presencia de soluciones de seguridad de ESET en cada cliente.

Las soluciones de seguridad de ESET son compatibles con redes que incluyan varios tipos de plataforma. Su red puede incluir una combinación de sistemas operativos actuales de Microsoft, Linux, macOS y sistemas operativos de dispositivos móviles (teléfonos móviles y tabletas).

ESET PROTECT y ESET PROTECT Cloud representan una nueva generación de un sistema de administración remota que presenta diferencias significativas con respecto a las versiones anteriores de ESET Remote Administrator. Puede comprobar la compatibilidad con versiones anteriores de productos de seguridad de ESET aquí:

- Productos compatibles con ESET PROTECT
- Productos compatibles con ESET PROTECT Cloud

Encontrará las diferencias entre ESET PROTECT y en la documentación de ESET PROTECT Cloud.

Si desea obtener más información, consulte:
- Documentación en línea de ESET PROTECT.
- Documentación en línea de ESET PROTECT Cloud.

Instalación remota

La instalación remota de ESET Endpoint Security for Android desde ESET PROTECT requiere lo siguiente:

- Instalación de Mobile Device Connector
- Inscripción de dispositivos móviles

Contextos de instalación de ESET Endpoint Security for Android

- El administrador envía por correo electrónico el vínculo de inscripción, el archivo APK de instalación y un proceso de instalación a los usuarios finales. El usuario pulsa el vínculo de inscripción y se le redirige al navegador de Internet Predeterminado de Android. El dispositivo ESET Endpoint Security for Android se inscribe y se conecta a ESET PROTECT. Si ESET Endpoint Security for Android no está instalado en el dispositivo, se redirigirá al usuario a la tienda de Google Play para que descargue la aplicación. Una vez descargada la aplicación, se sigue un proceso de instalación estándar.

- El administrador envía por correo electrónico el archivo de configuración de la aplicación, el archivo APK de instalación y un proceso de instalación a los usuarios finales. Tras la instalación, el usuario debe abrir el archivo de configuración de la aplicación. Se importan todos los ajustes y la aplicación se activa (siempre que se haya incluido la información de la licencia).

Inscripción de dispositivos con posibilidades de entrada limitadas

ESET Endpoint Security for Android le permite inscribir en ESET PROTECT Cloud dispositivos sin cámara, navegador o correo electrónico (por ejemplo, televisores, pantallas inteligentes, pantallas de publicidad, etc.). Para inscribir estos dispositivos, instale ESET Endpoint Security for Android en el dispositivo mediante Google Play o el archivo APK. Durante el asistente de inicio, en el paso **Administración remota**, seleccione **Sí, administrar de forma remota** y pulse **Dispositivo de entrada limitada**.

Entrante ESET PROTECT Cloud:

1.Haga clic en **Ordenadores** > **Agregar dispositivo** > **Android o iOS/iPadOS** > **Personalizar inscripción**.

2.Seleccione **Dispositivos Android con opciones de entrada limitadas** y seleccione su método de distribución preferido. Puede obtener más información sobre los métodos de distribución en la consola de ESET PROTECT Cloud.

3.Acepto el Acuerdo de licencia para el usuario final y la Política de privacidad.

4.Si se trata de un dispositivo nuevo, haga clic en **Agregar**. Rellene toda la información necesaria y haga clic en **Guardar**. Si va a agregar un dispositivo existente, seleccione el dispositivo correspondiente.

5.Recibe un vínculo de inscripción para el dispositivo. Haga clic en el vínculo y escriba el código de seguridad de seis dígitos mostrado en la sección **Administración remota** del asistente de inicio.

6.Haga clic en **Aceptar**.

El dispositivo se ha en ESET PROTECT Cloud.

Instalación local en el dispositivo

ESET Endpoint Security for Android ofrece al administrador la posibilidad de configurar y administrar equipo a nivel local si optan por no usar ESET PROTECT. La configuración de la aplicación se protege mediante una contraseña de administración, para que la aplicación esté bajo control administrativo total en todo momento.

Si el administrador de una pequeña empresa opta por no usar ESET PROTECT pero quiere proteger los dispositivos

corporativos y aplicar políticas de seguridad básicas, tiene dos opciones de administración local de los dispositivos:

1.Acceso físico a los dispositivos de la empresa y configuración manual de los ajustes.

2.El administrador puede preparar la configuración que desee en su dispositivo Android (con ESET Endpoint Security for Android instalado) y exportar estos ajustes a un archivo; consulte el apartado Importar/exportar configuración de esta guía para obtener más información). El administrador puede compartir el archivo exportado con los usuarios finales (por ejemplo por correo electrónico); puede importar el archivo en cualquier dispositivo en el que se ejecute ESET Endpoint Security for Android. Cuando el usuario abra y acepte el archivo de configuración recibido, se importarán automáticamente todos los ajustes y se activará la aplicación (siempre que se incluyera la información de la licencia). Todos los ajustes estarán protegidos por la contraseña de administración.

Descargar del sitio web de ESET

Descargue ESET Endpoint Security for Android escaneando el código QR que aparece a continuación con una aplicación de escaneo de códigos QR de su dispositivo móvil:

Otra opción es descargar el archivo APK de instalación de ESET Endpoint Security for Android del sitio web de ESET:

1.Descargue el archivo de instalación del sitio web de ESET.

2.Abra el archivo desde el área de notificaciones de Android o localícelo con una aplicación de gestión de archivos. Normalmente, el archivo se guarda en la carpeta de descargas.

3.Asegúrese de que las aplicaciones procedentes de Orígenes desconocidos estén autorizadas en su dispositivo. Para ello, pulse el icono del Lanzador en la pantalla de inicio de Android o diríjase a **Inicio** > **Menú**. Pulse **Ajustes** > **Seguridad**. La opción **Orígenes desconocidos** debe estar permitida.

4.Tras abrir el archivo, pulse **Instalar**.

Una versión de ESET Endpoint Security for Android descargada del sitio web de ESET solo puede actualizarse mediante la descarga de un archivo del sitio web de ESET o desde la aplicación. No se puede actualizar a través de Google Play.

Asistente de inicio

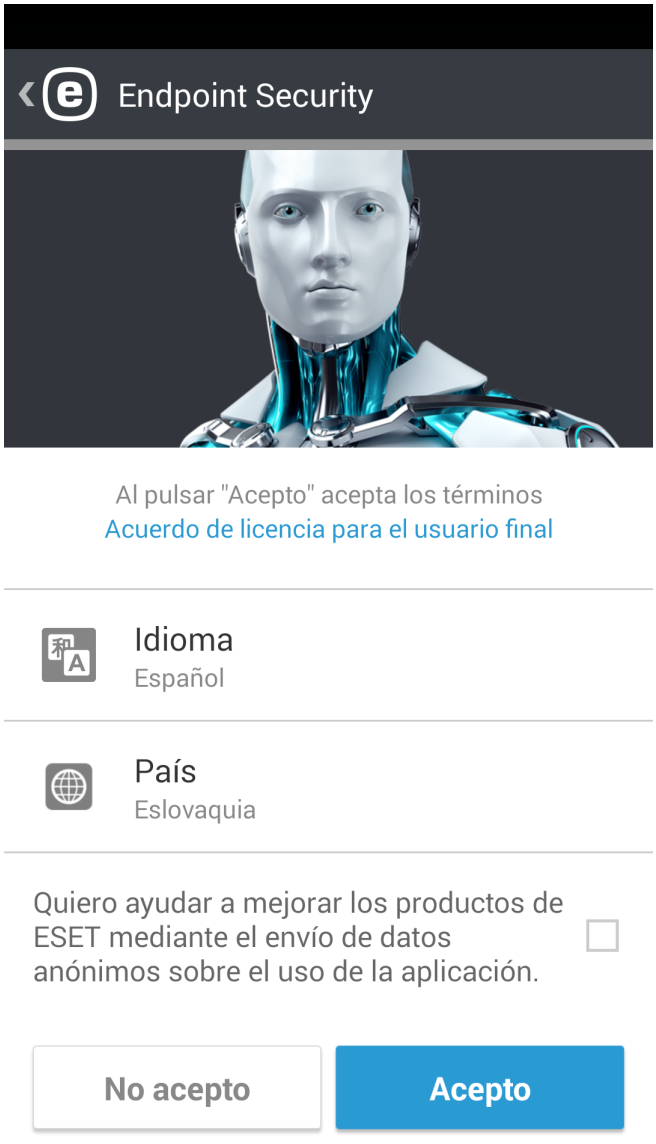
Tras instalar la aplicación, pulse **Configuración de administrador** y siga los mensajes del asistente de inicio. Este procedimiento está destinado exclusivamente a los administradores:

1.Seleccione el **Idioma** que desee usar en ESET Endpoint Security for Android.

2.Seleccione el **País** en el que actualmente trabaja o reside.

3.Si desea ayudar a mejorar los productos de ESET mediante el envío de datos anónimos sobre el uso de la aplicación, marque la casilla de verificación.

4.Pulse **Acepto**. Al pulsar **Acepto** indica que acepta el Acuerdo de licencia para el usuario final.



5.Pulse **Aceptar** para dar el consentimiento del usuario.

6.Seleccione **Sí, administrar de forma remota** para conectar ESET Endpoint Security for Android a ESET PROTECT o haga una configuración manual haciendo clic en **No, solo proteger**.

7.La configuración manual requiere la activación de los permisos para el teléfono y el almacenamiento.

Pulse **Continuar** y, a continuación, pulse **Permitir** para activar cada uno de los permisos.

8.Pulse **Continuar** para permitir el permiso "Dibujar sobre otras aplicaciones".

9.La configuración manual requiere la activación del producto. Puede activar ESET Endpoint Security for Android mediante una clave de licencia o a través de ESET Business Account (EBA).

10.Cree una contraseña de administrador.

11.**Protección contra desinstalación** impide que usuarios no autorizados desinstalen ESET Endpoint Security for Android. Pulse **Activar** y, a continuación, pulse **Activar** en el mensaje **Activar Administrador del dispositivo**.

12.Active el acceso de uso para permitir la correcta funcionalidad de la aplicación. Pulse **Continuar**, pulse **Aceptar** y, a continuación, pulse **ESET Endpoint Security for Android** para activar **Acceso de uso**. Pulse la flecha atrás dos veces para volver al Asistente de inicio.

13.Seleccione la opción que desee para **Permitir** o **Rechazar** la participación en el sistema de respuesta ESET LiveGrid. Si desea obtener más información acerca de ESET LiveGrid, consulte esta sección.

14.Seleccione la opción para que ESET Endpoint Security for Android deba **Activar detección** o **No activar detección** de aplicaciones potencialmente indeseables. En esta sección puede obtener más información sobre estas aplicaciones. Pulse **Siguiente**.

15.Pulse **Finalizar** para salir del Asistente de inicio e iniciar su primer análisis del dispositivo.

Desinstalación

ESET Endpoint Security for Android puede desinstalarse con el asistente de desinstalación disponible en el menú principal del programa, en **Configuración** > **Desinstalar**. Si la Protección contra desinstalación está activada, se le solicitará que introduzca la Contraseña de administración.

Otra opción es desinstalar el producto manualmente siguiendo los pasos indicados a continuación:

1.Pulse el icono de inicio en la pantalla de inicio de Android (o diríjase a **Inicio** > **Menú**) y pulse **Configuración** > **Seguridad** > **Administradores del dispositivo**. Cancele la selección de **ESET Endpoint Security for Android** y pulse **Desactivar**. Pulse **Desbloquear** e introduzca la contraseña de administración. Si no ha establecido ESET Endpoint Security for Android como administrador del dispositivo, omita este paso.

2.Vuelva a la **Configuración** y pulse **Administrar aplicaciones** > **ESET Endpoint Security for Android** > **Desinstalar**.

Activación del producto

Hay varias formas de activar ESET Endpoint Security for Android. La disponibilidad de un método de activación determinado podría variar en función del país y del medio de distribución (página web de ESET, etc.) de su producto.

Para activar ESET Endpoint Security for Android directamente en el dispositivo Android, pulse el icono **Menú**  en la pantalla principal de ESET Endpoint Security for Android y pulse **Licencia**.

Puede utilizar cualquiera de estos métodos para activar ESET Endpoint Security for Android:

- **Clave de licencia** – se trata de una cadena única que presenta el formato XXXX-XXXX-XXXX-XXXX-XXXX y sirve para identificar al propietario de la licencia y activar la licencia.

- **ESET Business Account**: es una cuenta creada en el portal de ESET Business Account con credenciales (dirección de correo electrónico y contraseña). Este método le permite gestionar varias licencias desde una ubicación.

ESET PROTECT puede activar dispositivos cliente de forma silenciosa con las licencias que le proporcione el administrador.

Documentación para equipos administrados de forma remota

Los productos para empresas de ESET y ESET Endpoint Security for Android pueden administrarse de forma remota en las estaciones de trabajo cliente, servidores y dispositivos móviles en un entorno en red desde una ubicación central. Los administradores de sistemas que administran más de 10 estaciones de trabajo cliente deben considerar usar una herramienta de administración remota de ESET. Estas herramientas permiten implementar soluciones de ESET, administrar tareas, aplicar políticas de seguridad, supervisar los estados del sistema y responder rápidamente a problemas o amenazas en ordenadores remotos desde una ubicación central.

Herramientas de administración remota ESET

ESET Endpoint Security for Android se puede administrar de forma remota con ESET PROTECT o ESET PROTECT Cloud.

- Introducción a ESET PROTECT

- Introducción a ESET PROTECT Cloud

Herramienta de migración
La versión 3.5 de ESET Endpoint Security for Android y posteriores es compatible con la Herramienta de migración para migrar de ESET PROTECT a ESET PROTECT Cloud.

Prácticas recomendadas

- Inscribir un dispositivo con ESET PROTECT

- Configurar una contraseña de administración en los ordenadores cliente conectados para evitar modificaciones no autorizadas

- Aplicar una política recomendada para aplicar las funciones de seguridad disponibles

Guías

- Cómo utilizar el modo de anulación

Dispositivo Android inscrito a través de Microsoft Intune

Cuando un dispositivo con Android 9 o posterior se inscribe a través de Microsoft Intune, la versión 3.5 de ESET Endpoint Security for Android y posteriores ignoran la siguiente configuración al aplicarse la política correspondiente:

- Seguridad del dispositivo
- Control de la aplicación
- Antirrobo

Introducción a ESET PROTECT

ESET PROTECT le permite administrar productos ESET en estaciones de trabajo, servidores y dispositivos móviles en un entorno de red desde una ubicación central.

Con ESET PROTECT Web Console, puede implementar soluciones ESET, administrar tareas, aplicar políticas de seguridad, supervisar el estado del sistema y responder rápidamente a problemas o amenazas en ordenadores remotos. Consulte también la visión general de los elementos de la infraestructura y la arquitectura de ESET PROTECT, la Introducción a ESET PROTECT Web Console y los Entornos de aprovisionamiento de escritorios compatibles.

ESET PROTECT lo conforman los siguientes componentes:

- ESET PROTECT Server: ESET PROTECT Server se puede instalar en servidores Windows y Linux, y también está disponible como dispositivo virtual. Se ocupa de la comunicación con los agentes, y recopila y almacena datos de aplicaciones en la base de datos.

- ESET PROTECT Consola Web: ESET PROTECT es la interfaz principal que le permite administrar ordenadores cliente en su entorno. Muestra información general del estado de los clientes en la red y le permite implementar de forma remota soluciones de ESET en ordenadores no administrados. Tras instalar ESET PROTECT Server, puede acceder a la consola web a través del navegador web. Si configura el servidor web para que esté disponible desde Internet, puede utilizar ESET PROTECT desde prácticamente cualquier lugar o dispositivo con conexión a Internet.

- ESET Management Agent: ESET Management Agent facilita la comunicación entre ESET PROTECT Server y los ordenadores cliente. El agente debe instalarse en el ordenador cliente para establecer comunicación entre ese ordenador y ESET PROTECT Server. Como está en el ordenador cliente y puede almacenar varios contextos de seguridad, el uso de ESET Management Agent reduce considerablemente el tiempo de reacción a las nuevas detecciones. Con ESET PROTECT Web Console puede implementar ESET Management Agent en los ordenadores no administrados que identifica Active Directory o el Sensor de RD de ESET. También puede instalar de forma manual ESET Management Agent en los ordenadores cliente en caso de que sea necesario.

- Rogue Detection Sensor: ESET PROTECT Rogue Detection (RD) Sensor detecta los ordenadores no administrados presentes en su red y envía su información a ESET PROTECT Server. Esto le permite agregar fácilmente nuevos ordenadores cliente a su red protegida. El Sensor de RD recuerda los ordenadores que se han detectado y no envía la misma información dos veces.

- Proxy HTTP Apache: es un servicio que puede usarse en combinación con ESET PROTECT para:

- Distribuir actualizaciones entre los ordenadores cliente y paquetes de instalación a ESET Management Agente.
- Reenviar la comunicación de las instancias de ESET Management Agente a ESET PROTECT Server.

- Mobile Device Connector: es un componente que permite la administración de dispositivos móviles con ESET PROTECT, gracias a la que puede administrar dispositivos móviles (Android e iOS) y ESET Endpoint Security for Android.

