ESET Endpoint Security for Android

Guía para el usuario

Haga clic aquí para mostrar la versión de ayuda de este documento

Digital Security
Progress. Protected.

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

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

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

REV. 12/04/2024

Introducción

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

ESET Endpoint Security for Android está disponible en la versión de Google Play y la versión web.

ESET Endpoint Security for Android versión 4 es compatible con:

- ESET PROTECT
- ESET PROTECT Cloud.

ESET Endpoint Security for Android está diseñado para proteger dispositivos móviles corporativos contra las últimas amenazas de malware y para asegurar sus datos, incluso si su dispositivo se pierde o si se lo roban. También ayuda a los administradores de sistemas a mantener sus dispositivos, en cumplimiento con las políticas de seguridad de la empresa.

ESET Endpoint Security for Android también puede aplicarse en pequeñas y medianas empresas sin la necesidad de una administración remota mediante ESET PROTECT. El técnico de TI, el administrador del sistema o el usuario pueden compartir su configuración de ESET Endpoint Security for Android con sus colegas. Este proceso disminuye por completo la necesidad de activar el producto y configurar cada uno de sus módulos manualmente, que de otra manera se requeriría inmediatamente después de la instalación de ESET Endpoint Security for Android.

Novedades de la versión 4

Agregado:

- Compatibilidad con Android 14.

Se mejoró

- Pequeñas mejoras visuales de la GUI de ESET Endpoint Security for Android

Versiones de ESET Endpoint Security for Android

Hay dos versiones de ESET Endpoint Security for Android disponibles:

- **ESET Endpoint Security for Android**: La versión de Google Play.
- **ESET Endpoint Security for Android**: La versión web con la función Filtro de llamadas.

Actualizaciones a la última versión

Las actualizaciones de ESET Endpoint Security for Android difieren según la versión instalada:

Actualizar la versión de Google Play de ESET Endpoint Security for Android

Si su dispositivo móvil está configurado para actualizar las aplicaciones de Google Play automáticamente, la actualización se realizará automáticamente.

Actualizar la versión web de ESET Endpoint Security for Android

Haga clic en el interruptor "Habilitar actualizaciones automáticas de aplicaciones" en ESET PROTECT Cloud o ESET PROTECT para realizar actualizaciones de aplicaciones de ESET Endpoint Security for Android. Después de eso, se le pedirá automáticamente al usuario final que actualice cada vez que haya una actualización disponible. Para obtener más información, visite nuestro artículo de la base de conocimiento.

Requisitos mínimos del sistema

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

- Sistema operativo: Android 6 (Marshmallow) y posterior
- Resolución de pantalla táctil: 480x800 píxeles
- CPU: ARM conjunto de instrucciones ARMv7, x86 Intel Atom
- Espacio libre de almacenamiento: 20 MB
- Conexión a Internet

Android Go no es compatible

No es compatible con dispositivos rooteados y Dual SIM. Algunas funciones (por ejemplo, Anti-Theft y filtro de llamadas) no están disponibles en las tabletas que no admiten llamadas y mensajes.

Registro de cambios

Usuarios que se conectan a ESET PROTECT y ESET PROTECT Cloud

ESET PROTECT y ESET PROTECT Cloud son aplicaciones que le permiten administrar los productos ESET en un entorno de red desde una ubicación central. El sistema de administración de tareas ESET PROTECT y ESET PROTECT Cloud le permite instalar las soluciones de seguridad ESET en equipos remotos y responder rápidamente a nuevos problemas y amenazas. ESET PROTECT no brinda protección contra códigos maliciosos por sí mismo. Sino que confía en la presencia de una solución de seguridad ESET en cada cliente.

Las soluciones de seguridad de ESET admiten redes que incluyen múltiples tipos de plataformas. Su red puede incluir una combinación de los sistemas operativos actuales de Microsoft, basados en Linux, macOS y de los sistemas operativos que operen en dispositivos móviles (teléfonos móviles y tabletas).

ESET PROTECT y ESET PROTECT Cloud son una nueva generación de un sistema de administración remota que difiere significativamente de las versiones anteriores de ESET Remote Administrator. Puede comprobar la compatibilidad con versiones anteriores de los productos de seguridad ESET aquí:

- Productos compatibles de ESET PROTECT
- Productos compatibles de ESET PROTECT Cloud

Puede buscar las diferencias entre ESET PROTECT y ESET PROTECT Cloud en nuestra documentación.

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

Descargue el ESET Endpoint Security for Android

Hay dos formas para descargar ESET Endpoint Security for Android:

Descargar ESET Endpoint Security for Android escaneando el código QR

Escanee el siguiente código QR con una aplicación para escanear QR en su dispositivo móvil:

Como alternativa, puede descargar el archivo APK de instalación de ESET Endpoint Security for Android desde el sitio web de ESET:

1.Descargue el archivo de instalación desde el sitio Web de ESET.

2.Abra el archivo desde el área de notificaciones de Android o ubíquelo con una aplicación de administración de navegación de archivos. El archivo se guarda, por lo general, en la carpeta Descargas.

3.Asegúrese de que las aplicaciones de Fuentes desconocidas estén permitidas en su dispositivo. Para hacerlo, toque el ícono del Iniciador en la pantalla de inicio de Android o vaya a **Inicio** > **Menú**. Toque **Configuración** > **Seguridad**. La opción **Fuentes desconocidas** debe estar habilitada.

4.Luego de abrir el archivo, toque **Instalar**.

si descargó ESET Endpoint Security for Android desde el sitio web de ESET, solo puedo realizar la actualización con un archivo descargado desde el sitio web de ESET o desde la aplicación misma. No se puede actualizar desde Google Play.