- Dispositivo virtual de ESET PROTECT: el dispositivo virtual de ESET PROTECT está pensado para aquellos usuarios que quieren ejecutar ESET PROTECT en un entorno virtualizado.

- ESET PROTECT Virtual Agent Host: un componente de ESET PROTECT que virtualiza entidades de agente para poder administrar máquinas virtuales sin agentes. Esta solución activa la automatización, la utilización de grupos dinámicos y el mismo nivel de administración de tareas de ESET Management Agent en los ordenadores físicos. El agente virtual recopila información de las máquinas virtuales y la envía a ESET PROTECT Server.

- Herramienta Mirror: la herramienta Mirror es necesaria para las actualizaciones de módulos sin conexión. Si los ordenadores cliente no tienen conexión a Internet, puede utilizar la herramienta Mirror para descargar archivos de actualización de servidores de actualizaciones de ESET y almacenarlos localmente.

- ESET Remote Deployment Tool: esta herramienta le permite implementar paquetes todo en uno creados en <%PRODUCT%> Consola Web. Permite distribuir con facilidad ESET Management Agent con un producto de ESET por los ordenadores de una red.

- ESET Business Account: el nuevo portal de licencias de productos empresariales de ESET le permite administrar las licencias. Consulte la sección <%EBA%> de este documento para obtener las instrucciones de activación del producto, o consulte la Guía del usuario de <%EBA%> para obtener más información sobre el uso de <%EBA%>. Si ya dispone de un nombre de usuario y una contraseña emitidos por ESET y desea convertirlos en una clave de licencia, consulte la sección Convertir credenciales de licencia heredada.

- ESET Enterprise Inspector: un completo sistema de detección y respuesta para equipos que incluye funciones como las siguientes: detección de incidentes, administración de incidentes y respuesta, recopilación de datos, indicadores de detección de riesgo, detección de anomalías, detección de comportamientos e incumplimientos de políticas.

Con ESET PROTECT Web Console puede implementar soluciones ESET, administrar tareas, aplicar políticas de seguridad, supervisar el estado del sistema y responder rápidamente a problemas o amenazas en ordenadores remotos.

Si desea más información, consulte la guía del usuario de ESET PROTECT en línea.

Introducción a ESET PROTECT Cloud

ESET PROTECT Cloud le permite administrar los productos de ESET en estaciones de trabajo y servidores en un entorno de red desde una ubicación central sin necesidad de tener un servidor físico o virtual como para ESET PROTECT oESET Security Management Center. Con (ESET PROTECT Cloud Consola Web), podrá implementar soluciones de ESET, administrar tareas, aplicar políticas de seguridad, supervisar el estado del sistema y responder rápidamente a problemas o amenazas que se produzcan en ordenadores remotos.

- Lea más acerca de esto en la guía del usuario de ESET PROTECT Cloud en línea

Políticas

El administrador puede aplicar configuraciones específicas a productos de ESET que se ejecutan en dispositivos cliente con las políticas de ESET PROTECT Web Console o ESET Security Management Center Web Console. Las políticas pueden aplicarse a dispositivos concretos o a grupos compuestos por varios dispositivos. También puede asignar varias políticas a un dispositivo o un grupo.

Para crear una política nueva, un usuario debe contar con los siguientes permisos: el permiso de **Lectura** para leer la lista de políticas, el permiso de **Uso** para asignar políticas a los ordenadores seleccionados y el permiso de **Escritura** para crear, modificar o editar las políticas.

Las políticas se aplican en el orden en el que se establezcan los grupos estáticos. No ocurre lo mismo con los grupos dinámicos, ya que en este caso se aplican las políticas a los grupos dinámicos secundarios en primer lugar. Esto le permite aplicar políticas que tienen una mayor repercusión en la parte superior del árbol de grupos y políticas más específicas en los subgrupos. Con el uso de indicadores, un usuario de ESET Endpoint Security for Android con acceso a grupos que se sitúan en la parte superior del árbol puede anular las políticas de los grupos inferiores. Este algoritmo se explica en la ayuda en línea de ESET PROTECT.

Al configurar políticas en el dispositivo se desactiva la opción de cambiar localmente la configuración controlada por políticas. Esta configuración se bloquea de modo que no se pueden realizar cambios ni siquiera en el modo de administración. Puede permitir que se realicen cambios temporales mediante la creación de una política de modo de anulación.

Para configurar determinadas políticas, puede que sea necesario conceder permisos adicionales a ESET Endpoint Security for Android localmente en el dispositivo afectado.

Le recomendamos que asigne políticas más genéricas (por ejemplo, la política del servidor de actualización) a grupos que están más arriba en el árbol de grupos. Debe asignar políticas más específicas (por ejemplo, la configuración de control de dispositivos) en la parte más inferior del árbol de grupos. Las políticas más bajas suelen anular la configuración de las políticas superiores cuando se fusionan (excepto cuando se define de otra forma con indicadores de políticas).

Políticas predeterminadas para ESET Endpoint Security for Android

Nombre de la directiva	Descripción de la directiva
General: protección máxima	ESET Endpoint Security for Android utiliza todas las opciones para garantizar la máxima protección del dispositivo.
General: configuración equilibrada	ESET Endpoint Security for Android utiliza la configuración recomendada para la mayoría de las configuraciones.
General: máximo rendimiento	ESET Endpoint Security for Android combina protección contra amenazas y una repercusión mínima en las tareas diarias y el rendimiento del dispositivo.

Aplicar políticas

Tras conectar ESET Endpoint Security for Android a la consola de administración de ESET, la práctica recomendada es aplicar una política recomendada o personalizada.

Hay varias políticas integradas para ESET Endpoint Security for Android:

Nombre de la directiva	Descripción de la directiva
General: protección máxima	ESET Endpoint Security for Android utiliza todas las opciones para garantizar la máxima protección del dispositivo.
General: configuración equilibrada	ESET Endpoint Security for Android utiliza la configuración recomendada para la mayoría de las configuraciones.
General: máximo rendimiento	ESET Endpoint Security for Android combina protección contra amenazas y una repercusión mínima en las tareas diarias y el rendimiento del dispositivo.

Para obtener más información sobre las políticas, consulte los temas siguientes:

- ESET PROTECT políticas
- ESET PROTECT Cloud políticas
- Apply a recommended or predefined policy for ESET Endpoint Security for Android using ESET Security Management Center

Indicadores

La política que se aplica a un ordenador cliente suele ser el resultado de una fusión de varias políticas que forman una política final. Al fusionar políticas, puede ajustar el comportamiento esperado de la política final según el orden de las políticas aplicadas con el uso de indicadores de políticas. Los indicadores definen cómo administrará la política una configuración determinada.

Para cada ajuste puede seleccionar uno de los siguientes indicadores:

No aplicar	La política no establecerá ningún ajuste que tenga este indicador. Como la política no define el ajuste, otras políticas que se apliquen posteriormente podrán modificar dicho ajuste.
Aplicar	Los ajustes que tengan el indicador **Aplicar** se aplicarán al ordenador cliente. No obstante, al fusionar políticas, se pueden sobrescribir con otras políticas aplicadas posteriormente. Cuando se envía a un ordenador cliente una política que contiene ajustes marcados con este indicador, estos ajustes modificarán la configuración local del ordenador cliente. Como este ajuste no es forzado, otras políticas aplicadas posteriormente pueden modificarla.
Forzar	Los ajustes que tengan el indicador **Forzar** tienen prioridad y ninguna política que se aplique posteriormente puede sobrescribirlos (aunque también tengan el indicador **Forzar**). De esta forma, se garantiza que otras políticas que se apliquen más tarde no puedan modificar este ajuste durante la fusión. Cuando se envía a un ordenador cliente una política que contiene ajustes marcados con este indicador, estos ajustes modificarán la configuración local del ordenador cliente.

Situación: el *administrador* quiere que el usuario *John* pueda crear o modificar políticas en su grupo de inicio y ver todas las políticas que ha creado el *administrador*, incluidas las políticas que presentan el indicador Forzar. El *administrador* quiere que *John* pueda ver todas las políticas, pero no que pueda modificar las políticas existentes creadas por el *administrador*. *John* solo puede crear o modificar políticas dentro de su grupo de inicio, San Diego.
Solución:el *administrador* debe seguir los siguientes pasos.
Crear conjuntos de permisos y grupos estáticos personalizados
1. Cree un nuevo Grupo estático llamado *San Diego*.
2. Cree un nuevo Conjunto de permisos llamado *Política: Todo John* con acceso al grupo estático *Todo* y con permiso de **Lectura** para **Políticas**.
3. Cree un nuevo Conjunto de permisos llamado *Política John* con acceso al grupo estático *San Diego* y con acceso a la funcionalidad del permiso de **Escritura** en **Grupo y ordenadores** y **Políticas**. Este conjunto de permisos otorga a *John* el permiso de crear o modificar políticas en su grupo de inicio *San Diego*.
4. Cree un nuevo usuario *John* y seleccione *Política: Todo John* y *Política John* en la sección **Conjuntos de permisos**.
Crear políticas
5. Cree la nueva política *Todo: activar el cortafuegos*, despliegue la sección **Configuración**, seleccione **ESET Endpoint para Windows**, desplácese hasta **Cortafuegos personal** > **Básico** y aplique toda la configuración mediante el indicador **Forzar**. Despliegue la sección **Asignar** y seleccione el grupo estático *Todos*.
6. Cree la nueva política *Grupo de John: activar el cortafuegos*, despliegue la sección **Configuración**, seleccione **ESET Endpoint para Windows**, desplácese hasta **Cortafuegos personal** > **Básico** y aplique toda la configuración mediante el indicador **Aplicar**. Despliegue la sección **Asignar** y seleccione el grupo estático *San Diego*.
Resultado
Las políticas creadas por el *administrador* se aplicarán en primer lugar porque se aplicaron indicadores de **Forzar** a la configuración de la política. Los ajustes a los que se haya aplicado el indicador Forzar tienen prioridad y ninguna otra política que se aplique más tarde puede sobrescribirlos. Las políticas creadas por el usuario *John* se aplicarán después de las políticas creadas por el administrador.
Para consultar el orden final de las políticas, desplácese hasta **Más** > **Grupos** > **San Diego**. Seleccione el ordenador y, a continuación, **Mostrar detalles**. Haga clic en **Políticas aplicadas** en la sección **Configuración**.

Usar el modo de anulación

Los usuarios con ESET Endpoint Security for Android (versión 2.1 y posteriores) instalado en su ordenador pueden utilizar la función de anulación. El modo de anulación permite a los usuarios de nivel dispositivo cliente cambiar la configuración del producto ESET instalado durante un tiempo establecido, incluso si hay una política aplicada a esta configuración. Una vez transcurrido el tiempo establecido, se restablecerá la configuración establecida por las políticas.

Según la configuración de la política predeterminada, ESET Endpoint Security for Android analiza el dispositivo una vez finalizada la sesión de reemplazo. Puede cambiar este comportamiento con la opción **Analizar el dispositivo tras una sesión de reemplazo**.

- Para cambiar la configuración localmente en el dispositivo en el modo de anulación, debe introducir la contraseña de administración de ESET Endpoint Security for Android.
- No puede detener el modo de anulación desde ESET Web Console una vez que se activa. El modo de anulación se deshabilitará automáticamente cuando venza el tiempo de anulación.
- El usuario que utiliza el modo de anulación debe tener una contraseña de administrador de ESET Endpoint Security for Android. De lo contrario, el usuario no podrá acceder a la configuración de ESET Endpoint Security for Android. Puede crear una contraseña de anulación de administración temporal para cada política.

Para configurar el **modo de anulación**:

1. Haga clic en **Políticas** > **Nueva política**.
2. En la sección **Básico**, escriba un **Nombre** y una **Descripción** para la política.
3. En la sección **Configuración**, seleccione **ESET Endpoint Security for Android**.
4. Haga clic en **Configuración** en las opciones de la política.
5. Expanda **Configuración del modo de anulación** y configure las reglas para el modo de anulación.
6. En la sección **Asignar**, seleccione los dispositivos correspondientes.
7. Revise la configuración en la sección **Resumen** y haga clic en **Finalizar**.

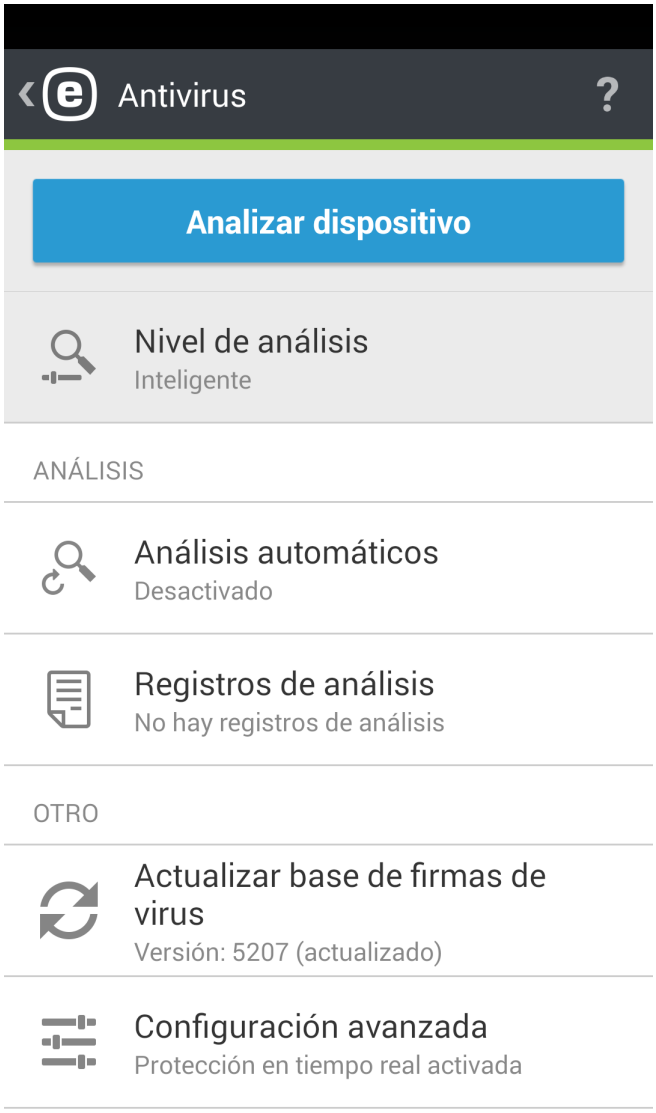
Si *John* tiene un problema porque la configuración de su equipo está bloqueando algunas funciones importantes o el acceso web en su dispositivo, el Administrador podrá permitir que *John* anule su política de punto de conexión existente y ajuste la configuración manualmente en su dispositivo. Después, ESET PROTECT Cloud podrá solicitar la nueva configuración, por lo que el Administrador podrá crear una nueva política a raíz de la misma.
Para hacerlo, siga estos pasos:
1.Haga clic en **Políticas** > **Nueva política**.
2.Complete los campos **Nombre** y **Descripción**. En la sección **Configuración**, seleccione **ESET Endpoint Security for Android**.
3.Haga clic en **Configuración** en las opciones de la política.
4.Despliegue la configuración de **Modo de anulación** y active el modo de anulación durante una hora.
5.Haga clic en **Establecer** en las credenciales de anulación para crear una contraseña de administración temporal para John. Escriba la contraseña (por ejemplo, 12345) dos veces y haga clic en **Aceptar**.
6.Asigne la política al *Smartphone de John* y haga clic en **Finalizar** para guardar la política.
7.*John* debe introducir la contraseña de administración para activar el **modo de anulación** en su ESET Endpoint Security for Android y cambiar la configuración manualmente en su dispositivo.
8.En la consola web de ESET PROTECT Cloud, vaya a **Equipos**, seleccione *Smartphone de John* y haga clic en **Mostrar detalles**.
9.En la sección **Configuración**, haga clic en **Solicitar configuración** para programar una tarea de cliente para obtener la configuración del cliente.
10.Aparece la nueva configuración. Seleccione el producto correspondiente y, a continuación, haga clic en **Abrir configuración**.
11.Revise la configuración y, a continuación, haga clic en **Convertir en política**.
12.Complete los campos **Nombre** y **Descripción**.
13.En la sección **Configuración** puede modificar los ajustes si es necesario.
14.En la sección **Asignar**, asigne esta política al *smartphone de John* (o a otros).
15.Haga clic en **Finalizar**. No olvide eliminar la política de anulación cuando ya no la necesite.

Contraseña de anulación

Esta opción le permite crear una contraseña de administrador temporal para permitir a los usuarios modificar la configuración del dispositivo cliente sin tener acceso a la contraseña de administrador real. Haga clic en **Establecer** junto a la política para introducir la contraseña de anulación.

Antivirus

El módulo Antivirus protege su dispositivo de código malicioso mediante el bloqueo de las amenazas y, posteriormente, desinfectándolas o poniéndolas en cuarentena.



Analizar dispositivo

La opción **Analizar dispositivo** puede usarse para buscar amenazas en su dispositivo.

Hay tipos de archivos predefinidos que se analizan de forma predeterminada. El análisis completo del dispositivo revisa la memoria, los procesos en ejecución y las bibliotecas de enlaces dinámicos dependientes, así como los archivos que se encuentran en el almacenamiento interno y en el almacenamiento extraíble. En el apartado Registros del análisis se guardará un archivo de registro con un resumen breve del análisis.