Descargar ESET Endpoint Security for Android desde Google Play

Abra la aplicación Google Play Store en su dispositivo Android y busque ESET Endpoint Security for Android (o solo ESET).

Como alternativa, para descargar el programa puede hacer clic en este enlace o escanear el código QR a continuación:

https://play.google.com/store/apps/details?id=com.eset.endpoint

Instalación remota

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

- Instalación del Mobile Device Connector
- Inscripción de dispositivos móviles

Situaciones de instalación de ESET Endpoint Security for Android

- El administrador envía por correo electrónico el enlace de inscripción, el archivo APK de instalación y un proceso de instalación a los usuarios finales. El usuario toca el enlace de inscripción y se redirige al navegador predeterminado de Internet 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 Google Play Store para que descargue la aplicación. Una vez descargada la aplicación, se sigue una 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 importa toda la configuración, y se activa la aplicación (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 dispositivos sin cámara, navegador o correo electrónico (por ejemplo, televisores, pantallas inteligentes, pantallas de publicidad, etc.) en ESET PROTECT Cloud. Para inscribir estos dispositivos, instale ESET Endpoint Security for Android en el dispositivo a través de Google Play o el archivo APK. Durante el asistente de inicio en el paso **Administración remota**, seleccione **Sí, administrar de forma remota** y toque **Dispositivo de entrada limitada**.

En ESET PROTECT Cloud:

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

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

3.Acepto el Acepto el Acuerdo de licencia de usuario final y confirmo estar de acuerdo con la Política de

privacidad.

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

5.Recibirá un enlace de inscripción para el dispositivo. Haga clic en el enlace y escriba el código de seguridad de seis dígitos que se muestra en la sección **Administración remota** del asistente de inicio.

6.Haga clic en **Aceptar**.

Se ha inscrito el dispositivo en ESET PROTECT Cloud.

Reinscripción de dispositivos

Si su dispositivo móvil ha dejado de conectarse, puede reinscribirlo por correo electrónico o código QR si tiene acceso físico al dispositivo.

> **Reinscripción de dispositivos**
> Para obtener instrucciones visuales sobre cómo reinscribir su dispositivo, lea nuestro artículo de la base de conocimientos.

Instalación local en el dispositivo

ESET Endpoint Security for Android ofrece a los administradores la opción de configurar y administrar localmente el punto de conexión si eligen no utilizar ESET PROTECT. Todas las configuraciones de la aplicación están protegidas por la contraseña del administrador, por lo que la aplicación está bajo control total en todo momento.

Si el administrador de una empresa pequeña decide no utilizar ESET PROTECT pero aún desea proteger los dispositivos corporativos y aplicar políticas de seguridad básicas, tiene dos opciones para administrar los dispositivos localmente:

1.El acceso físico a cada dispositivo de la empresa y una configuración manual de los ajustes.

2.El administrador puede preparar la configuración deseada en su dispositivo Android (con ESET Endpoint Security for Android instalado) y exportar estos ajustes a un archivo (consulte la sección Importar/Exportar configuraciones de esta guía para obtener más información). El administrador puede compartir el archivo exportado con los usuarios finales (por ejemplo, por correo electrónico); ellos pueden importar el archivo en cualquier dispositivo que ejecute ESET Endpoint Security for Android. Cuando el usuario abre y acepta el archivo de configuración recibido, se importará automáticamente toda la configuración y se activará la aplicación (siempre y cuando se haya proporcionado la información de la licencia). Todas las configuraciones estarán protegidas por la contraseña del administrador.

Asistente de inicio

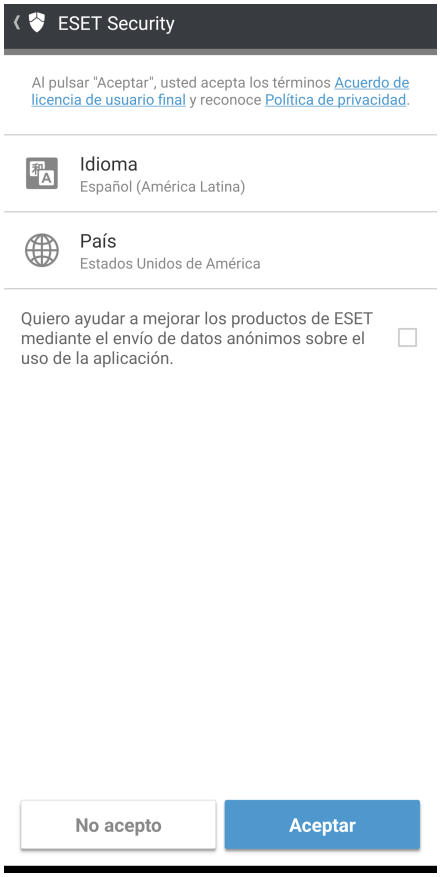
Una vez instalada la aplicación, toque **Configuración del administrador** y siga las instrucciones del asistente de inicio. Este procedimiento fue creado solo para Administradores:

1.Seleccione el **Idioma** que desea utilizar 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 con el envío de datos anónimos sobre el uso de la aplicación, marque la casilla.

4.Toque **Aceptar**. Al tocar **Aceptar**, acepta el Acuerdo de licencia del usuario final.



5.Toque **Aceptar** para aceptar 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 tocar en **No, simplemente proteger**.

7.La configuración manual requiere que los permisos del almacenamiento y del teléfono estén activados. Toque **Continuar** y luego toque **Permitir** para habilitar cada uno de los permisos.

8.Toque **Continuar** para permitir el permiso Escribir sobre otras aplicaciones.

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

10.Crear contraseña de administrador.

11.**Protección contra la desinstalación** evita que usuarios no autorizados desinstalen ESET Endpoint Security for Android. Toque **Habilitar** y, luego, toque **Activar** en la indicación **Activar la aplicación de administración de este dispositivo**.

12.Habilite Acceso de uso para el correcto funcionamiento de la aplicación. Toque **Continuar** y luego, toque ESET Endpoint Security for Android para habilitar **Acceso de uso**. Toque dos veces la flecha de retorno para volver al Asistente de inicio.

13.Seleccione la opción para **Permitir** o **No permitir** participación en el sistema de comentarios de ESET

LiveGrid. Para leer más acerca de ESET LiveGrid®, consulte esta sección.

14.Seleccione la opción de ESET Endpoint Security for Android para **Permitir detección** o **No permitir detección** de aplicaciones potencialmente no deseadas. Puede encontrar más detalles sobre dichas aplicaciones en esta sección. Toque **Siguiente**.

15.Toque **Finalizar** para salir del Asistente de inicio y comenzar la primera exploración del dispositivo.

Desinstalación

Puede desinstalar ESET Endpoint Security for Android manualmente siguiendo estos pasos:

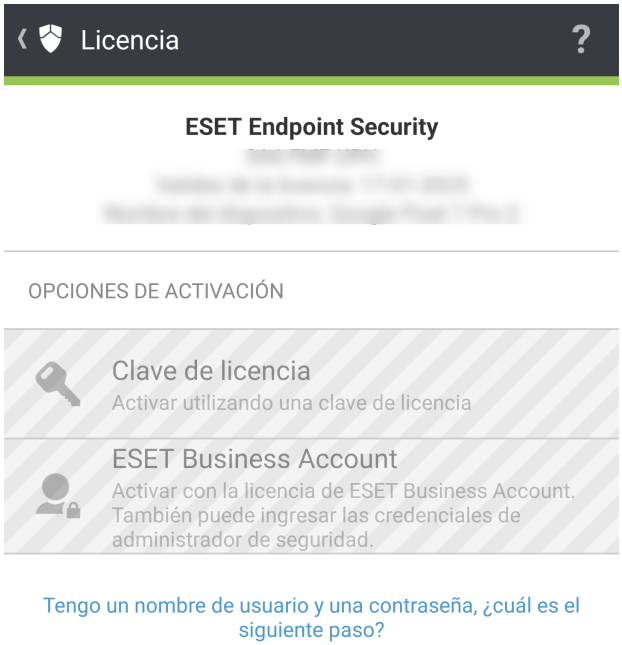
> **Importante**
> Esta guía se basa en la configuración de Android stock. El proceso de desintalación puede variar en función del fabricante del dispositivo.

1.En su dispositivo Android, abra **Configuración** > **Datos biométricos y seguridad** > **Otra configuración de seguridad** > **Aplicaciones de administración del dispositivo**. DeseleccioneESET Endpoint Security for Android y toque **Desactivar**. Toque **Desbloquear** e ingrese la Contraseña de admin. Si no ha establecido ESET Endpoint Security for Android como el Administrador del dispositivo, saltee este paso.

2.Vuelva a **Configuraciones** y toque **Aplicaciones** > **ESET Endpoint Security for Android** > **Desinstalar** > **OK**.

Activación del producto

Hay múltiples maneras para activar ESET Endpoint Security for Android. La disponibilidad de un escenario de activación particular en la ventana de activación puede variar dependiendo del país así como de los medios de distribución (CD/DVD, página Web de ESET, etc.) para su producto.



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

Puede usar cualquiera de los siguientes métodos para activar ESET Endpoint Security for Android:

- **Clave de licencia**-una cadena única en el formato XXXX-XXXX-XXXX-XXXX-XXXX que se utiliza para la identificación del propietario de la licencia y para la activación de la licencia.
- **ESET Business Account**: una cuenta creada en el portal de ESET Business Account con credenciales (dirección de correo electrónico y contraseña). Este método le permite administrar múltiples licencias desde una ubicación.

ESET PROTECT tiene la capacidad de activar dispositivos de clientes de manera silenciosa con el uso de licencias que el administrador pone a disposición.

Documentación para puntos de conexión administrados de forma remota

Los productos comerciales de ESET y ESET Endpoint Security for Android pueden administrarse de forma remota en las estaciones de trabajo de 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 de cliente pueden considerar el uso de una herramienta de administración remota de ESET. Las herramientas de administración remota de ESET pueden implementar soluciones de ESET, administrar tareas, aplicar políticas de seguridad, supervisar los estados del sistema y responder rápidamente a problemas o amenazas en equipos remotos desde una ubicación central.

Herramientas de administración remota de ESET

ESET Endpoint Security for Android puede administrarse de forma remota mediante ESET PROTECT o ESET PROTECT Cloud.

- Introducción a ESET PROTECT
- Introducción a ESET PROTECT Cloud

> **Herramienta de migración**
> La versión 3.5 y posteriores de ESET Endpoint Security for Android son compatibles con la Herramienta de migración para migrar de ESET PROTECT a ESET PROTECT Cloud.

Prácticas recomendadas

- Inscribir un dispositivo mediante ESET PROTECT
- Configure una contraseña de administración en los equipos de cliente conectados para evitar modificaciones no autorizadas
- Aplicar una política recomendada para que se cumplan las características de seguridad disponibles

Guías de procedimientos

- Cómo utilizar el modo de anulación

Inscripción de un dispositivo Android a través de Microsoft Intune

> Cuando se inscribe su dispositivo Android 9 y versiones posteriores a través de Microsoft Intune, las a versiones 3.5 y posteriores de ESET Endpoint Security for Android ignoran las siguientes configuraciones cuando se aplica la política correspondiente:
> - Seguridad del dispositivo
> - Control de la aplicación
> - Anti-Theft

Introducción a ESET PROTECT

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

Al usar la consola web de ESET PROTECT, puede implementar soluciones ESET, administrar tareas, aplicar políticas de seguridad, controlar el estado del sistema y responder rápidamente a problemas o detecciones en equipos remotos. Consulte también el resumen de elementos de arquitectura e infraestructura ESET PROTECT, Introducción a la consola web de ESET PROTECT y Entornos de aprovisionamiento de dispositivos de escritorio compatibles.