Si desea anular un análisis que ya está en curso, pulse el icono .

Nivel de análisis

Es posible elegir entres dos niveles de análisis distintos:

- **Análisis inteligente**: el Análisis inteligente analizará las aplicaciones instaladas, los archivos DEX (archivos ejecutables del SO Android), los archivos del SO (bibliotecas), los archivos ZIP con una profundidad de análisis máxima de tres archivos comprimidos anidados y el contenido de la tarjeta SD.

- **Exhaustivo**: se analizarán todos los tipos de archivo, sea cual sea su extensión, tanto de la memoria interna como de la tarjeta SD.

Análisis automáticos

Además de los análisis a petición del dispositivo, ESET Endpoint Security for Android ofrece también análisis automáticos. Si desea aprender a usar el Análisis al cargar y el Análisis programado, lea este apartado.

Registros del análisis

El apartado Registros del análisis contiene datos completos de los análisis completados en forma de archivos de registro. Consulte el apartado Registros de análisis del antivirus de este documento para obtener más información.

Actualizar módulos de detección

ESET Endpoint Security for Android incluye, de forma predeterminada, una tarea de actualización para garantizar que el programa se actualiza regularmente. Para ejecutar la actualización manualmente, pulse **Actualizar módulos de detección**.

i para evitar un uso innecesario del ancho de banda, las actualizaciones se publican cuando se agrega una nueva amenaza. A pesar de que una licencia activa le concede acceso a las actualizaciones, su proveedor de servicios móviles podría cobrarle las transferencias de datos.

Puede encontrar descripciones detalladas de la configuración avanzada del antivirus en el apartado Configuración avanzada de este documento.

Análisis automáticos

Nivel de análisis

Es posible elegir entres dos niveles de análisis distintos. Este ajuste se aplicará tanto al Análisis al cargar como al Análisis programado:

- **Análisis inteligente**: el Análisis inteligente analizará las aplicaciones instaladas, los archivos DEX (archivos ejecutables del SO Android), los archivos del SO (bibliotecas), los archivos ZIP con una profundidad de análisis máxima de tres archivos comprimidos anidados y el contenido de la tarjeta SD.
- **Exhaustivo**: se analizarán todos los tipos de archivo, sea cual sea su extensión, tanto de la memoria interna como de la tarjeta SD.

Análisis al cargar

Cuando se seleccione esta opción, el análisis comenzará automáticamente cuando el dispositivo esté en estado de inactividad (totalmente cargado y conectado a un cargador).

Análisis programado

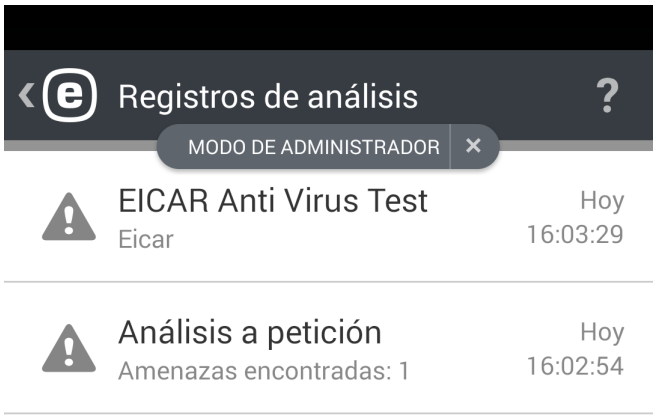
El Análisis programado le permite ejecutar un análisis automático del dispositivo a una hora predefinida. Para programar un análisis, pulse  junto a **Análisis programado** y especifique las fechas y horas a las que deba iniciarse el análisis. La selección predeterminada es lunes a las 4 de la mañana.

Registros del análisis

Los registros del análisis se crean después de cada análisis programado o análisis del dispositivo iniciado manualmente.

En cada registro se incluye la siguiente información:

- Fecha y hora del suceso
- Duración del análisis
- Número de archivos analizados
- Resultado del análisis o errores detectados durante el mismo



Reglas para ignorar

Si gestiona ESET Endpoint Security for Android de forma remota desde ESET PROTECT, puede definir los archivos que no se marcarán como maliciosos. Los archivos que se añadan a las **Reglas para ignorar** se ignorarán en

futuros análisis. Para crear una regla debe especificar la siguiente información:

- un nombre de archivo con la extensión "apk" correspondiente
- El nombre de una aplicación, p. ej. uk.co.extorian.EICARAntiVirusTest.
- El nombre de la amenaza detectada por los programas antivirus, p. ej. Android/MobileTX.A (este campo es obligatorio).

esta función no está disponible en la aplicación ESET Endpoint Security for Android.

Configuración avanzada

Protección en tiempo real

Esta opción le permite activar o desactivar el análisis en tiempo real. Este análisis se inicia automáticamente durante el inicio del sistema, y analiza los archivos con los que interactúa. Analiza automáticamente la carpeta de descargas, los archivos de instalación APK y todos los archivos de la tarjeta SD después de montarla.

Sistema de reputación ESET LiveGrid

ESET LiveGrid es un sistema de prevención diseñado para proporcionar niveles adicionales de seguridad a su dispositivo. Controla de manera constante los programas y procesos en ejecución del sistema comparándolos con los datos más recientes recopilados de millones de usuarios de ESET de todo el mundo. Esto nos permite ofrecer una protección proactiva más precisa y mayores velocidades de análisis a todos los usuarios de ESET. Se recomienda activar esta función.

Sistema de respuesta ESET LiveGrid

Nos permite recopilar estadísticas anónimas, informes de bloqueo y datos de diagnóstico sobre objetos sospechosos, que procesamos automáticamente para crear mecanismos de detección en nuestro sistema en la nube.

Detectar aplicaciones potencialmente indeseables

Una aplicación potencialmente no deseada es un programa que contiene software publicitario, instala barras de herramientas, realiza un seguimiento de los resultados de sus búsquedas o tiene otros objetivos poco claros. Existen determinados casos en los que podría creer que las ventajas de una aplicación indeseable compensan los riesgos asociados. Este es el motivo que hace que ESET asigne a estas aplicaciones una categoría de riesgo más baja, en comparación con otros tipos de software malicioso.

Detectar aplicaciones potencialmente peligrosas

Existen muchas aplicaciones legítimas cuya función es simplificar la administración de los dispositivos que están en red. Sin embargo, en las manos equivocadas se pueden utilizar con fines maliciosos. La opción Detectar aplicaciones potencialmente no seguras le permite supervisar estos tipos de aplicaciones y bloquearlos, si así lo prefiere. *Aplicaciones potencialmente no seguras* es la clasificación utilizada para el software comercial legítimo. En esta clasificación se incluyen programas como herramientas de acceso remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones.

Bloquear amenazas sin resolver

Este ajuste determina la acción que se realizará cuando el análisis concluya y se hayan encontrado amenazas. Si activa esta opción, ESET Endpoint Security for Android bloqueará el acceso a los archivos clasificados como amenazas.

Medios extraíbles

Puede elegir la acción que desea que se realice cuando se inerte en el dispositivo el medio extraíble:

- **Analizar siempre**: el medio extraíble se analizará siempre
- **No analizar**: no se analizarán los medios extraíbles.
- **Mostrarme opciones**: la opción de análisis de un medio extraíble se mostrará cuando se inserte el medio.

Actualizaciones de la base de firmas de virus

Esta opción le permite establecer el intervalo de tiempo para la frecuencia con la que se descargan automáticamente las actualizaciones de la base de datos de amenazas. Estas actualizaciones se publican cuando se añade una nueva amenaza a la base de datos. Se recomienda mantener esta opción ajustada en el valor predeterminado (Todos los días).

Antigüedad máx. de la base de datos personalizada

Este ajuste define el periodo de tiempo entre actualizaciones de la base de datos de amenazas tras el cual se le pedirá que actualice ESET Endpoint Security for Android.

Servidor de actualización

Con esta opción puede optar por actualizar su dispositivo desde el **Servidor de prueba**. Las actualizaciones previas a su lanzamiento se han sometido a pruebas internas estrictas y pronto estarán disponibles al público en general. Puede beneficiarse de activar las actualizaciones de prueba mediante el acceso a los métodos y soluciones de detección más recientes. Sin embargo, las actualizaciones de prueba podrían no ser totalmente estables en todo momento. La lista de módulos actuales puede encontrarse en el apartado **Acerca de**: pulse el icono de Menú en la pantalla principal de ESET Endpoint Security for Android y pulse **Acerca de** > **ESET Endpoint Security for Android**. Se recomienda que los usuarios básicos dejen la opción **Servidor de lanzamiento** seleccionada de forma predeterminada.

ESET Endpoint Security for Android le permite crear copias de los archivos de actualización, que puede utilizar para actualizar otros dispositivos de la red. El uso de un **Espejo local**: es conveniente realizar una copia de los archivos de actualización del entorno de red local, dado que no necesitan descargarse del servidor de actualización del proveedor varias veces ni que los descarguen todas las estaciones de trabajo. En este documento puede consultar información detallada sobre cómo configurar el servidor mirror desde los productos ESET Endpoint para Windows.

Antirrobo

La función Antirrobo protege su dispositivo móvil del acceso no autorizado.

Si pierde su dispositivo o alguien se lo roba y sustituye su tarjeta SIM por una nueva (que no es de confianza), ESET Endpoint Security for Android bloqueará el dispositivo automáticamente y enviará un SMS de alerta a los números de teléfono que haya definido el usuario. Este mensaje incluirá el número de teléfono de la tarjeta SIM

actualmente insertada, el número IMSI (International Mobile Subscriber Identity) y el número de IMEI (International Mobile Equipment Identity) del teléfono. El usuario no autorizado no sabrá que este mensaje se ha enviado, puesto que se eliminará automáticamente de los hilos de mensajes del dispositivo. También puede solicitar las coordenadas GPS del dispositivo móvil perdido o borrar de forma remota todos los datos almacenados en el dispositivo.

La función Tarjetas SIM de confianza no está disponible en dispositivos con Android 10 y versiones posteriores.

Las funciones de Antirrobo ayudan a los administradores a proteger y localizar un dispositivo perdido. Las acciones pueden desencadenarse desde ESET PROTECT.

Cuando los comandos se ejecutan desde ESET PROTECT, el administrador recibe una confirmación en ESET PROTECT.

Al recibir información de ubicación (comando **Buscar**), el administrador que utiliza ESET PROTECT recibe la información de ubicación en forma de coordenadas GPS.

Todos los comandos Antirrobo también pueden efectuarse desde ESET PROTECT. Las nuevas funciones de administración de dispositivos móviles permiten a los administradores ejecutar los comandos Antirrobo con tan solo unos clics. Las tareas se envían inmediatamente para su ejecución por medio de un nuevo componente de procesamiento de comandos push (Mobile Device Connector) que ahora forma parte de la infraestructura de ESET PROTECT.

Contactos del administrador

Esta es la lista de números de teléfono del administrador protegida por la contraseña de administración. Los comandos de Antirrobo solo pueden enviarse desde números de confianza. Estos números también se emplean para notificaciones relacionadas con acciones de Antirrobo.

Cómo agregar contacto de administración

Se presupone que, durante el asistente de inicio de Antirrobo, se introducen el nombre del administrador y el número de teléfono. Si el contacto contiene más de un número de teléfono, se tendrán en cuenta todos los números asociados.

Los contactos de administración pueden agregarse o modificarse en el apartado **Antirrobo** > **Contactos de administración**.

Información de pantalla de bloqueo

El administrador tiene la posibilidad de definir información personalizada (nombre de la empresa, dirección de correo electrónico, mensaje) que se mostrará cuando el dispositivo se bloquee, con la opción de llamar a uno de los contactos de administración predefinidos.

Esta información incluye:

- Nombre de la empresa (opcional)

- Dirección de correo electrónico (opcional)
- Un mensaje personalizado

Tarjetas SIM de confianza

En el apartado **SIM de confianza** se muestra la lista de tarjetas SIM de confianza aceptadas por ESET Endpoint Security for Android. Si inserta una tarjeta SIM que no aparece en esta lista, la pantalla se bloqueará y se enviará un SMS de alerta al administrador.

Para agregar una nueva tarjeta SIM, pulse el icono ➕. Escriba el **Nombre** de la tarjeta SIM (por ejemplo, Casa, Trabajo) y su número IMSI (Identidad Internacional del Abonado a un Móvil). El número IMSI suele aparecer como un número de 15 dígitos impreso en la tarjeta SIM. En algunos casos podría ser más corto.

Para eliminar una tarjeta SIM de la lista, mantenga pulsada la entrada y, a continuación, pulse el icono 🗑.

La función Tarjetas SIM de confianza no está disponible en dispositivos con Android 10 y versiones posteriores.

La función SIM de confianza no está disponible en dispositivos CDMA, WCDMA y que solo dispongan de conectividad Wi-Fi.

Comandos remotos

Los comandos remotos pueden desencadenarse directamente desde la consola de ESET PROTECT:

Buscar dispositivo

Recibirá un mensaje de texto con las coordenadas GPS del dispositivo de destino y un vínculo a dicha su ubicación en Google Maps. Este dispositivo enviará un nuevo SMS si hay una ubicación más precisa disponible tras 10 minutos.

Bloquear dispositivo

Esto bloqueará el dispositivo. Podrá desbloquearlo con la contraseña de administrador o el comando de desbloqueo remoto.

Desbloquear dispositivo bloqueado

El dispositivo se desbloquea y la tarjeta SIM introducida actualmente en el dispositivo se guarda como SIM de confianza.

Sonido de Sirena/Modo perdido

El dispositivo se bloqueará y emitirá un sonido muy alto durante 5 minutos (o hasta que se desbloquee). Una potente sirena sonará incluso si el dispositivo está en silencio.

Restablecimiento de fábrica mejorado

Este comando restablece la configuración de fábrica del dispositivo. Se borrarán todos los datos a los que pueda accederse y se quitarán los encabezados de los archivos. El proceso puede tardar varios minutos.

Control de aplicaciones

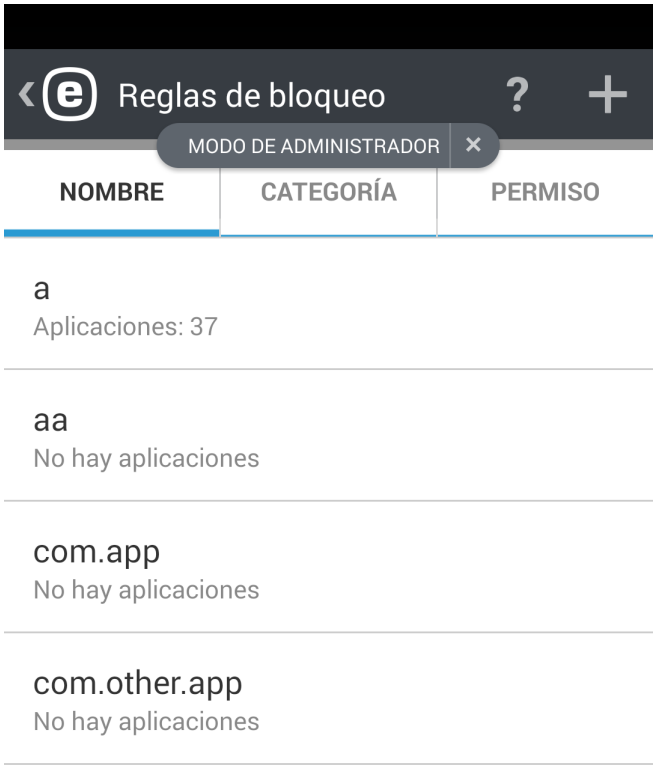
La función **Control de aplicaciones** ofrece a los administradores la opción de supervisar las aplicaciones instaladas, bloquear el acceso a aplicaciones definidas y reducir el riesgo de exposición solicitando a los usuarios que desinstalen aplicaciones concretas. El administrador puede seleccionar varios métodos de filtrado de aplicaciones:

- Definir manualmente las aplicaciones que deben bloquearse
- Bloqueo por categoría (por ejemplo, juegos o redes sociales)
- Bloqueo por permisos (por ejemplo, aplicaciones que realizan un seguimiento de la ubicación)
- Bloqueo por origen (por ejemplo, aplicaciones instaladas desde orígenes que no sean Google Play)

Reglas de bloqueo

En el apartado **Control de aplicaciones** > **Bloqueo** > **Reglas de bloqueo** puede crear las reglas de bloqueo de aplicaciones basándose en los siguientes criterios:

- Nombre de la aplicación o nombre del paquete
- Categoría
- Permisos



Bloquear aplicación

Bloqueo por nombre de la aplicación

ESET Endpoint Security for Androidofrece a los administradores la posibilidad de bloquear una aplicación según su nombre o el nombre del paquete. El apartado **Reglas de bloqueo** contiene un resumen de las reglas creadas y la lista de aplicaciones bloqueadas.

Para modificar una regla existente, mantenga pulsada la regla y, a continuación, pulse **Editar** . Para quitar varias entradas de regla de la lista, mantenga pulsada una de las entradas, seleccione las entradas que desee quitar y, a continuación, pulse **Quitar** . Si desea borrar toda la lista, pulse **SELECCIONAR TODO** y, a continuación, pulse Quitar .