ESET PROTECT está compuesto por los siguientes componentes:

- Servidor deESET PROTECT : el servidor de ESET PROTECT se puede instalar tanto en Windows como en Linux y también viene como un Dispositivo virtual. Maneja la comunicación con los Agentes, y recoge y almacena los datos de la aplicación en la base de datos.

- Consola Web deESET PROTECT : La consola web de ESET PROTECT es la interfaz principal que le permite administrar los equipos cliente en su entorno. Muestra una visión general del estado de los clientes en su red y le permite implementar las soluciones de ESET en equipos no administrados en forma remota. Después de instalar el Servidor ESET PROTECT, puede acceder a la Consola Web mediante su navegador web. Si elige que el servidor web sea accesible desde Internet, puede usar ESET PROTECTdesde cualquier lugar y dispositivo con conexión a Internet.

- Agente ESET Management: el Agente ESET Management facilita la comunicación entre el servidor ESET PROTECT y los equipos cliente. El Agente debe estar instalado en el equipo cliente para establecer comunicación entre ese equipo y el servidor ESET PROTECT. Dado que se ubica en el equipo cliente y puede almacenar diferentes escenarios de seguridad, el uso del Agente ESET Management disminuye significativamente el tiempo de reacción frente a nuevas detecciones. Al usar la consola web de ESET PROTECT puede implementar el agente ESET Management en equipos sin gestión reconocidos por Active Directory o ESET Sensor de RD. También puede instalar manualmente el Agente ESET Management en equipos cliente, de ser necesario.

- Sensor de Rogue Detection: El Sensor de Rogue Detection (RD) de ESET PROTECT detecta equipos no administrados en su red y envía la información de dichos equipos al Servidor ESET PROTECT. Esto le permite agregar fácilmente nuevos equipos cliente a su red segura. El sensor RD recuerda los equipos que han sido detectados y no enviará la misma información dos veces.

- ESET Bridge (Proxy HTTP): puede usar ESET Bridge con ESET PROTECT como servicio proxy para:

  - Distribuir las actualizaciones a equipos clientes y paquetes de instalación para el agente ESET Management.

  - Enviar comunicación de agentes ESET Management al servidor ESET PROTECT.

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

- El aparato virtual (VA) de ESET PROTECT: La VA ESET PROTECT está destinada para los usuarios que desean ejecutar ESET PROTECT en un ambiente virtualizado.

- ESET PROTECT Host del agente virtual: Un componente del ESET PROTECT que virtualiza las entidades del

agente para permitir la administración de máquinas virtuales sin agentes. Esta solución permite la automatización, el uso de grupos dinámicos y el mismo nivel de administración de tareas que los Agente ESET Management en equipos físicos. El agente virtual recopila información de las máquinas virtuales y la envía al servidor ESET PROTECT.

- Herramienta de replicación: La herramienta de replicación es necesaria para las actualizaciones de los módulos fuera de línea. Si los equipos de su cliente no tienen conexión a Internet, puede usar la herramienta de replicación para descargar los archivos de actualización de los servidores de actualización de ESET y almacenarlos localmente.

- ESET Remote Deployment Tool: Esta herramienta le sirve para implementar paquetes todo en uno creados en la consola web de <%PRODUCT%>. Es una forma cómoda de distribuir el agente ESET Management con un producto ESET en equipos a través de una red.

- ESET Business Account: El portal de licencias para los productos comerciales de ESET le permite administrar las licencias. Consulte la sección de <%EBA%> este documento para obtener instrucciones sobre cómo activar su producto o consulte la Guía del usuario de <%EBA%>*** para obtener más información sobre cómo usar <%EBA%>.

- ESET Enterprise Inspector: un sistema integral de detección y respuesta de punto de conexión que incluye características como: detección de incidentes, administración y respuesta ante incidentes, recolección de datos, indicadores de detección de riesgos potenciales, detección de anomalías, detección de comportamiento e incumplimientos de políticas.

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

Para obtener más información, consulte la Guía para el usuario en línea de ESET PROTECT.

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 el requisito de tener que contar con un servidor físico o virtual, como ESET PROTECT. Con la consola web ESET PROTECT Cloud, puede implementar soluciones ESET, administrar tareas, aplicar políticas de seguridad, supervisar el estado del sistema y responder rápidamente a problemas o amenazas en equipos remotos.

- Lea más al respecto en la Guía para el usuario en línea de ESET PROTECT Cloud.

Políticas

El administrador puede enviar configuraciones específicas a productos ESET que se ejecutan en los dispositivos de clientes mediante políticas de la Consola web de ESET PROTECT. Una política se puede aplicar directamente a dispositivos individuales o grupos de dispositivos. También puede asignar varias políticas a un dispositivo o grupo.

Un usuario debe tener los siguientes permisos para crear una nueva política: Permiso de **Lectura** para leer la lista de políticas, Permiso de **Uso** para asignar políticas a los equipos de destino y Permiso de **Escritura** para crear, modificar o editar políticas.

Las políticas se aplican en el orden en que se organizan los Grupos estáticos. Esto no es cierto en el caso de los Grupos dinámicos, donde las políticas se aplican primero a los Grupos dinámicos más recientes. Esto le permite aplicar políticas con mayor impacto en la parte superior del árbol de grupos y aplicar políticas más específicas a los subgrupos. Al usar indicadores un usuario de ESET Endpoint Security for Android con acceso a grupos que se encuentran en la parte superior del árbol puede anular las políticas de los grupos inferiores. Este algoritmo se explica en Ayuda en línea del ESET PROTECT.

La configuración de las políticas en el dispositivo desactiva la opción de cambiar la configuración controlada por políticas a nivel local. Estos ajustes se bloquean contra cambios incluso en el modo de Administrador. Puede permitir que se realicen cambios temporales mediante la creación de una política de Modo de anulación.

Para configurar determinadas políticas, puede que deba conceder permisos adicionales a ESET Endpoint Security for Android a nivel local en el dispositivo afectado.

Recomendamos que asigne políticas más genéricas (por ejemplo, la política del servidor de actualización) a los grupos que se ubiquen en la parte superior del árbol de grupos. Las políticas más específicas (por ejemplo, la configuración del control de dispositivos) se deben asignar al grupo que se ubique en la parte inferior del árbol grupos. Las políticas inferiores suelen reemplazar las configuraciones de las superiores cuando se combinan (a menos que se defina lo contrario con indicadores de políticas).

Políticas predeterminadas para ESET Endpoint Security for Android

Nombre de la política	Descripción de la política
General - Protección máxima	ESET Endpoint Security for Android usa todas las opciones para garantizar la máxima protección del dispositivo.
General - Configuración balanceada	ESET Endpoint Security for Android usa la configuración recomendada para la mayoría de los ajustes.
General - Rendimiento máximo	ESET Endpoint Security for Android combina protección contra amenazas y un impacto mínimo en las tareas diarias y el rendimiento del dispositivo.

Aplicar políticas

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

Hay varias políticas incorporadas para ESET Endpoint Security for Android:

Nombre de la política	Descripción de la política
General - Protección máxima	ESET Endpoint Security for Android usa todas las opciones para garantizar la máxima protección del dispositivo.
General - Configuración balanceada	ESET Endpoint Security for Android usa la configuración recomendada para la mayoría de los ajustes.
General - Rendimiento máximo	ESET Endpoint Security for Android combina protección contra amenazas y un impacto mínimo en las tareas diarias y el rendimiento del dispositivo.

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

- ESET PROTECT políticas

- ESET PROTECT Cloud políticas
- Aplique una política recomendada o predefinida para ESET Endpoint Security for Android mediante ESET PROTECT

Indicadores

Las políticas que se aplican a un equipo cliente suelen ser el resultado de varias políticas que se fusionan en una política final. Al fusionar políticas, puedes ajustar el comportamiento deseado de la política final, debido al orden de las políticas aplicadas, con el uso de indicadores de política. Los indicadores definen cómo la política manejará una configuración específica.

Para cada configuración, puede seleccionar uno de los siguientes indicadores:

No corresponde	Cualquier configuración que tenga este indicador no está establecida por la política. Dado que la política no establece la configuración, se puede cambiar por otras políticas aplicadas posteriormente.
Aplicar	La configuración con el indicador **Aplicar** se aplicará al equipo cliente. Sin embargo, al fusionar políticas, se pueden sobrescribir con otras políticas aplicadas posteriormente. Cuando se envía una política a un equipo cliente que contiene configuraciones marcadas con este indicador, dichas configuraciones cambiarán la configuración local del equipo cliente. Dado que la configuración no es forzada, todavía se puede modificar mediante otras políticas aplicadas posteriormente.
Forzar	Las configuraciones con el indicador **Forzar** tienen prioridad y no se pueden sobrescribir con ninguna política aplicada posteriormente (incluso si también tiene un indicador de **Forzar**). Esto asegura que otras políticas aplicadas posteriormente no podrán cambiar esta configuración durante la fusión. Cuando se envía una política a un equipo cliente que contiene configuraciones marcadas con este indicador, dichas configuraciones cambiarán la configuración local del equipo cliente.

Escenario: El *Administrador* desea permitir al usuario *John* crear o editar políticas en su grupo hogar y ver todas las políticas creadas por el*Administrador* incluyendo las Políticas que tienen indicadores de Forzar. El *Administrador* quiere permitirle a *John* ver todas las políticas, pero que no pueda editar políticas ya existentes creadas por el *Administrador*. *John* solo puede crear o editar políticas dentro de su Grupo hogar, San Diego.
ResoluciónEl *Administrador* tiene que seguir estos pasos:
Crear grupos estáticos personalizados y conjuntos de permisos
1. Crear un nuevo Grupo estático llamado *San Diego*.
2. Crear un nuevo Conjunto de permisos llamado *Todas las Políticas -John* con acceso al grupo estático *Todos* y permisos de **Lectura** para **Políticas**.
3. Crear un nuevo Conjunto de permisos llamado *Política John* con acceso al grupo estático *San Diego*, con acceso a funcionalidad y permiso de **Escritura** para **Grupo y equipos** y **Políticas**. Este conjunto de permisos permite a *John* crear o editar políticas en su Grupo hogar, *San Diego*.
4. Crear un nuevo usuario para *John* y, en la sección **Conjunto de permisos**, seleccionar *Todas las Políticas - John* y *Política John*.
Crear políticas
5. Crear una nueva política *Todos - Habilitar Firewall*, expandir la sección **Configuración**, seleccionar **ESET Endpoint para Windows**, ir a **Firewall personal** > **Básico** y aplicar todas las configuraciones mediante un indicador **Forzar**. Expandir la sección **Asignar** y seleccionar el Grupo estático *Todos*.
6. Crear una nueva política *Grupo de John- Habilitar Firewall*, expandir la sección **Configuración**, seleccionar **ESET Endpoint para Windows**, ir a **Firewall personal** > **Básico** y aplicar todas las configuraciones mediante un indicador **Aplicar**. Expandir la sección **Asignar** y seleccionar el Grupo estático *San Diego*.
Resultado
Las Políticas creadas por el *Administrador* se aplicarán en primer lugar desde que se aplicaron los indicadores de **Forzar** a la configuración de las políticas. La configuración con el indicador de Forzar aplicado tienen prioridad y no se pueden sobrescribir con otra política aplicada posteriormente. Las políticas creadas por el usuario *John* se aplicarán después de las políticas creadas por el Administrador. Para ver el orden final de las políticas, vaya a **Más** > **Grupos** > **San Diego**. Seleccione el equipo y seleccione **Mostrar detalles**. En la sección de **Configuración**, haga clic en **Políticas aplicadas**.