Cuando bloquee una aplicación en función de su nombre, ESET Endpoint Security for Android buscará la coincidencia exacta con un nombre de aplicación iniciada. Si cambia la GUI de ESET Endpoint Security for Android a un idioma diferente, debe volver a introducir el nombre de la aplicación en ese idioma para continuar bloqueándola.

Para evitar cualquier problema con los nombres localizados de la aplicación, se recomienda bloquear estas aplicaciones por el nombre de sus paquetes; un identificador único de la aplicación que no puede modificarse durante el tiempo de ejecución ni reutilizarse en otra aplicación.

En el caso de un administrador local, un usuario puede encontrar el nombre del paquete de la aplicación en **Control de aplicaciones** > **Estado de la protección** > **Aplicaciones permitidas**. Al pulsar en la aplicación, la pantalla **Detalle** mostrará el nombre del paquete de la aplicación. Para bloquear la aplicación, siga estos pasos.

Cómo bloquear una aplicación en función de su nombre

1. Pulse **Control de aplicaciones** > **Bloqueo** > **Bloquear aplicación** > **Bloquear por nombre**.

2. Seleccione si desea bloquear la aplicación en función de su nombre o del nombre del paquete.

3. Escriba las palabras que provocarán el bloqueo de la aplicación. Utilice una coma (,) para separar las palabras.

Por ejemplo, la inclusión de la palabra "*poker*" en el campo **Nombre de la aplicación** bloqueará todas las aplicaciones que contengan "*poker*" en su nombre. Si introduce "*com.poker.game*" en el campo **Nombre del paquete**, ESET Endpoint Security for Android bloqueará solo una aplicación.

Bloqueo por categoría de la aplicación

ESET Endpoint Security for Android ofrece al administrador la posibilidad de bloquear la aplicación según las categorías de aplicaciones predefinidas. El apartado **Reglas de bloqueo** contiene un resumen de las reglas creadas y la lista de aplicaciones bloqueadas.

Si desea modificar la regla existente, mantenga pulsada la regla y pulse **Editar** .

Para quitar varias entradas de regla de la lista, mantenga pulsada una de las entradas, seleccione las entradas que desee quitar y pulse **Quitar** . Si desea borrar toda la lista, pulse **Seleccionar todo**.

Cómo bloquear una aplicación en función de su categoría

1. Pulse **Control de aplicaciones** > **Bloqueo** > **Bloquear aplicación** > **Bloquear por categoría**.

2. Seleccione las categorías predefinidas con las casillas de verificación y pulse **Bloquear**.

Bloquear en función de los permisos de la aplicación

ESET Endpoint Security for Android ofrece al administrador la posibilidad de bloquear la aplicación según sus permisos. El apartado **Reglas de bloqueo** contiene un resumen de las reglas creadas y la lista de aplicaciones bloqueadas.

Si desea modificar la regla existente, mantenga pulsada la regla y pulse **Editar** .

Para quitar varias entradas de regla de la lista, mantenga pulsada una de las entradas, seleccione las entradas que desee quitar y pulse **Quitar** . Si desea borrar toda la lista, pulse **Seleccionar todo**.

Cómo bloquear una aplicación en función de sus permisos

1.Pulse **Control de aplicaciones** > **Bloqueo** > **Bloquear aplicación** > **Bloquear por permiso**.

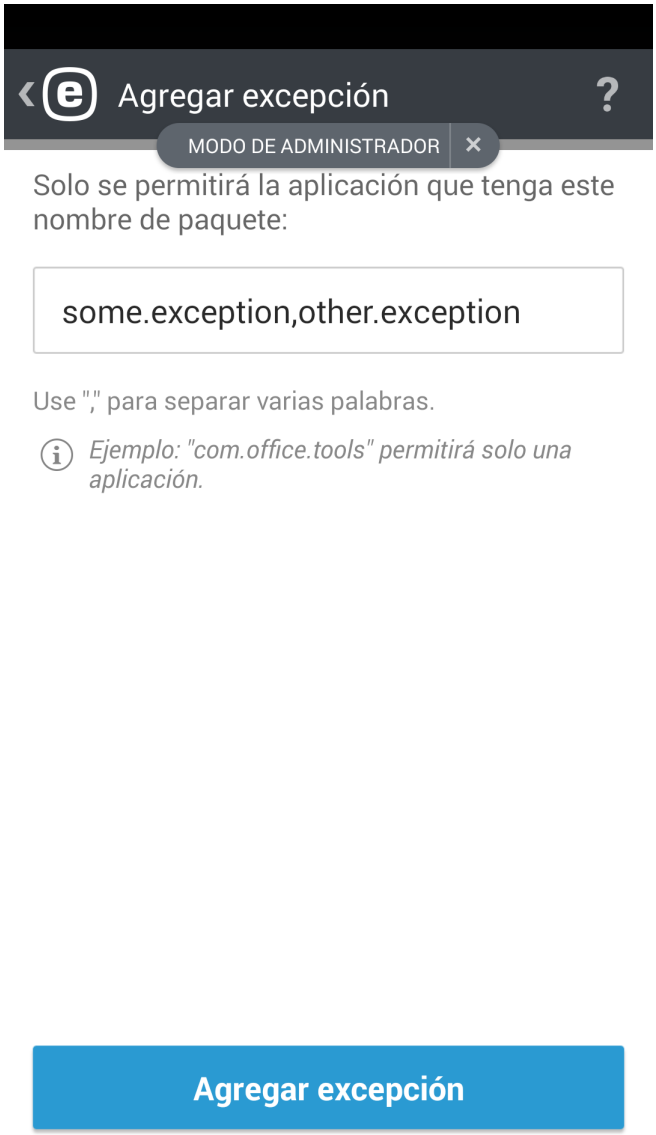
2.Seleccione los permisos con las casillas de verificación y pulse **Bloquear**.

Bloquear orígenes desconocidos

De forma predeterminada, ESET Endpoint Security for Android no bloquea las aplicaciones obtenidas a través de Internet ni de ningún origen que no sea Google Play. El apartado **Aplicaciones bloqueadas** contiene un resumen de las aplicaciones bloqueadas (nombre del paquete, regla aplicada), y la opción de desinstalarla o agregarla a la lista blanca (apartado **Excepciones**).

Excepciones

Pulse **Control de aplicaciones** > **Bloqueo** > **Excepciones** > **Agregar excepción**. Puede crear excepciones para excluir una aplicación concreta de la lista de aplicaciones bloqueadas. Los administradores que gestionen ESET Endpoint Security for Android de forma remota pueden emplear esta nueva función para determinar si un dispositivo concreto cumple con la política de aplicaciones instaladas de la empresa.



Cómo agregar excepciones

Además de agregar la nueva excepción (mediante la introducción del nombre del paquete de la aplicación), las aplicaciones pueden añadirse a una lista blanca al excluirlas de la lista de **Aplicaciones bloqueadas**:

1. En la aplicación ESET Endpoint Security for Android, pulse **Control de aplicaciones**.
2. Pulse **Bloqueo** > **Aplicaciones bloqueadas**.
3. Seleccione la aplicación que desee agregar a la lista blanca.
4. Pulse el icono de los tres puntos de la esquina superior derecha y, a continuación, pulse **Agregar excepción**.
5. Escriba la contraseña de administración y pulse **Entrar**.

Aplicaciones obligatorias

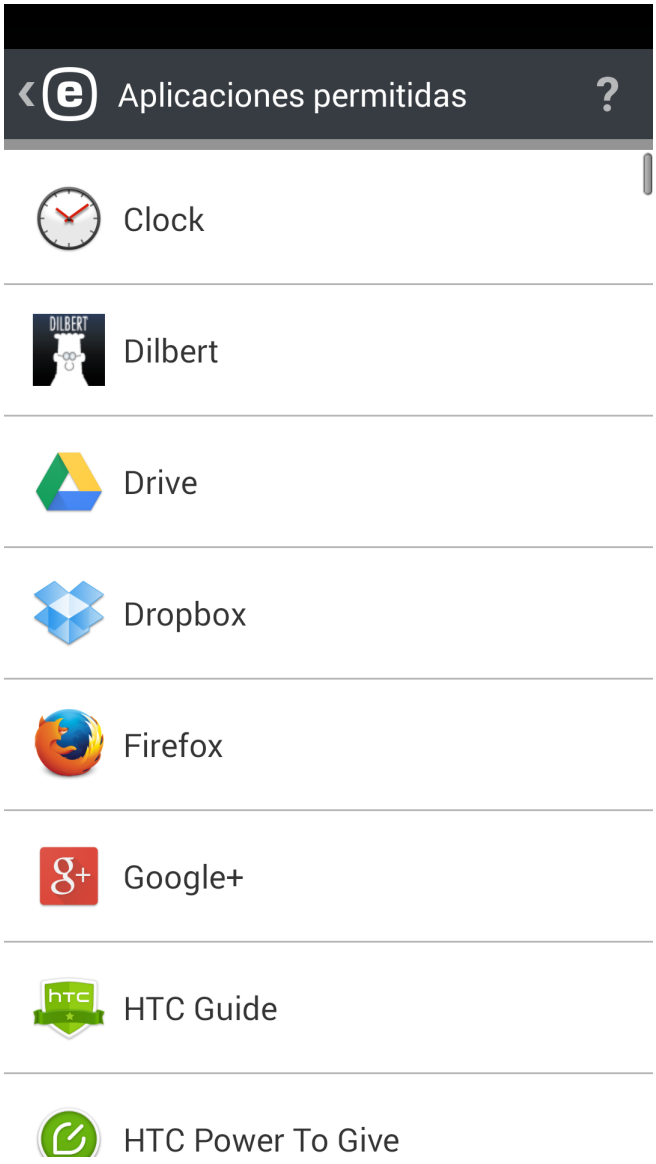
Si gestiona ESET Endpoint Security for Android de forma remota desde ESET PROTECT, puede definir qué aplicaciones deben estar instaladas en el dispositivo de destino Se necesita la siguiente información:

- Nombre de la aplicación visible para el usuario.
- Nombre exclusivo del paquete de la aplicación, p. ej. *com.eset.ems2.gp*.
- URL en la que el usuario puede acceder al vínculo de descarga. También puede usar vínculos de Google Play, como p. ej. https://play.google.com/store/apps/details?id=com.eset.ems2.gp

esta función no está disponible en la aplicación ESET Endpoint Security for Android.

Aplicaciones permitidas

En esta sección se expone una visión general de las aplicaciones instaladas que no bloquean las reglas de bloqueo.

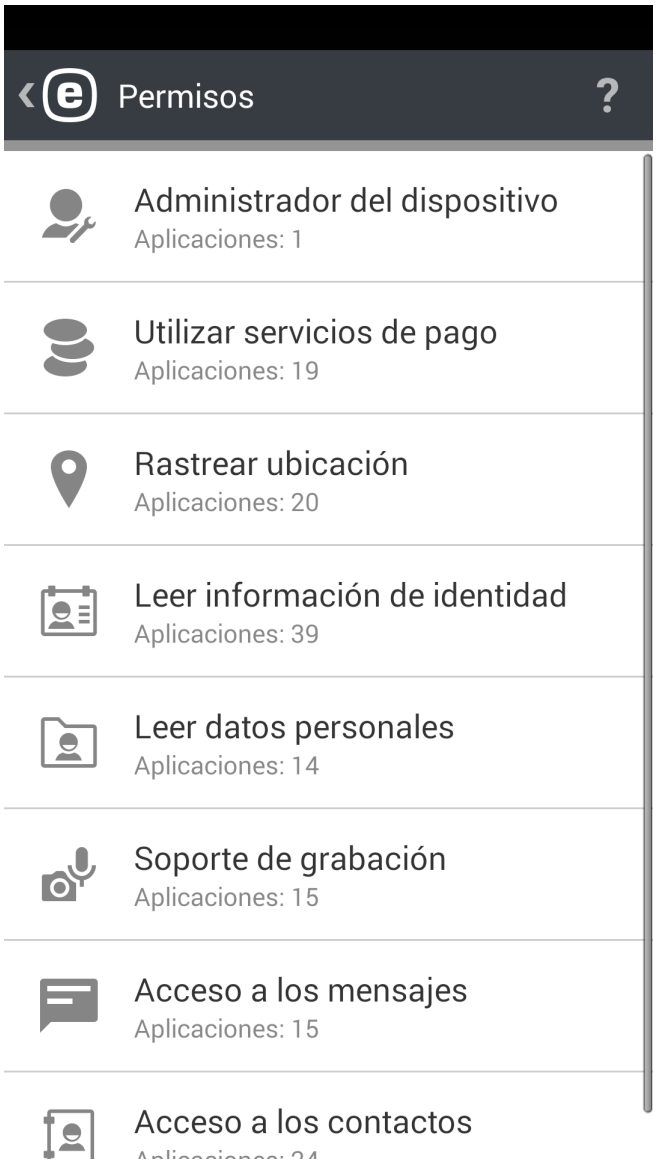


Permisos

Esta función realiza un seguimiento del comportamiento de las aplicaciones que tienen acceso a datos personales o de la empresa, y permite al administrador supervisar el acceso a las aplicaciones basándose en categorías de permisos predefinidas.

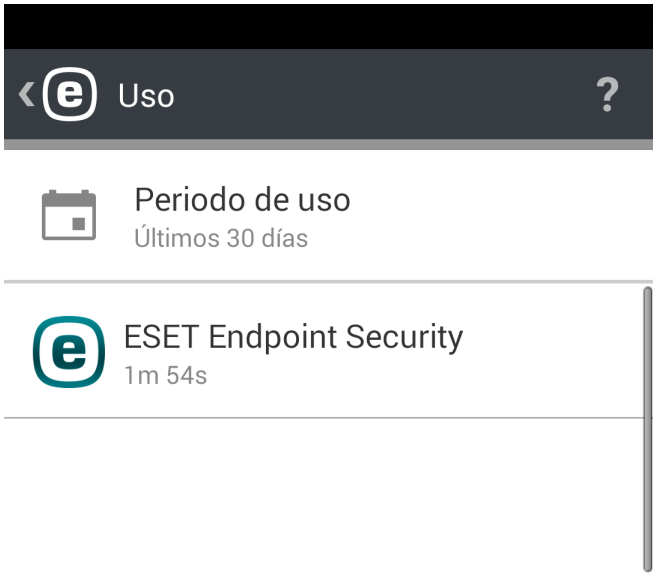
Algunas de las aplicaciones que tiene instaladas en el dispositivo podrían tener acceso a servicios que le suponen un gasto, que controlan su ubicación o que leen su información de identificación, sus contactos o sus mensajes de texto. ESET Endpoint Security for Android ofrece una auditoría de dichas aplicaciones.

En esta sección puede ver la lista de aplicaciones clasificadas en categorías. Pulse cada categoría para ver su descripción detallada. Si desea acceder a los detalles de permisos de cada aplicación, pulse la aplicación en cuestión.



Uso

En este apartado, el administrador puede supervisar el tiempo durante el que un usuario utiliza aplicaciones determinadas. Para filtrar la descripción general por periodo de uso, utilice la opción **Intervalo**.



Seguridad del dispositivo

Seguridad del dispositivo ofrece a los administradores opciones para realizar las siguientes tareas:

- Ejecutar políticas de seguridad básicas en dispositivos móviles y definir políticas de ajustes importantes del dispositivo
- Especificar la seguridad exigida del bloqueo de la pantalla
- Restringir el uso de la cámara integrada

Política de bloqueo de pantalla

En este apartado el administrador puede efectuar las siguientes acciones:

- establecer un nivel de seguridad mínimo (patrón, PIN, contraseña) para el código de bloqueo de pantalla del sistema, así como definir la complejidad del código (por ejemplo, la longitud mínima del código).
- establecer el número máximo de intentos de desbloqueo erróneos (tras el cual el dispositivo restablecerá la configuración predeterminada de fábrica).
- establecer la antigüedad máxima del código de bloqueo de pantalla.
- Establecer el temporizador de bloqueo de la pantalla.

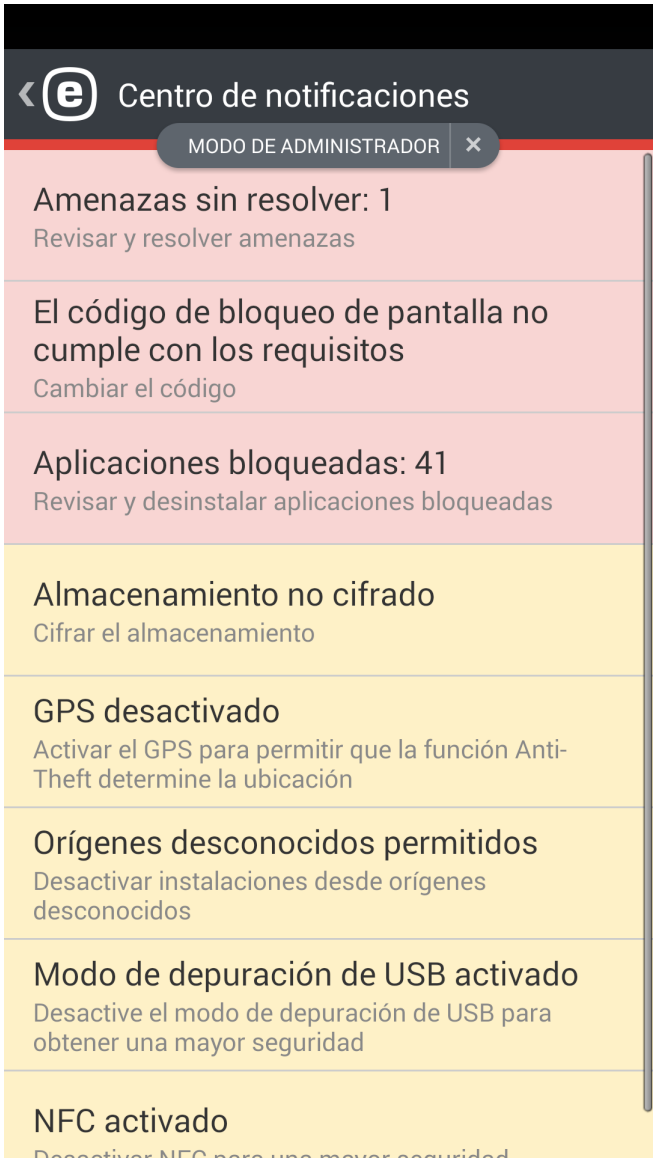
ESET Endpoint Security for Android informa automáticamente al usuario y al administrador de si la configuración actual del dispositivo cumple con las políticas de seguridad corporativas. Si el dispositivo no cumple con las mismas, la aplicación indicará al usuario automáticamente qué cambios deben efectuarse para que vuelva a cumplir con ellas.

Política de configuración del dispositivo

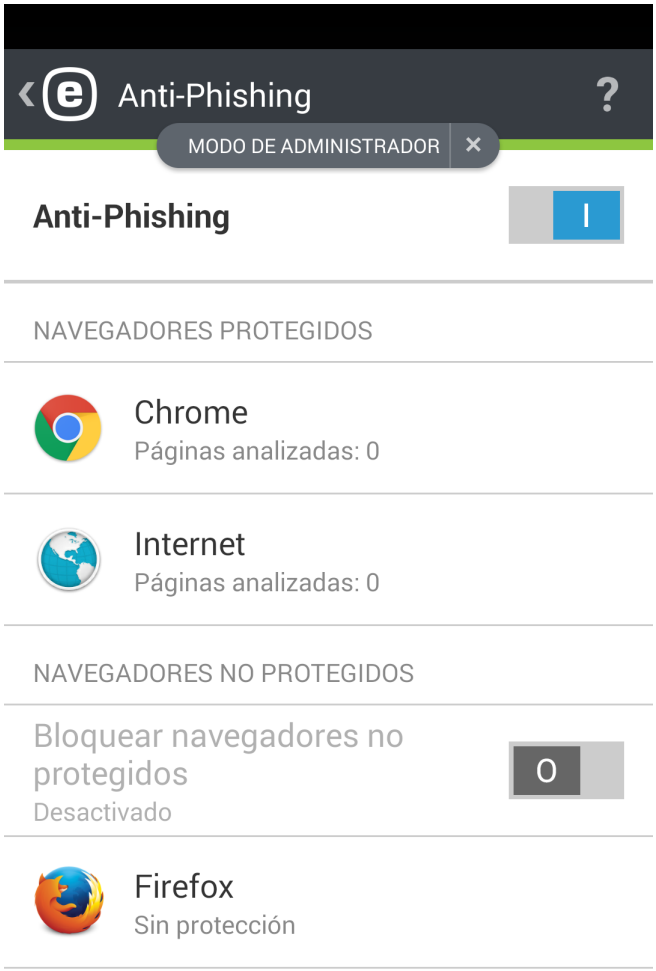
Seguridad del dispositivo incluye también su **Política de configuración del dispositivo** (opción que formaba parte anteriormente de la función **Auditoría de seguridad**), la cual ofrece al administrador del sistema la posibilidad de supervisar la configuración predefinida del dispositivo para determinar si está en el estado recomendado.

Entre los ajustes del dispositivo se incluyen los siguientes:

- Wi-Fi
- Satélites de GPS
- Servicios de localización
- Memoria
- Itinerancia de datos
- Itinerancia de llamadas
- Orígenes desconocidos
- Modo de depuración
- NFC
- Cifrado del almacenamiento
- Dispositivo rooteado



Antiphishing



El *phishing* es una actividad delictiva en la que se aplica ingeniería social, es decir, se manipula al usuario para obtener información confidencial. El phishing suele utilizarse para acceder a datos confidenciales, como números de cuentas bancarias, números de tarjetas de crédito, números PIN o nombres de usuario y contraseñas.

Se recomienda mantener **Antiphishing** habilitado. ESET Endpoint Security for Android analiza las direcciones URL; los posibles ataques de phishing procedentes de sitios web o dominios incluidos en la base de datos de código malicioso de ESET se bloqueará, y se mostrará una notificación de advertencia en la que se le informará del ataque.

IMPORTANTE: Antiphishing se integra en los navegadores web más utilizados con el sistema operativo Android. En general, la protección Antiphishing está disponible para Chrome, Firefox, Opera, Opera Mini, Dolphin, Samsung y los navegadores que se incluyen preinstalados de serie en los dispositivos Android. El resto de navegadores se mostrarán como desprotegidos, y el acceso a ellos puede bloquearse pulsando el interruptor  .

Para que ESET Antiphishing funcione correctamente, debe habilitar **Accesibilidad** en la configuración del sistema Android.

Conceder el permiso de accesibilidad de ESET Endpoint Security for

Android al instalarlo desde el archivo .apk en Android 13

> **Nota**
> Por motivos de seguridad, Android 13 restringe el uso del permiso de accesibilidad a las aplicaciones instaladas desde archivos .apk. Esto evitar que se acceda a él de forma desinformada.
>
> **¿Cómo utiliza ESET Endpoint Security for Android este permiso?**
> Usamos este permiso para acceder a las URL de los sitios web que visita. Analizamos estos sitios web en busca de intención maliciosa, como phishing, malware u otras actividades peligrosas.
> Cuando se detecta un subproceso, el sitio web se bloquea para protegerle a usted y a su información confidencial.
> Los datos a los que se accede mediante el permiso de accesibilidad no se comparten con terceros.

Para resolver el problema de accesibilidad:

1. Abra **Configuración** > **Accesibilidad** > **Aplicaciones descargadas**. La opción ESET Endpoint Security for Android estará de color gris.

2. Pulse la aplicación ESET Endpoint Security for Android para abrir el cuadro de diálogo **Configuración restringida**.

3. A continuación, pulse **"Aceptar"**.

4. Vaya a **Configuración** > **Aplicaciones** > ESET Endpoint Security for Android para abrir la **información de la aplicación**.

5. Pulse el icono del menú de tres puntos ⋮ en la esquina superior derecha > **Permitir configuración restringida**.

Una vez concedido el permiso de accesibilidad, puede empezar a usar la aplicación.

Control web

Utilice la configuración del Control de acceso web para proteger su empresa frente al riesgo de responsabilidad jurídica. Por ejemplo, el Control de acceso web le permite regular el acceso a sitios web que infrinjan los derechos de propiedad intelectual. El objetivo es impedir que los empleados accedan a páginas con contenido inapropiado o perjudicial, o páginas que puedan afectar negativamente a la productividad.

Los empleados o administradores del sistema pueden prohibir el acceso a más de 27 categorías de sitios web predefinidas y más de 140 subcategorías, y registrar estas visitas.

El Control de acceso web es una función administrada. Toda la configuración se controla desde ESET PROTECT Cloud.

> Para que el Control de acceso web funcione, un dispositivo administrado debe cumplir los siguientes requisitos:
> - ESET Endpoint Security for Android versión 3 o posterior.
> - Android versión 8 o posterior.
> - Inscrito en ESET PROTECT Cloud con permisos de administrador del dispositivo.

Navegadores protegidos

- Chrome
- Chrome Beta
- Firefox
- Firefox Beta
- Opera
- Opera Beta
- Opera Mini
- Opera Mini Beta
- Navegador para TV Opera
- Samsung Internet
- Mint
- Navegador Yandex
- DuckDuckGo
- Navegador Kiwi
- Edge
- Silk en dispositivos de Amazon
- Navegador Mi
- Navegador Xiaomi Mi
- Vewd en Android TV
- Las aplicaciones que utilizan componentes protegidos del navegador para la visualización web también están protegidas.

Filtro de llamadas

El **filtro de llamadas** bloquea las llamadas entrantes/salientes en función de las reglas definidas por el usuario.

Cuando se bloquea una llamada entrante, no se muestra ninguna notificación. La ventaja de este comportamiento es que no sufrirá las molestias de información no solicitada, pero siempre puede consultar los registros en busca de llamadas que puedan haberse bloqueado por error.

El Filtro de llamadas no funciona en tabletas no compatibles con llamadas.

Para bloquear las llamadas del último número de teléfono recibido, pulse **Bloquear la última llamada entrante**. Al hacerlo se creará una nueva regla.

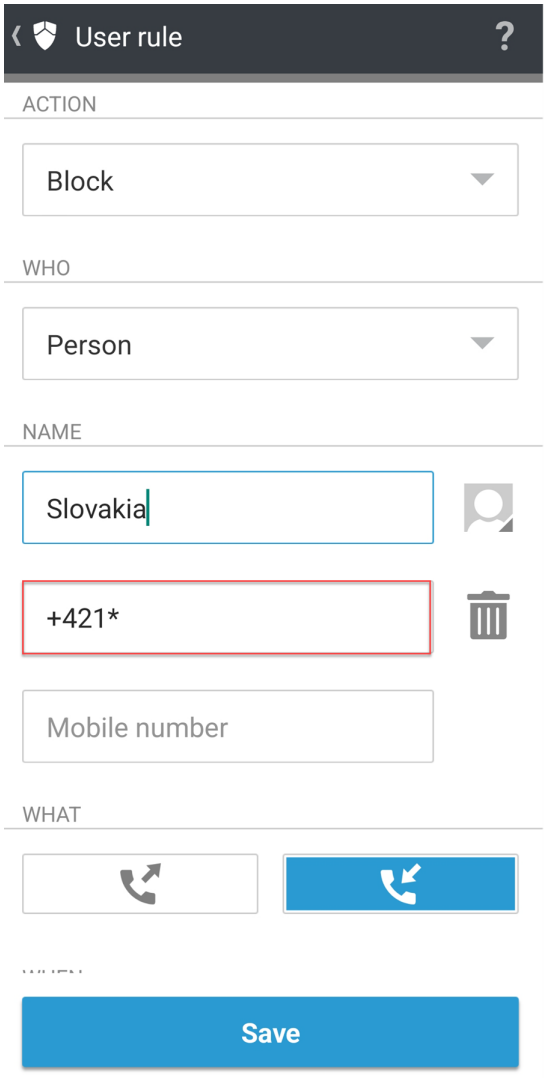
Bloquear números de teléfono con comodines

Puede bloquear un intervalo de números mediante los comodines descritos en la siguiente tabla:

Comodín	Descripción
*	representa varios caracteres
?	representa un solo carácter

Ejemplo

Si no desea recibir llamadas de un país concreto, escriba el código del país y el carácter comodín * en el campo **Número de teléfono móvil**, y se bloquearán todas las llamadas entrantes del país que comience por ese patrón de números. Si quiere excluir algún número de teléfono de ese país, agregue una regla nueva con la acción **Permitir**. En la siguiente imagen se muestra cómo bloquear todas las llamadas de Eslovaquia.



Reglas

Como usuario puede crear reglas de usuario sin necesidad de introducir la contraseña de administración. Las reglas de administración solo pueden crearse en el modo de administración. Las reglas de administración sobrescribirán las reglas de usuario.

Puede encontrar más información sobre la creación de reglas nuevas en este apartado.

Si desea eliminar una entrada de regla existente de la lista **Reglas**, mantenga pulsada la entrada y, a continuación, pulse el icono **Quitar** .

Cómo agregar una regla nueva

Para agregar una regla nueva, pulse **Agregar regla** o pulse el icono de la esquina superior derecha de la pantalla **Reglas**.

Especifique una persona o un grupo de números de teléfono. ESET Endpoint Security for Android reconocerá los grupos de contactos guardados en sus Contactos (por ejemplo, Familia, Amigos o Compañeros). **Todos los números desconocidos** incluirá los números de teléfono que no estén guardados en su lista de contactos. Puede usar esta opción para bloquear las llamadas de teléfono no deseadas (por ejemplo, las llamadas de empresas que le ofrecen servicios) o para impedir que sus empleados llamen a números desconocidos. La opción **Todos los números conocidos** hace referencia a todos los números de teléfono guardados en su lista de contactos. **Números ocultos** se aplicará a personas que tengan su número de teléfono oculto intencionadamente a través de la restricción de identificación de llamadas (CLIR).

Especifique qué debe bloquearse o permitirse:

- Llamadas de voz salientes
- Llamadas de voz entrantes

Si desea aplicar la regla solo durante un periodo de tiempo especificado, pulse **Siempre** > **Personalizado** y seleccione los días de la semana y el intervalo de tiempo durante el que desee aplicar la regla. De forma predeterminada se seleccionan sábado y domingo. Esta función puede resultar práctica si no quiere que se le moleste durante reuniones, viajes de negocio, noches o durante el fin de semana.

NOTA: si está en el extranjero, todos los números de teléfono que introduzca en la lista deben incluir el código de marcación internacional seguido del nombre en cuestión (por ejemplo, +1610100100).

Historial

En el apartado **Historial** puede ver las llamadas y los mensajes bloqueados o permitidos por el Filtro de llamadas. Cada registro incluye el nombre del evento, el número de teléfono correspondiente, la fecha y la hora del suceso.

Si desea modificar una regla relacionada con el número de teléfono o con un contacto que se bloqueó, seleccione la entrada en la lista pulsándola y pulse el icono .

Si desea quitar dicha entrada de la lista, selecciónela y pulse el icono . Para quitar más entradas, mantenga pulsada una de las entradas, seleccione las entradas que desee quitar y pulse el icono .

Configuración

Idioma – De forma predeterminada ESET Endpoint Security for Android se instala en el idioma establecido en la configuración regional del dispositivo (en la configuración de teclado e idioma del SO Android). Si desea cambiar el idioma de la interfaz de usuario de la aplicación, pulse Idioma y seleccione el idioma que quiera.

País – Seleccione el país en el que actualmente trabaja o reside.

Actualizar – Para disfrutar de la máxima protección es importante usar la versión más reciente de ESET Endpoint Security for Android. Pulse Actualizar para ver si hay una versión más reciente disponible para su descarga desde el sitio web de ESET.

Identificador del dispositivo – Configura o cambia el nombre de identificación de su dispositivo para el administrador, en caso de que el dispositivo sea objeto de robo o pérdida.

Administración remota – Conecte el dispositivo a ESET PROTECT.

Configuración avanzada

Haga clic en **Configuración avanzada** para abrir la sección Configuración avanzada.

Notificación permanente – ESET Endpoint Security for Android muestra el icono de notificación en la esquina superior izquierda de la pantalla (barra de estado de Android). Si no quiere que este icono se muestre, cancele la selección de Notificación permanente.

Notificaciones de permisos – Consulte el apartado Administración de permisos.

Enviar datos de uso – Esta opción ayuda a mejorar los productos de ESET mediante el envío de datos anónimos sobre el uso de la aplicación. No se enviará información confidencial. Si no activó esta opción durante el asistente de inicio de instalación, puede hacerlo en la sección Configuración > Configuración avanzada.

Contraseña de administración – Esta opción le permite configurar una nueva contraseña de administración y cambiar la contraseña actual. Para obtener más información, consulte el apartado Contraseña de administración de este documento.

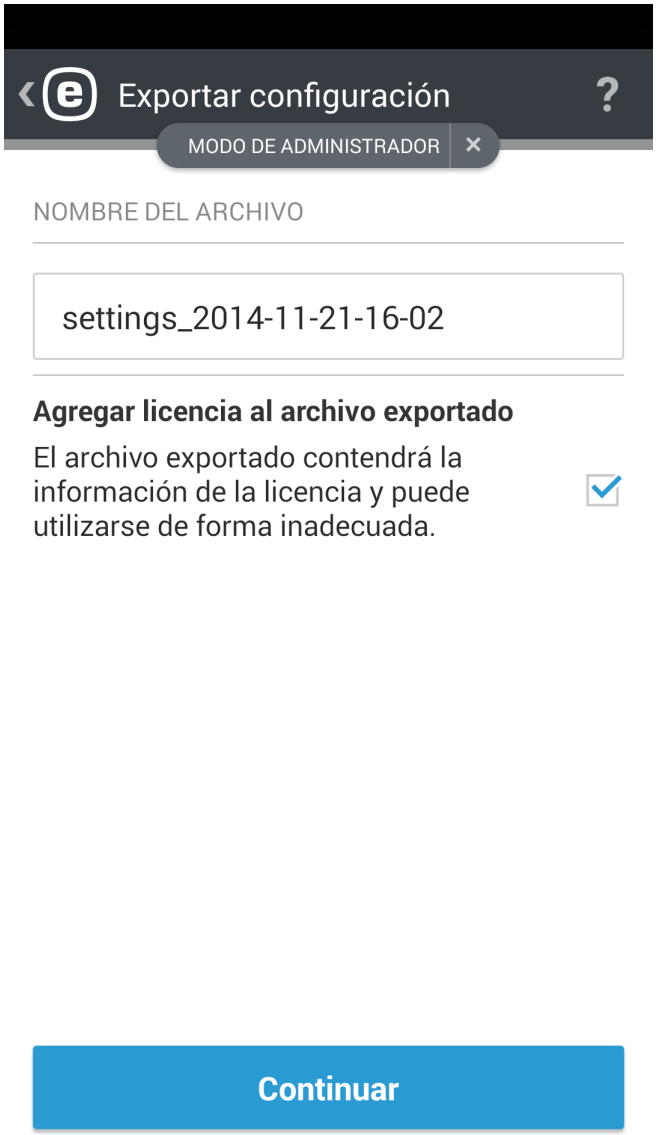
Importar/exportar configuración – Importa o exporta la configuración de una aplicación ESET Endpoint.