Usar Modo de anulación

Los usuarios con ESET Endpoint Security for Android (versión 2.1 y posteriores) instalado en sus máquinas pueden usar la característica de Anulación. El modo de anulación permite a los usuarios, a nivel de dispositivo de cliente, cambiar la configuración del producto ESET instalado durante un período definido, incluso si hay una política aplicada a dicha característica. Una vez transcurrido el período establecido, la configuración volverá a la configuración definida por las políticas.

De acuerdo a la configuración predeterminada de políticas, ESET Endpoint Security for Android explora el dispositivo una vez finalizada la sesión de anulación. Puede cambiar esto con **Explorar el dispositivo tras una sesión de anulación**.

- Para cambiar la configuración en el dispositivo a nivel local mientras está en el modo de anulación, debe escribir la contraseña de administrador de ESET Endpoint Security for Android.
- No se puede detener el modo de anulación desde la consola web de ESET una vez que se habilitó. El modo de anulación se deshabilitará automáticamente cuando venza el período de anulación.
- El usuario que usa 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**, ingrese un **Nombre** y una **Descripción** para la política.

3.En la sección **Configuración**, seleccione **ESET Endpoint Security for Android**.

4.En las opciones de política, haga clic en **Configuración**.

5.Expanda la **configuración del modo de anulación** y configure reglas para el modo de anulación.

6.En la sección **Asignar**, seleccione los dispositivos correspondientes.

7.Repase la configuración en el sección **Resumen** y haga clic en Finalizar.

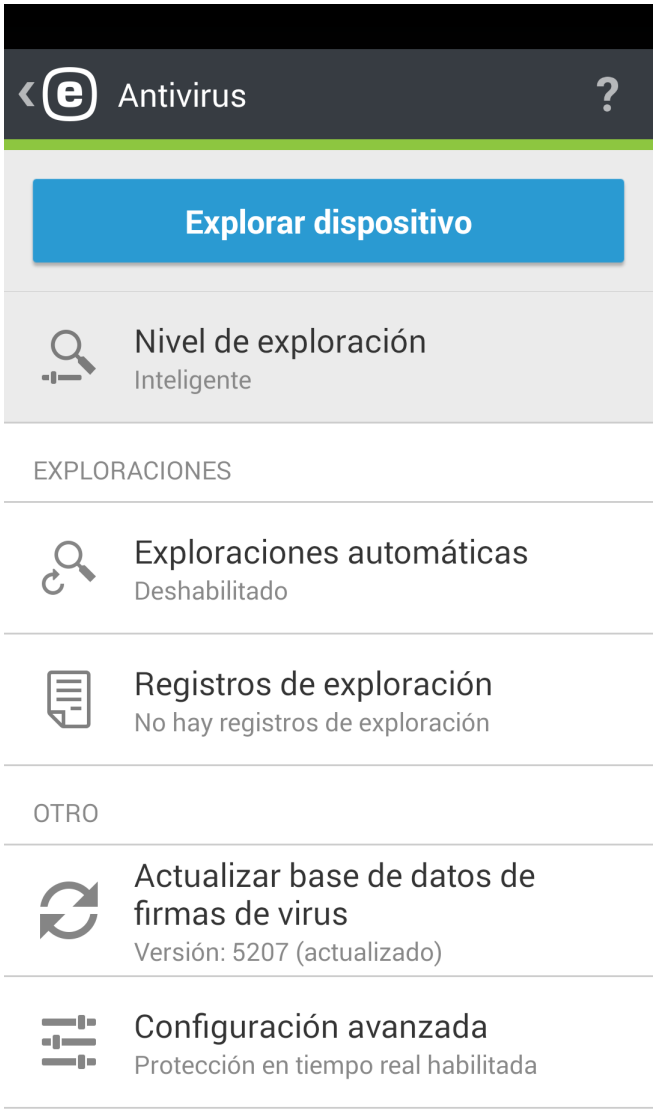
Si *John* tiene un problema con la configuración de su punto de conexión porque bloquea alguna funcionalidad importante o el acceso a la web en su dispositivo, el Administrador puede permitir que *John* anule la política existente de su punto de conexión y que corrija la configuración manualmente en su dispositivo. Luego, es posible que ESET PROTECT Cloud solicite estos ajustes para que el Administrador pueda crear una nueva política de ellos.
Para hacerlo, siga los siguientes 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 política.
4.Amplíe la configuración del **Modo de anulación** y active el modo de anulación durante una hora.
5.Haga clic en **Definir** 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 a el *teléfono inteligente de John* y haga clic en **Finalizar** para guardar la política.
7.*John* debe ingresar la contraseña de administrador para activar el **modo de anulación** en su ESET Endpoint Security for Android y cambiar los ajustes en forma manual en su dispositivo.
8.En la consola web de ESET PROTECT Cloud, navegue a **Equipos**, seleccione el *smartphone de John* y haga clic en **Mostrar detalles**.
9.Para programar una tarea de cliente para obtener la configuración de cliente, en la sección **Configuración**, haga clic en **Solicitar configuración**.
10.Aparece la nueva configuración. Seleccione el producto aplicable y, a continuación, haga clic en **Abrir configuración**.
11.Revise la configuración y, luego, haga clic en **Convertir a política**.
12.Complete los campos **Nombre** y **Descripción**.
13.En la sección **Configuración**, modifique la configuración, de ser necesario.
14.En la sección **Asignar**, asigne esta política al *smartphone de John* (u otros).
15.Haga clic en **Terminar**. No olvide quitar la política de anulación una vez que ya no la necesite.