Desinstalar – La ejecución del asistente de desinstalación eliminará permanentemente ESET Endpoint Security for Android y las carpetas de cuarentena del dispositivo. Si se activó la Protección contra desinstalación, se le solicitará que introduzca la Contraseña de administración.

Importar/exportar configuración

Para compartir fácilmente la configuración de un dispositivo móvil con otro, si los dispositivos no están administrados por ESET PROTECT, ESET Endpoint Security for Android incluye la posibilidad de exportar e importar la configuración del programa. El administrador puede exportar manualmente la configuración del

dispositivo a un archivo que posteriormente puede compartirse (por correo electrónico, por ejemplo), e importarse en cualquier dispositivo en el que se ejecute la aplicación cliente. Cuando el usuario acepte el archivo de configuración recibido, se definirán automáticamente todos los ajustes y se activará la aplicación (siempre que se incluyera la información de la licencia). Todos los ajustes estarán protegidos por la contraseña de administrador.



Exportar configuración

Si desea exportar la configuración actual de ESET Endpoint Security for Android, indique el nombre del archivo de configuración; la fecha y la hora actuales se incluirán automáticamente. También puede añadir la información de licencia (clave de licencia o dirección de correo electrónico y contraseña de la cuenta del administrador de seguridad) al archivo exportado, pero debe tener en cuenta que esta información no se cifrará y podría utilizarse inadecuadamente.

En el próximo paso, seleccione el método con el que desee compartir el archivo:

- Red Wi-Fi
- Bluetooth

- Correo electrónico
- Gmail
- Aplicación de gestión de archivos (por ejemplo ASTRO File Manager o ES File Explorer)

Importar configuración

Si desea importar la configuración desde un archivo del dispositivo, utilice una aplicación de gestión de archivos para encontrar el archivo de configuración y seleccione ESET Endpoint Security for Android.

La configuración también puede importarse mediante la selección de un archivo en el apartado **Historial**.

Historial

Historial le proporciona la lista de archivos de configuración importados y le permite compartirlos, importarlos o quitarlos.

Contraseña de administración

La **Contraseña de administrador** es necesaria para desbloquear un dispositivo, enviar comandos de Antirrobo, acceder a funciones protegidas por contraseña y desinstalar ESET Endpoint Security for Android.

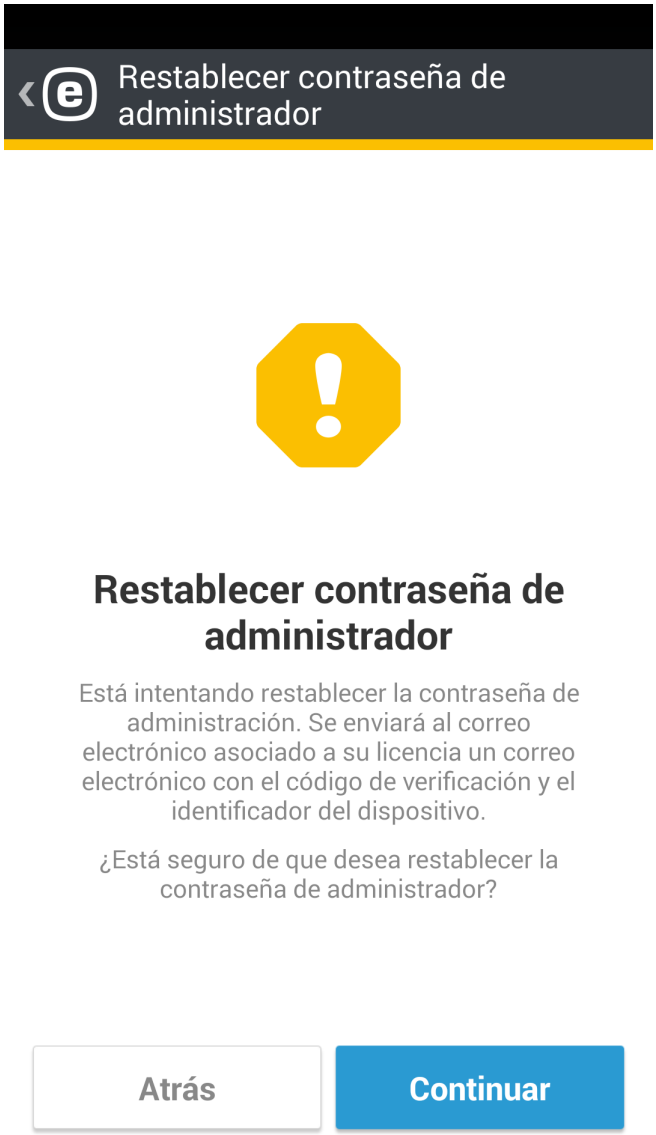
La creación de una **contraseña de administración** impide que los usuarios cambien la configuración y desinstalen ESET Endpoint Security for Android.

Elija la contraseña con cuidado. Para aumentar la seguridad, utilice una combinación de letras en minúscula, letras en mayúscula y números.

Para restablecer la contraseña de administración en un dispositivo que tiene la pantalla bloqueada:

1.Pulse **¿Olvidó su contraseña?** > **Continuar** > **Solicitar código de verificación**. Si el dispositivo no está conectado a Internet, pulse el vínculo **Restablecimiento sin conexión** y póngase en contacto con el servicio de soporte técnico de ESET.

2.Se enviará un mensaje de correo electrónico con el código de verificación y el ID del dispositivo a la dirección de correo electrónico asociada con la licencia de ESET. El código de verificación permanecerá activo durante siete días. Introduzca el código de verificación y una nueva contraseña en la pantalla de bloqueo de su dispositivo.



Administración remota

ESET PROTECT le permite administrar ESET Endpoint Security for Android en un entorno de red directamente desde una ubicación central.

El uso de ESET PROTECT no solo aumenta el nivel de seguridad, sino que además facilita la administración de todos los productos ESET instalados en las estaciones de trabajo y los dispositivos móviles cliente. Los dispositivos con ESET Endpoint Security for Android pueden conectarse a ESET PROTECT utilizando cualquier tipo de conexión a Internet, como WiFi, LAN, WLAN, red de datos móviles (3G, 4G LTE, HSDPAGPRS), etc. siempre que se trate de una conexión a Internet normal (sin proxy ni cortafuegos) y ambos equipos estén configurados correctamente.

Al conectar a ESET PROTECT a través de una red de datos móviles, el éxito de la conexión depende del proveedor de servicios móviles, y requiere una conexión a Internet completa.

Para conectar un dispositivo a ESET PROTECT, agregue el dispositivo a la lista Ordenadores en ESET PROTECT Web Console inscriba el dispositivo con la tarea **Inscripción de dispositivo** e introduzca la **Dirección del servidor de conector de dispositivo móvil**.

El vínculo de inscripción (dirección del servidor MDC) usa el formato estándar `https://MDCserver:port/token` en ESET PROTECT. El vínculo contiene los siguientes valores:

- **servidorMDC**: el nombre de DNS completo o la dirección IP pública que ejecuta el Mobile Device Connector (MDC). El nombre del servidor solo se puede utilizar si la conexión se realiza a través de una red Wi-Fi interna.

- **Puerto**: el número de puerto utilizado para conectar al Mobile Device Connector.

- **Token**: la cadena de caracteres generada por el administrador en ESET PROTECT Web Console.

Para obtener más información sobre cómo administrar la red con ESET PROTECT, consulte los siguientes temas de ayuda en línea:

- Cómo gestionar las políticas

- Cómo crear tareas del cliente

- Más información sobre los informes

Identificador del dispositivo

El identificador del dispositivo ayuda al administrador a identificar el dispositivo en caso de robo o pérdida.

Administración de permisos

En Android 6 (Marshmallow), Google introdujo un nuevo sistema de administración de permisos y ESET Endpoint Security for Android es compatible con él. Las aplicaciones diseñadas para Android 6.0 solicitarán permisos en cuanto empiece a usarlas. En lugar de conceder acceso a una aplicación durante el proceso de instalación, se le solicitará la primera vez que la aplicación quiera acceder a una función concreta del dispositivo.

ESET Endpoint Security for Android requiere acceso a las siguientes funciones:

- **Accesibilidad**: es necesario para el correcto funcionamiento de Antiphishing.

- **Contactos**: es necesario para la funcionalidad Antirrobo y Filtro de llamadas.

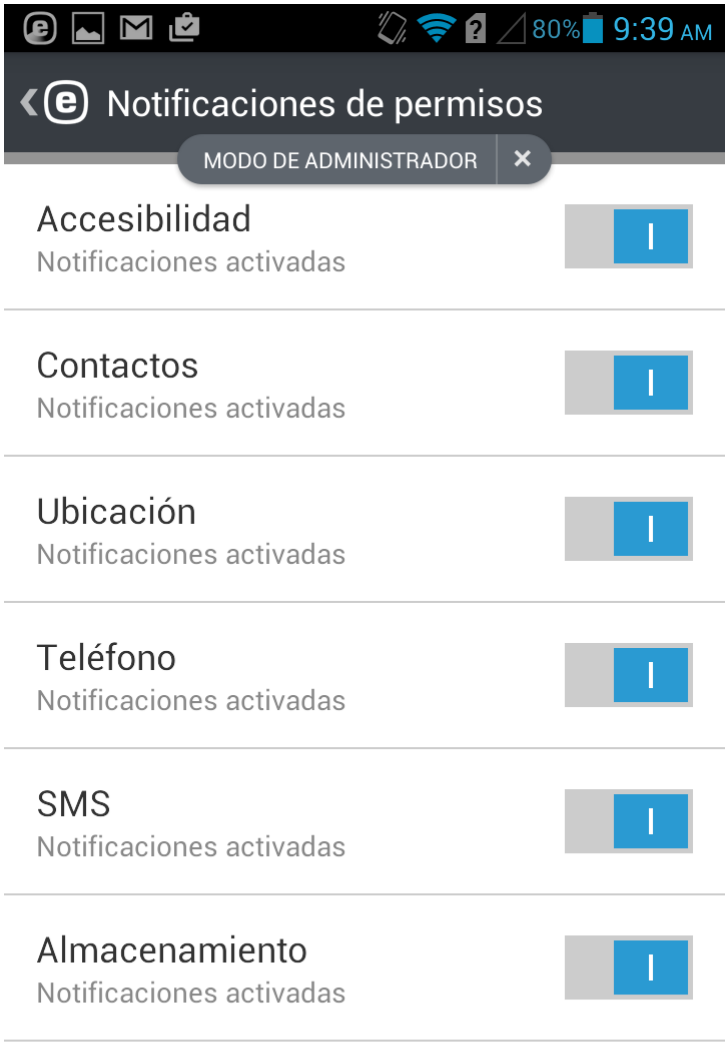
- **Ubicación**: Antirrobo

- **Teléfono**: Antirrobo y Filtro de llamadas.

- **SMS**: Antirrobo y Filtro de llamadas.

- **Almacenamiento**: Antivirus y Antirrobo.

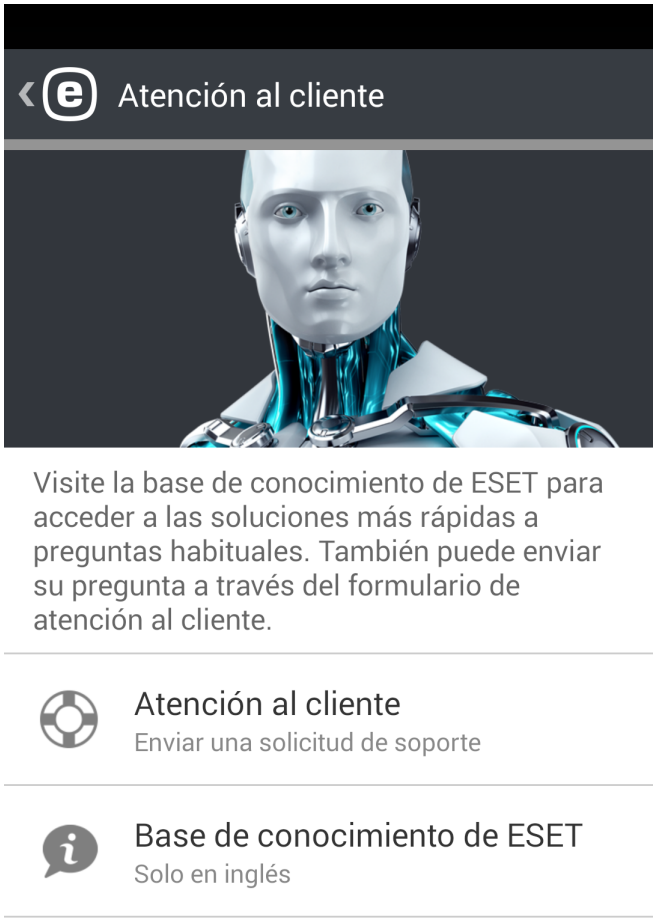
El administrador puede desactivar la supervisión de estos permisos en **Configuración** > **Notificaciones de permisos**.



Atención al cliente

Los especialistas de atención al cliente de ESET están disponibles para prestar ayuda administrativa y ofrecer soporte técnico relacionado con ESET Endpoint Security for Android o cualquier otro producto de ESET.

Para enviar una solicitud de soporte directamente desde su dispositivo, pulse el icono Menú en la pantalla principal de ESET Endpoint Security for Android, pulse **Atención al cliente** > **Atención al cliente** y cumplimente los campos obligatorios.



ESET Endpoint Security for Android incluye funciones de registro avanzado para ayudarle a diagnosticar posibles problemas técnicos. Para ofrecer a ESET un registro detallado de la aplicación, asegúrese de que esté seleccionada la opción **Enviar registro de la aplicación** (predeterminado). Pulse **Enviar** para enviar su solicitud. Un especialista del Servicio de atención al cliente de ESET se pondrá en contacto con usted en la dirección de correo electrónico que haya facilitado.

Programa de mejora de la experiencia del cliente

Al unirse al Programa de mejora de la experiencia de los clientes, proporciona a ESET información anónima relativa al uso de nuestros productos. En nuestra Política de privacidad puede obtener más información sobre el tratamiento de los datos.

Su consentimiento

La participación en este programa es voluntaria y solo se realiza con su consentimiento. Tras unirse, la participación es pasiva, lo que significa que no tiene que hacer nada más. Puede modificar la configuración del producto en cualquier momento para revocar su consentimiento. Al hacerlo nos impedirá continuar con el tratamiento de sus datos anónimos.

¿Qué tipos de información recopilamos?

Datos sobre interacciones con el producto

Estos datos nos ofrecen información sobre cómo se usan nuestros productos. Gracias a ellos podemos saber, por ejemplo, qué funcionalidades se usan con más frecuencia, qué configuración modifican los usuarios o cuánto tiempo pasan utilizando el producto.

Datos sobre dispositivos

Recopilamos esta información para comprender dónde y en qué dispositivos se usan nuestros productos. Entre los datos más habituales se incluyen el modelo de dispositivo, el país, la versión y el nombre del sistema operativo.

Datos de diagnósticos de error

También se recopila información sobre errores y bloqueos, como por ejemplo qué error se ha producido y qué acciones lo han provocado.

¿Por qué recopilamos esta información?

Esta información anónima nos permite mejorar nuestros productos para usuarios como usted. Nos ayuda a conseguir que sean más prácticos, sencillos de usar y a que tengan la menor cantidad de fallos posible.

¿Quién controla esta información?

ESET, spol. s r.o. es el único responsable del tratamiento de los datos recopilados en el marco del programa. Esta información no se comparte con terceros.

Acuerdo de licencia para el usuario final

Fecha de entrada en vigor: 19 de octubre de 2021.

IMPORTANTE: Lea los términos y condiciones de la aplicación del producto que se detallan a continuación antes de descargarlo, instalarlo, copiarlo o utilizarlo. **LA DESCARGA, LA INSTALACIÓN, LA COPIA O LA UTILIZACIÓN DEL SOFTWARE IMPLICAN SU ACEPTACIÓN DE ESTOS TÉRMINOS Y CONDICIONES Y DE LA POLÍTICA DE PRIVACIDAD.**

Acuerdo de licencia para el usuario final

En virtud de los términos de este Acuerdo de licencia para el usuario final ("Acuerdo"), firmado por ESET, spol. s r. o., con domicilio social en Einsteinova 24, 85101 Bratislava, Slovak Republic, empresa inscrita en el Registro Mercantil administrado por el tribunal de distrito de Bratislava I, sección Sro, número de entrada 3586/B, número de registro comercial 31333532 ("ESET" o "el Proveedor") y usted, una persona física o jurídica ("Usted" o el "Usuario final"), tiene derecho a utilizar el Software definido en el artículo 1 del presente Acuerdo. El Software definido en el artículo 1 del presente Acuerdo puede almacenarse en un soporte de datos, enviarse por correo electrónico, descargarse de Internet, descargarse de los servidores del Proveedor u obtenerse de otras fuentes en virtud de los términos y condiciones especificados a continuación.

ESTO NO ES UN CONTRATO DE VENTA, SINO UN ACUERDO SOBRE LOS DERECHOS DEL USUARIO FINAL. El proveedor sigue siendo el propietario de la copia del software y del soporte físico incluidos en el paquete de

venta, así como de todas las copias que el usuario final pueda realizar en virtud de este acuerdo.

Al hacer clic en las opciones "Acepto" o "Acepto…" durante la instalación, la descarga, la copia o la utilización del Software, expresa su aceptación de los términos y condiciones de este Acuerdo y acepta la Política de Privacidad. Si no acepta todos los términos y condiciones de este Acuerdo o la Política de Privacidad, haga clic en la opción de cancelación, cancele la instalación o descarga o destruya o devuelva el Software, el soporte de instalación, la documentación adjunta y el recibo de compra al Proveedor o al lugar donde haya adquirido el Software.

USTED ACEPTA QUE SU UTILIZACIÓN DEL SOFTWARE INDICA QUE HA LEÍDO ESTE ACUERDO, QUE LO COMPRENDE Y QUE ACEPTA SU SUJECIÓN A LOS TÉRMINOS Y CONDICIONES.

1. **Software**. En este acuerdo, el término "Software" se refiere a: (i) el programa informático que acompaña a este Acuerdo y todos sus componentes; (ii) todo el contenido de los discos, CD-ROM, DVD, mensajes de correo electrónico y documentos adjuntos, o cualquier otro soporte que esté vinculado a este Acuerdo, incluido el código objeto del Software proporcionado en un soporte de datos, por correo electrónico o descargado de Internet; (iii) todas las instrucciones escritas y toda la documentación relacionada con el Software, especialmente todas las descripciones del mismo, sus especificaciones, todas las descripciones de las propiedades o el funcionamiento del Software, todas las descripciones del entorno operativo donde se utiliza, las instrucciones de uso o instalación del software o todas las descripciones de uso del mismo ("Documentación"); (iv) copias, reparaciones de posibles errores, adiciones, extensiones y versiones modificadas del software, así como actualizaciones de sus componentes, si las hay, para las que el Proveedor le haya concedido una licencia en virtud del artículo 3 de este Acuerdo. El Software se proporciona únicamente en forma de código objeto ejecutable.

2. **Instalación, Ordenador y una Clave de licencia**. El Software suministrado en un soporte de datos, enviado por correo electrónico, descargado de Internet, descargado de los servidores del Proveedor u obtenido de otras fuentes requiere instalación. Debe instalar el Software en un Ordenador correctamente configurado que cumpla, como mínimo, los requisitos especificados en la Documentación. El método de instalación se describe en la Documentación. No puede haber programas informáticos o hardware que puedan afectar negativamente al Software instalados en el Ordenador donde instale el Software. Ordenador significa hardware, lo que incluye, entre otros elementos, ordenadores personales, portátiles, estaciones de trabajo, ordenadores de bolsillo, smartphones, dispositivos electrónicos de mano u otros dispositivos electrónicos para los que esté diseñado el Software, en el que se instale o utilice. Clave de licencia significa la secuencia exclusiva de símbolos, letras, números o signos especiales facilitada al Usuario final para permitir el uso legal del Software, su versión específica o la ampliación de la validez de la Licencia de conformidad con este Acuerdo.

3. **Licencia**. Siempre que haya aceptado los términos de este Acuerdo y cumpla con todos los términos y condiciones aquí especificados, el Proveedor le concederá los siguientes derechos (la "Licencia"):

a) **Instalación y uso.** Tendrá el derecho no exclusivo e intransferible de instalar el Software en el disco duro de un ordenador u otro soporte permanente para el almacenamiento de datos, de instalar y almacenar el Software en la memoria de un sistema informático y de implementar, almacenar y mostrar el Software.

b) **Estipulación del número de licencias.** El derecho de uso del software está sujeto a un número de usuarios finales. La expresión "un usuario final" se utilizará cuando se haga referencia a lo siguiente: (i) la instalación del software en un sistema informático o (ii) un usuario informático que acepta correo electrónico a través de un Agente de usuario de correo (“un AUC”) cuando el alcance de una licencia esté vinculado al número de buzones de correo. Si el AUC acepta correo electrónico y, posteriormente, lo distribuye de forma automática a varios usuarios, el número de usuarios finales se determinará según el número real de usuarios para los que se distribuyó el correo electrónico. Si un servidor de correo realiza la función de una pasarela de correo, el número de usuarios finales será equivalente al número de usuarios de servidor de correo a los que dicha pasarela preste servicios. Si se envía un número indefinido de direcciones de correo electrónico a un usuario, que las acepta (por ejemplo, mediante alias), y el cliente no distribuye los mensajes automáticamente a más usuarios, se necesita una

licencia para un ordenador. No utilice la misma licencia en varios ordenadores de forma simultánea. El Usuario final tiene derecho a introducir la Clave de licencia en el Software si tiene derecho a utilizar el Software de acuerdo con la limitación derivada del número de licencias otorgadas por el Proveedor. La Clave de licencia se considera confidencial: no debe compartir la Licencia con terceros ni permitir que terceros utilicen la Clave de licencia, a menos que lo permitan este Acuerdo o el Proveedor. Si su Clave de licencia se ve expuesta, notifíqueselo inmediatamente al Proveedor.

c) **Home Edition o Business Edition.** La versión Home Edition del Software se utilizará exclusivamente en entornos privados o no comerciales para uso doméstico y familiar. Debe obtener una versión Business Edition del Software para poder utilizarlo en entornos comerciales y en servidores de correo, relays de correo, puertas de enlace de correo o puertas de enlace a Internet.

d) **Vigencia de la licencia.** Tiene derecho a utilizar el Software durante un período de tiempo limitado.

e) **Software OEM.** El Software clasificado como "OEM" solo se puede utilizar en el equipo con el que lo haya obtenido. No se puede transferir a otro ordenador.

f) **Software de prueba y NFR.** El Software cuya venta esté prohibida o de prueba no se puede pagar, y únicamente se debe utilizar para demostraciones o para probar las características del Software.

g) **Terminación de la licencia.** La licencia se terminará automáticamente cuando concluya su período de vigencia. Si no cumple algunas de las disposiciones de este acuerdo, el proveedor podrá cancelarlo sin perjuicio de los derechos o soluciones legales que tenga a su disposición para estos casos. En caso de cancelación de la Licencia, Usted debe eliminar, destruir o devolver (a sus expensas) el Software y todas las copias de seguridad del mismo a ESET o a la tienda donde lo haya adquirido. Tras la terminación de la Licencia, el Proveedor estará autorizado a cancelar el derecho que tiene el Usuario final para utilizar las funciones del Software que requieren conexión a los servidores del Proveedor o de terceros.

4. **Funciones con requisitos de recopilación de datos y conexión a Internet.** El Software necesita conexión a Internet para funcionar correctamente, y debe conectarse periódicamente a los servidores del Proveedor o a servidores de terceros; además, se recopilarán datos de acuerdo con la Política de Privacidad. La conexión a Internet y la recopilación de datos son necesarias para las siguientes funciones del Software:

a) **Actualizaciones del software.** El Proveedor podrá publicar actualizaciones del Software ("Actualizaciones") cuando lo estime oportuno, aunque no está obligado a proporcionarlas. Esta función se activa en la sección de configuración estándar del software y las actualizaciones se instalan automáticamente, a menos que el usuario final haya desactivado la instalación automática de actualizaciones. Para proporcionar Actualizaciones, es necesario verificar la autenticidad de la licencia, lo que incluye información sobre el ordenador o la plataforma en los que está instalado el Software, de acuerdo con la Política de Privacidad.

La Política de final de la vida útil ("Política de final de la vida útil"), disponible en https://go.eset.com/eol_business, puede regir la forma de proporcionar las Actualizaciones. No se proporcionarán Actualizaciones después de que el Software o cualquiera de sus funciones lleguen a la fecha de final de la vida útil definida en la Política de final de la vida útil.

b) **Envío de amenazas e información al proveedor**. El software incluye funciones que recogen muestras de virus informáticos y otros programas informáticos maliciosos, así como objetos sospechosos, problemáticos, potencialmente indeseables o potencialmente inseguros como archivos, direcciones URL, paquetes de IP y tramas Ethernet ("amenazas") y posteriormente las envía al Proveedor, incluida, a título enunciativo pero no limitativo, información sobre el proceso de instalación, el Ordenador o la plataforma en la que el Software está instalado e información sobre las operaciones y las funciones del Software ("Información"). La Información y las Amenazas pueden contener datos (incluidos datos personales obtenidos de forma aleatoria o accidental) sobre el Usuario final u otros usuarios del ordenador en el que el Software está instalado, así como los archivos afectados por las

Amenazas junto con los metadatos asociados.

La información y las amenazas pueden recogerse mediante las siguientes funciones del software:

i. La función del sistema de reputación LiveGrid incluye la recopilación y el envío al proveedor de algoritmos hash unidireccionales relacionados con las amenazas. Esta función se activa en la sección de configuración estándar del software.

ii. La función del Sistema de Respuesta LiveGrid incluye la recopilación y el envío al Proveedor de las Amenazas con los metadatos y la Información asociados. Esta función la puede activar el Usuario final durante el proceso de instalación del Software.

El Proveedor solo podrá utilizar la Información y las Amenazas recibidas con fines de análisis e investigación de las Amenazas y mejora de la verificación de la autenticidad del Software y de la Licencia, y deberá tomar las medidas pertinentes para garantizar la seguridad de las Amenazas y la Información recibidas. Si se activa esta función del Software, el Proveedor podrá recopilar y procesar las Amenazas y la Información como se especifica en la Política de Privacidad y de acuerdo con la normativa legal relevante. Estas funciones se pueden desactivar en cualquier momento.

A los efectos de este Acuerdo, es necesario recopilar, procesar y almacenar datos que permitan al Proveedor identificarle, de acuerdo con la Política de Privacidad. Acepta que el Proveedor puede comprobar por sus propios medios si está utilizando el Software de conformidad con las disposiciones de este Acuerdo. Acepta que, a los efectos de este Acuerdo, es necesaria la transferencia de sus datos, durante la comunicación entre el Software y los sistemas informáticos del Proveedor o sus socios comerciales, como parte de la red de distribución y asistencia técnica del Proveedor, para garantizar la funcionalidad del Software y la autorización para utilizar el Software y proteger los derechos del Proveedor.

Tras la terminación de este Acuerdo, el Proveedor y sus socios comerciales, como parte de la red de distribución y asistencia técnica del Proveedor, estarán autorizados a transferir, procesar y almacenar sus datos identificativos fundamentales para fines relacionados con la facturación, la ejecución del Acuerdo y la transmisión de notificaciones en su Ordenador.

En la Política de Privacidad, disponible en el sitio web del Proveedor y accesible directamente desde el proceso de instalación, pueden encontrarse detalles sobre privacidad, protección de datos personales y Sus derechos como persona interesada. También puede visitarla desde la sección de ayuda del Software.

5. **Ejercicio de los derechos de usuario final**. Debe ejercer los derechos del Usuario final en persona o a través de sus empleados. Tiene derecho a utilizar el Software solamente para asegurar sus operaciones y proteger los Ordenadores o los sistemas informáticos para los que ha obtenido una Licencia.

6. **Restricciones de los derechos.** No puede copiar, distribuir, extraer componentes ni crear versiones derivadas del software. El uso del software está sujeto a las siguientes restricciones:

a) Puede realizar una copia del software en un soporte de almacenamiento permanente, a modo de copia de seguridad para el archivo, siempre que esta no se instale o utilice en otro ordenador. La creación de más copias del software constituirá una infracción de este acuerdo.

b) No puede utilizar, modificar, traducir ni reproducir el software, ni transferir los derechos de uso del software o copias del mismo de ninguna forma que no se haya establecido expresamente en este acuerdo.

c) No puede vender, conceder bajo licencia, alquilar, arrendar ni prestar el software, ni utilizarlo para prestar servicios comerciales.

d) No puede aplicar la ingeniería inversa, descompilar ni desmontar el software, ni intentar obtener de otra manera su código fuente, salvo que la ley prohíba expresamente esta restricción.

e) Acepta que el uso del software se realizará de conformidad con la legislación aplicable en la jurisdicción donde se utilice, y que respetará las restricciones aplicables a los derechos de copyright y otros derechos de propiedad intelectual.

f) Usted manifiesta estar de acuerdo en usar el software y sus funciones únicamente de manera tal que no se vean limitadas las posibilidades del usuario final de acceder a tales servicios. El proveedor se reserva el derecho de limitar el alcance de los servicios proporcionados a ciertos usuarios finales, a fin de permitir que la máxima cantidad posible de usuarios finales pueda hacer uso de esos servicios. El hecho de limitar el alcance de los servicios también significará la total anulación de la posibilidad de usar cualquiera de las funciones del software y la eliminación de los datos y la información que haya en los servidores del proveedor o de terceros en relación con una función específica del software.

g) Se compromete a no realizar actividades que impliquen el uso de la Clave de licencia en contra de los términos de este Acuerdo o que signifiquen facilitar la Clave de licencia a personas no autorizadas a utilizar el Software, como transferir la Clave de licencia utilizada o sin utilizar de cualquier forma, así como la reproducción no autorizada, la distribución de Claves de licencia duplicadas o generadas o el uso del Software como resultado del uso de una Clave de licencia obtenida de fuentes distintas al Proveedor.

7. **Copyright**. El software y todos los derechos, incluidos, entre otros, los derechos propietarios y de propiedad intelectual, son propiedad de ESET y/o sus proveedores de licencias. Los propietarios están protegidos por disposiciones de tratados internacionales y por todas las demás leyes aplicables del país en el que se utiliza el software. La estructura, la organización y el código del software son secretos comerciales e información confidencial de ESET y/o sus proveedores de licencias. Solo puede copiar el software según lo estipulado en el artículo 6 (a). Todas las copias autorizadas en virtud de este acuerdo deben contener los mismos avisos de copyright y de propiedad que aparecen en el software. Por el presente acepta que, si aplica técnicas de ingeniería inversa al código fuente del software, lo descompila, lo desmonta o intenta descubrirlo de alguna otra manera que infrinja las disposiciones de este acuerdo, se considerará de forma automática e irrevocable que la totalidad de la información así obtenida se deberá transferir al proveedor y que este será su propietario a partir del momento en que dicha información exista, sin perjuicio de los derechos del proveedor con respecto a la infracción de este acuerdo.

8. **Reserva de derechos**. Por este medio, el Proveedor se reserva todos los derechos del Software, excepto por los derechos concedidos expresamente bajo los términos de este Acuerdo a Usted como el Usuario final del Software.

9. **Versiones en varios idiomas, software en soporte dual, varias copias**. Si el software es compatible con varias plataformas o idiomas, o si recibe varias copias del software, solo puede utilizar el software para el número de sistemas informáticos y para las versiones para los que haya obtenido una licencia. No puede vender, arrendar, alquilar, sublicenciar, prestar o transferir ninguna versión o copias del Software no utilizado por Usted.

10. **Comienzo y rescisión del Acuerdo.** Este acuerdo es efectivo a partir de la fecha en que acepte sus términos. Puede terminar este acuerdo en cualquier momento mediante la desinstalación, destrucción o devolución (a sus expensas) del software, todas las copias de seguridad y todo el material relacionado que le hayan suministrado el proveedor o sus socios comerciales. Su derecho a usar el Software y sus funciones puede estar sujeto a la Política de final de la vida útil. Cuando el Software o cualquiera de sus funciones lleguen a la fecha de final de la vida útil definida en la Política de final de la vida útil, dejará de tener derecho a utilizar el Software. Independientemente del modo de terminación de este acuerdo, las disposiciones de los artículos 7, 8, 11, 13, 19 y 21 seguirán en vigor de forma ilimitada.

11. **DECLARACIONES DEL USUARIO FINAL**. COMO USUARIO FINAL, USTED RECONOCE QUE EL SOFTWARE SE

SUMINISTRA "TAL CUAL", SIN GARANTÍA EXPRESA O IMPLÍCITA DE NINGÚN TIPO Y DENTRO DEL ALCANCE MÁXIMO PERMITIDO POR LA LEGISLACIÓN APLICABLE. NI EL PROVEEDOR, SUS PROVEEDORES DE LICENCIAS O SUS AFILIADOS NI LOS TITULARES DEL COPYRIGHT OFRECEN NINGUNA GARANTÍA O DECLARACIÓN, EXPRESA O IMPLÍCITA; EN PARTICULAR, NINGUNA GARANTÍA DE VENTAS O IDONEIDAD PARA UNA FINALIDAD ESPECÍFICA O GARANTÍAS DE QUE EL SOFTWARE NO INFRINJA UNA PATENTE, DERECHOS DE PROPIEDAD INTELECTUAL, MARCAS COMERCIALES U OTROS DERECHOS DE TERCEROS. NI EL PROVEEDOR NI NINGUNA OTRA PARTE GARANTIZAN QUE LAS FUNCIONES CONTENIDAS EN EL SOFTWARE SATISFAGAN SUS REQUISITOS O QUE EL SOFTWARE FUNCIONE SIN INTERRUPCIONES NI ERRORES. ASUME TODOS LOS RIESGOS Y RESPONSABILIDAD DE LA SELECCIÓN DEL SOFTWARE PARA CONSEGUIR LOS RESULTADOS QUE DESEA Y DE LA INSTALACIÓN, EL USO Y LOS RESULTADOS OBTENIDOS.