Anular contraseña

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 **Definir** junto a la política para introducir la contraseña de anulación.

Antivirus

El módulo Antivirus asegura el dispositivo contra códigos maliciosos mediante el bloqueo de amenazas y su posterior limpieza o envío a cuarentena.



Explorar dispositivo

Explorar dispositivo puede ser utilizado para verificar infiltraciones en el dispositivo.

Algunos tipos de archivos predefinidos se analizan en forma predeterminada. Una exploración completa del dispositivo verifica la memoria, los procesos en ejecución y sus bibliotecas de vínculos dinámicos dependientes, como también los archivos que son una parte del almacenamiento interno y extraíble. Se guardará un resumen breve de la exploración en un archivo de registro disponible en la sección “Registros de la exploración”.

Si desea abortar una exploración en progreso, toque el icono .

Nivel de exploración

Existen 2 niveles distintos de exploración para seleccionar:

- **Inteligente**: la exploración inteligente explorará las aplicaciones instaladas, archivos DEX (archivos ejecutables para Android OS), archivos SO (bibliotecas) y archivos ZIP con una profundidad máxima de exploración de 3 archivos anidados y contenido de tarjeta SD.

- **Profunda**: todos los tipos de archivos, independientemente de su extensión, serán explorados tanto en la memoria interna como en la tarjeta SD.

Exploraciones automáticas

Además de la exploración del dispositivo bajo demanda, ESET Endpoint Security for Android también ofrece exploraciones automáticas. Para obtener más información sobre la utilización de la Exploración en cargador y la Exploración programada, lea esta sección.

Registros de la exploración

La sección “Registros de la exploración” contiene los datos detallados de las exploraciones completadas en forma de archivos de registro. Consulte la sección Registros de exploraciones del antivirus de este documento para obtener más información.

Actualización de los módulos de detección

De manera predeterminada, ESET Endpoint Security for Android incluye una tarea de actualización para asegurar que el programa sea actualizado regularmente. Para ejecutar la actualización manualmente, toque **Actualizar módulos de detección**.

> Para evitar el uso innecesario de ancho de banda, las actualizaciones se envían según corresponda cuando se agrega una nueva amenaza. A pesar de que las actualizaciones son gratuitas con la licencia activa, es posible que el prestador de servicios móviles le cobre por la transferencia de datos.

Se pueden encontrar descripciones detalladas de las configuraciones Avanzadas del Antivirus en la sección Configuraciones avanzadas de este documento.

Exploraciones automáticas

Nivel de exploración

Existen 2 niveles distintos de exploración para seleccionar. Esta configuración se aplicará a la Exploración en cargador y a la Exploración programada:

- **Inteligente**: la exploración inteligente explorará las aplicaciones instaladas, archivos DEX (archivos ejecutables para Android OS), archivos SO (bibliotecas) y archivos ZIP con una profundidad máxima de exploración de 3 archivos anidados y contenido de tarjeta SD.
- **Profunda**: todos los tipos de archivos, independientemente de su extensión, serán explorados tanto en la memoria interna como en la tarjeta SD.

Exploración en cargador

Cuando se selecciona, se iniciará la exploración de manera automática cuando el dispositivo está en estado inactivo (completamente cargado y conectado a un cargador).

Exploración programada

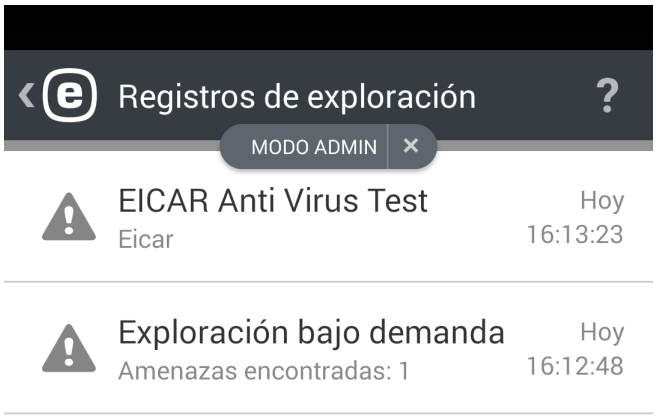
La Exploración programada le permite ejecutar una exploración de dispositivo automáticamente en un momento predefinido. Para programar una exploración, toque  junto a **Exploración programada** y especifique las fechas y horarios para el inicio de la exploración. De manera predeterminada, se selecciona el lunes a las 4 de la mañana.

Registros de la exploración

Los Registros de la exploración se crean después de cada Exploración programada o de una exploración ejecutada de manera manual.

Cada registro contiene:

- la fecha y la hora del suceso
- la duración de la exploración
- la cantidad de objetos explorados
- el resultado o los errores encontrados durante la exploración



Ignorar reglas

Si administra ESET Endpoint Security for Android de manera remota desde ESET PROTECT, tiene la opción de definir los archivos que no serán informados como maliciosos. Los archivos agregados a **Ignorar reglas** serán

ignorados en las exploraciones futuras. Para crear una regla, debe especificar lo siguiente:

- un nombre de archivo con una extensión "apk" adecuada
- un nombre del paquete de la aplicación, por ejemplo, uk.co.extorian.EICARAntiVirusTest
- el nombre de la amenaza según la detectaron los programas antivirus, por ejemplo Android/MobileTX.A (este campo es obligatorio)

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

Configuración avanzada

Protección en tiempo real

Esta opción le permite activar y desactivar el explorador en tiempo real. Este explorador se ejecuta automáticamente con el inicio del sistema y explora los archivos con los cuales usted interactúa. Explora automáticamente la carpeta de Descargas, los archivos de instalación APK y todos los archivos en la tarjeta SD una vez montada.

Sistema de reputación de ESET LiveGrid®

ESET LiveGrid® es un sistema preventivo diseñado para proporcionar seguridad adicional a su dispositivo. Monitorea constantemente los procesos y programas en ejecución del sistema contra la última inteligencia recopilada de millones de usuarios de a nivel mundial. Esto nos permite ofrecer una protección proactiva y una velocidad de exploración más precisas y optimizadas a todos los usuarios de ESET. Recomendamos que habilite esta función. Recomendamos que habilite esta función.

Sistema de comentarios de ESET LiveGrid®

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

Detectar aplicaciones potencialmente no deseadas

Una aplicación no deseada es un programa que contiene adware, instala barras de herramientas, rastrea los resultados de búsquedas o tiene otros objetivos que no son claros. En algunas situaciones, puede pensar que los beneficios de la aplicación no deseada superan los riesgos. Por este motivo, ESET les asigna a estas aplicaciones una categoría de bajo riesgo en comparación con otros tipos de software malicioso.

Detectar aplicaciones potencialmente no seguras

Existen muchas aplicaciones legítimas diseñadas para simplificar la administración de dispositivos en red. Sin embargo, en manos equivocadas, pueden ser utilizados con propósitos maliciosos. La opción Detectar aplicaciones potencialmente no seguras le permite supervisar y bloquear estas aplicaciones.*Aplicaciones potencialmente no seguras* es la clasificación usada para programas comerciales y legítimos. Esta clasificación incluye herramientas de acceso remoto, aplicaciones para adivinar las contraseñas y registradores de pulsaciones.

Bloquear amenazas no resueltas

Esta configuración determina la acción a realizarse una vez finalizada la exploración y encontradas las amenazas.

Si activa esta opción, ESET Endpoint Security for Android bloqueará el acceso a los archivos categorizados como amenazas.

Medios extraíbles

Puede elegir la acción luego de que el medio extraíble se inserta en el dispositivo:

- **Explorar siempre**: los medios extraíbles se explorarán siempre.
- **No explorar**: los medios extraíbles no se explorarán.
- **Mostrarme opciones**: la opción para explorar un medio extraíble se mostrará luego de insertar el medio.

Actualizaciones de bases de datos de módulos de detección

Esta opción le permite establecer el intervalo de tiempo para la frecuencia en que se descargan automáticamente las actualizaciones de la base de datos de amenazas. Estas actualizaciones se envían según corresponda cuando se agrega una nueva amenaza a la base de datos. Recomendamos que deje esta opción en el valor predeterminado (Todos los días).

Personalizar la antigüedad máxima para la base de datos

Esta configuración define el tiempo entre las actualizaciones de la base de datos de amenazas tras el cual se le notificará actualizar ESET Endpoint Security for Android.

Actualizar servidor

Con esta opción, puede seleccionar actualizar el dispositivo desde el **Servidor de prueba**. Las actualizaciones previas a su lanzamiento se han sometido a pruebas internas y estarán disponibles al público en general en breve. Puede beneficiarse de la habilitación de las actualizaciones previas al lanzamiento mediante el acceso a las soluciones y los métodos de detección más recientes. Sin embargo, es posible que las actualizaciones previas a su lanzamiento no sean estables todo el tiempo. La lista de módulos actuales se puede encontrar en la sección **Acerca de**: toque el ícono Menú  en la pantalla principal de ESET Endpoint Security for Android y toque **Acerca de** > **ESET Endpoint Security for Android**. Se recomienda que los usuarios sin experiencia dejen la opción **Servidor de lanzamiento** seleccionada, como aparece en forma predeterminada.

ESET Endpoint Security for Android le permite crear copias de archivos de actualización que se pueden usar para actualizar otros dispositivos en la red. El uso de un Mirror local (una copia de los archivos de actualización en el entorno de la LAN) es conveniente debido a que los archivos de actualización no necesitan descargarse desde el servidor de actualización del proveedor reiteradamente por cada dispositivo móvil. Puede encontrar información detallada acerca de cómo configurar el servidor mirror con productos ESET Endpoint para Windows en este documento.

Anti-Theft

La función Anti-Theft protege a su dispositivo móvil frente a accesos no autorizados.

Si pierde su dispositivo o alguien se lo roba y reemplaza la tarjeta SIM por una nueva (no confiable), ESET Endpoint Security for Android bloqueará el dispositivo automáticamente y se enviará un SMS de alerta a los números de teléfono definidos por el usuario. En el mensaje se incluirá el número telefónico de la tarjeta SIM insertada, el código IMSI (Identidad Internacional del Abonado a un Móvil, por sus siglas en inglés) de la tarjeta y

el código IMEI (Identidad Internacional del Equipo Móvil, por sus siglas en inglés) del teléfono. El usuario no autorizado no tendrá conocimiento de que se envió este mensaje, ya que se eliminará automáticamente de la cadena de mensajes de su dispositivo. También puede solicitar las coordenadas GPS del dispositivo móvil perdido o eliminar en forma remota todos los datos almacenados en este.

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

Las características de Anti-