12. **Ninguna obligación adicional**. Este Acuerdo no crea obligaciones del lado del Proveedor y sus licenciatarios, excepto las obligaciones específicamente indicadas en este Acuerdo.

13. **LIMITACIÓN DE RESPONSABILIDAD**. HASTA EL ALCANCE MÁXIMO PERMITIDO POR LA LEGISLACIÓN APLICABLE, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O SUS PROVEEDORES DE LICENCIAS SERÁN RESPONSABLES DE PÉRDIDAS DE BENEFICIOS, DE INGRESOS, DE VENTAS O DE DATOS NI DE COSTES DERIVADOS DE LA OBTENCIÓN DE PRODUCTOS O SERVICIOS DE SUSTITUCIÓN, DE DAÑOS A LA PROPIEDAD, DE DAÑOS PERSONALES, DE LA INTERRUPCIÓN DEL NEGOCIO, DE LA PÉRDIDA DE INFORMACIÓN COMERCIAL O DE DAÑOS ESPECIALES, DIRECTOS, INDIRECTOS, ACCIDENTALES, ECONÓMICOS, DE COBERTURA, CRIMINALES O SUCESIVOS, CAUSADOS DE CUALQUIER MODO, YA SEA A CAUSA DE UN CONTRATO, UNA CONDUCTA INADECUADA INTENCIONADA, UNA NEGLIGENCIA U OTRO HECHO QUE ESTABLEZCA RESPONSABILIDAD, DERIVADOS DE LA INSTALACIÓN, EL USO O LA INCAPACIDAD DE USO DEL SOFTWARE, INCLUSO EN EL CASO DE QUE AL PROVEEDOR O A SUS PROVEEDORES DE LICENCIAS O FILIALES SE LES HAYA NOTIFICADO LA POSIBILIDAD DE DICHOS DAÑOS. DADO QUE DETERMINADOS PAÍSES Y JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE RESPONSABILIDAD, PERO PUEDEN PERMITIR LA LIMITACIÓN DE RESPONSABILIDAD, EN DICHOS CASOS, LA RESPONSABILIDAD DEL PROVEEDOR, SUS EMPLEADOS, LICENCIATARIOS O AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR LA LICENCIA.

14. Ninguna de las disposiciones de este acuerdo se establece en perjuicio de los derechos estatutarios de una parte que actúe como consumidor en contra de lo aquí dispuesto.

15. **Soporte técnico**. ESET y los terceros contratados por ESET proporcionarán soporte técnico, a su discreción, sin ningún tipo de garantía o declaración. No se proporcionará soporte técnico después de que el Software o cualquiera de sus funciones lleguen a la fecha de final de la vida útil definida en la Política de final de la vida útil. El usuario final debe realizar una copia de seguridad de todos los datos, aplicaciones de software y programas almacenados en el ordenador antes de recibir soporte técnico. ESET y/o los terceros contratados por ESET no se hacen responsables de los daños, las pérdidas de datos, elementos en propiedad, software o hardware ni las pérdidas de ingresos a causa de la prestación del servicio de soporte técnico. ESET y/o los terceros contratados por ESET se reservan el derecho de determinar que la solución de un problema no entra dentro del ámbito de soporte técnico. ESET se reserva el derecho de rechazar, anular o terminar, a su discreción, la disposición de servicio técnico. Pueden ser necesarios los datos de Licencia, la Información y otros datos de acuerdo con la Política de Privacidad para prestar soporte técnico.

16. **Transferencia de la licencia**. El software se puede transferir de un sistema informático a otro, a no ser que se indique lo contrario en los términos del acuerdo. Si no se infringen los términos del acuerdo, el usuario solo puede transferir la licencia y todos los derechos derivados de este acuerdo a otro usuario final de forma permanente con el consentimiento del proveedor, y con sujeción a las siguientes condiciones: (i) el usuario final original no conserva ninguna copia del software; (ii) la transferencia de derechos es directa, es decir, del usuario final original al nuevo usuario final; (iii) el nuevo usuario final asume todos los derechos y obligaciones correspondientes al usuario final original en virtud de los términos de este acuerdo; (iv) el usuario final original proporciona al nuevo usuario final la documentación necesaria para verificar la autenticidad del software, tal

como se especifica en el artículo 17.

17. **Verificación de la autenticidad del Software.** El Usuario final puede demostrar su derecho a utilizar el Software de las siguientes maneras: (i) mediante un certificado de licencia emitido por el Proveedor o un tercero designado por el Proveedor; (ii) mediante un acuerdo de licencia por escrito, si se ha celebrado dicho acuerdo; (iii) mediante el envío de un mensaje de correo electrónico enviado por el Proveedor con la información de la licencia (nombre de usuario y contraseña). Pueden ser necesarios los datos de Licencia y de identificación del Usuario final de acuerdo con la Política de Privacidad para verificar la autenticidad del Software.

18. **Licencia para organismos públicos y gubernamentales de EE.UU.**. El software se proporcionará a los organismos públicos, incluido el gobierno de Estados Unidos, con los derechos y las restricciones de licencia descritos en este acuerdo.

19. **Cumplimiento de las normas de control comercial**.

a) No puede exportar, reexportar, transferir ni poner el Software a disposición de ninguna persona de alguna otra forma, ni directa ni indirectamente, ni usarlo de ninguna forma ni participar en ninguna acción si ello puede tener como resultado que ESET o su grupo, sus filiales o las filiales de cualquier empresa del grupo, así como las entidades controladas por dicho grupo ("Filiales"), incumplan las Leyes de control comercial o sufran consecuencias negativas debido a dichas Leyes, entre las que se incluyen

i. cualquier ley que controle, restrinja o imponga requisitos de licencia en relación con la exportación, la reexportación o la transferencia de bienes, software, tecnología o servicios, publicada oficialmente o adoptada por cualquier autoridad gubernamental, estatal o reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados miembros o cualquier país en el que deban cumplirse obligaciones en virtud del Acuerdo o en el que ESET o cualquiera de sus Filiales estén registradas u operen y

ii. cualesquier sanciones, restricciones, embargos o prohibiciones de importación o exportación, de transferencia de fondos o activos o de prestación de servicios, todo ello en los ámbitos económico, financiero y comercial o en cualquier otro ámbito, o cualquier medida equivalente, impuestos por cualquier autoridad gubernamental, estatal o reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados miembros o cualquier país en el que deban cumplirse obligaciones en virtud del Acuerdo o en el que ESET o cualquiera de sus Filiales estén registradas u operen.

(los actos jurídicos a los que se hace referencia en los puntos i e ii. anteriores se denominan, conjuntamente, "Leyes de control comercial").

b) ESET tiene derecho a suspender las obligaciones adquiridas en virtud de estos Términos o a rescindir los Términos con efecto inmediato en el caso de que:

i. con una base razonable para fundamentar su opinión, ESET determine que el Usuario ha incumplido o es probable que incumpla lo dispuesto en el Artículo 19 a) del Acuerdo; o

ii. el Usuario final o el Software queden sujetos a las Leyes de control comercial y, como resultado, con una base razonable para fundamentar su opinión, ESET determine que continuar cumpliendo las obligaciones adquiridas en virtud del Acuerdo podría causar que ESET o sus Filiales incumplieran las Leyes de control comercial o sufrieran consecuencias negativas debido a dichas Leyes.

c) Ninguna disposición del Acuerdo tiene por objeto inducir u obligar a ninguna de las partes a actuar o dejar de actuar (ni a aceptar actuar o dejar de actuar) de forma incompatible con las Leyes de control comercial aplicables o de forma penalizada o prohibida por dichas Leyes, y ninguna disposición del Acuerdo debe interpretarse en ese sentido.

20. **Avisos**. Los avisos y las devoluciones del Software y la Documentación deben enviarse a ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, sin perjuicio del derecho de ESET a comunicarle los cambios que se produzcan en este Acuerdo, en las Políticas de privacidad, en la Política de final de la vida útil y en la Documentación de conformidad con el art. 22 del Acuerdo. ESET puede enviarle correos electrónicos y notificaciones en la aplicación a través del Software o publicar la comunicación en su sitio web. Acepta recibir comunicaciones legales de ESET en formato electrónico, lo que incluye cualquier comunicación sobre cambios en los Términos, los Términos especiales o las Políticas de privacidad, cualquier propuesta o aceptación de contrato o invitación para negociar, avisos u otras comunicaciones legales. Dicha comunicación electrónica se considerará recibida por escrito, a menos que la legislación aplicable requiera específicamente una forma de comunicación diferente.

21. **Legislación aplicable**. Este acuerdo se regirá e interpretará de conformidad con la legislación eslovaca. El usuario final y el proveedor aceptan que los principios del conflicto entre las leyes y la Convención de las Naciones Unidas para la Venta Internacional de Bienes no serán de aplicación. Acepta expresamente que las disputas o reclamaciones derivadas de este acuerdo y relacionadas con el proveedor, así como las disputas o reclamaciones relacionadas con el uso del software, se resolverán en el Tribunal del Distrito de Bratislava I. Acepta expresamente la jurisdicción de dicho tribunal.

22. **Disposiciones generales**. El hecho de que alguna de las disposiciones de este acuerdo no sea válida o aplicable no afectará a la validez de las demás disposiciones del acuerdo, que seguirán siendo válidas y aplicables de conformidad con las condiciones aquí estipuladas. Este Acuerdo se ha formalizado en inglés. Si se realiza una traducción del Acuerdo por motivos de comodidad o por cualquier otro motivo, o en caso de discrepancia entre las versiones de este Acuerdo en diferentes idiomas, prevalecerá la versión en inglés.

ESET se reserva el derecho a realizar cambios en el Software y a modificar los términos de este Acuerdo, sus Anexos, la Política de Privacidad, la Política de final de la vida útil y la Documentación, o de cualquier parte de lo anterior, en cualquier momento mediante la actualización del documento pertinente (i) para reflejar los cambios del Software o en la forma en la que ESET desarrolla su actividad, (ii) por motivos legales, de legislación o de seguridad, o (iii) para evitar un uso inadecuado o perjuicios. Se le notificará cualquier modificación del Acuerdo por correo electrónico, mediante una notificación en la aplicación o a través de otros medios electrónicos. Si no está de acuerdo con los cambios propuestos para el Acuerdo, puede rescindirlo de acuerdo con el art. 10 en el plazo de 30 días después de recibir un aviso del cambio. A menos que rescinda el Acuerdo dentro de este límite de tiempo, los cambios propuestos se considerarán aceptados y estarán vigentes para Usted a partir de la fecha en que reciba un aviso del cambio.

Este es el Acuerdo completo entre el Proveedor y Usted en relación con el Software y sustituye cualquier otra representación, debate, compromiso, comunicación o publicidad previas relacionadas con el Software.

EULAID: EULA-PRODUCT-LG; 3537.0

Política de privacidad

ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, República Eslovaca, registrada en el Registro Mercantil administrado por el Tribunal de Distrito de Bratislava I, Sección Sro, n.º de entrada 3586/B, número de registro de la empresa 31333532, como controlador de datos («ESET» o «Nosotros»), quiere ser transparente en cuanto al procesamiento de datos personales y la privacidad de sus clientes. Para alcanzar este objetivo, publicamos esta Política de privacidad con el único fin de informar a nuestros clientes («Usuario final» o «Usted») sobre los siguientes temas:

- Procesamiento de datos personales
- Confidencialidad de los datos

- Derechos del titular de los datos

Procesamiento de datos personales

Los servicios prestados por ESET implementados en el producto se prestan de acuerdo con los términos del Acuerdo de licencia para el usuario final ("EULA"), pero algunos pueden requerir atención específica. Queremos proporcionarle más detalles sobre la recopilación de datos relacionada con la prestación de nuestros servicios. Prestamos diferentes servicios descritos en el EULA y en la documentación de producto, como el servicio de actualización, ESET LiveGrid®, protección contra mal uso de datos, soporte, etc. Para que todo funcione, debemos recopilar la siguiente información:

- Estadísticas sobre actualizaciones y de otro tipo con información relativa al proceso de instalación y a su ordenador, lo que incluye la plataforma en la que está instalado nuestro producto e información sobre las operaciones y la funcionalidad de nuestros productos, como el sistema operativo, información sobre el hardware, identificadores de instalación, identificadores de licencias, dirección IP, dirección MAC o ajustes de configuración del producto.
- Algoritmos hash unidireccionales relativos a infiltraciones que forman parte del sistema de reputación ESET LiveGrid®, lo que mejora la eficiencia de nuestras soluciones contra malware mediante la comparación de los archivos analizados con una base de datos de elementos incluidos en listas blancas y negras disponibles en la nube.
- Muestras sospechosas y metadatos que forman parte del sistema de respuesta ESET LiveGrid®, lo que permite a ESET reaccionar inmediatamente ante las necesidades de los usuarios finales y responder a las amenazas más recientes. Dependemos de que Usted nos envíe
  - infiltraciones como posibles muestras de virus y otros programas malintencionados y sospechosos; objetos problemáticos, potencialmente no deseados o potencialmente peligrosos, como archivos ejecutables, mensajes de correo electrónico marcados por Usted como spam o marcados por nuestro producto;
  - información sobre dispositivos de la red local, como el tipo, el proveedor, el modelo o el nombre del dispositivo;
  - información relativa al uso de Internet, como dirección IP e información geográfica, paquetes de IP, URL y marcos de Ethernet;
  - archivos de volcado de memoria y la información contenida en ellos.

No deseamos recopilar sus datos más allá de este ámbito, pero en ocasiones es imposible evitarlo. Los datos recopilados accidentalmente pueden estar incluidos en malware (recopilados sin su conocimiento o aprobación) o formar parte de nombres de archivos o URL, y no pretendemos que formen parte de nuestros sistemas ni tratarlos con el objetivo declarado en esta Política de privacidad.

- La información de licencia, como el ID de licencia, y los datos personales como el nombre, los apellidos, la dirección y la dirección de correo electrónico son necesarios para la facturación, la verificación de la autenticidad de la licencia y la prestación de nuestros servicios.
- La información de contacto y los datos contenidos en sus solicitudes de soporte pueden ser necesarios para el servicio de soporte. Según el canal que elija para ponerse en contacto con nosotros, podemos recopilar datos como su dirección de correo electrónico, su número de teléfono, información sobre licencias, datos del producto y descripción de su caso de asistencia. Es posible que le pidamos que nos facilite otra información para prestar el servicio de asistencia técnica.

Confidencialidad de los datos

ESET es una empresa que opera en todo el mundo a través de filiales o socios que forman parte de su red de distribución, servicio y asistencia. La información procesada por ESET puede transferirse a y de filiales o socios para cumplir el CLUF en aspectos como la prestación de servicios, la asistencia o la facturación. Según su ubicación y el servicio que decida utilizar, podemos vernos obligados a transferir sus datos a un país para el que no exista una decisión de adecuación de la Comisión Europea. Incluso en este caso, todas las transferencias de información cumplen la legislación sobre protección de datos y solo se realizan si es necesario. Deben implementarse sin excepción las cláusulas contractuales tipo, las reglas corporativas vinculantes u otra medida de seguridad adecuada.

Hacemos todo lo posible para evitar que los datos se almacenen más tiempo del necesario durante la prestación de servicios de acuerdo con el EULA. Nuestro período de retención puede ser mayor que el período de validez de su licencia para que tenga tiempo de renovarla de forma sencilla y cómoda. Pueden continuar tratándose estadísticas y otros datos minimizados y seudonimizados de ESET LiveGrid® con fines estadísticos.

ESET implementa medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado para los posibles riesgos. Hacemos todo lo posible para garantizar en todo momento la confidencialidad, la integridad, la disponibilidad y la resiliencia de los sistemas y los servicios de tratamiento. Sin embargo, en caso de filtración de información que ponga en peligro sus derechos y libertades, estamos preparados para notificárselo a la autoridad supervisora y a los interesados. Como titular de los datos, tiene derecho a presentar una reclamación ante una autoridad supervisora.

Derechos del titular de los datos.

ESET se rige por la legislación de Eslovaquia y, al ser parte de la Unión Europea, en este país se debe cumplir la correspondiente legislación sobre protección de datos. Sin perjuicio de las condiciones establecidas por las leyes de protección de datos aplicables, en su calidad de interesado, tiene los siguientes derechos:

- derecho a solicitar a ESET acceso a sus datos personales;
- derecho de rectificación de sus datos personales en caso de que sean incorrectos (también tiene derecho a completarlos en caso de que estén incompletos);
- derecho a solicitar la eliminación de sus datos personales;
- derecho a solicitar la restricción del procesamiento de sus datos personales;
- derecho a oponerse al procesamiento;
- derecho a presentar una reclamación y
- derecho a la portabilidad de datos.

Si desea ejercer sus derechos como titular de los datos o tiene preguntas o dudas, envíenos un mensaje a:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk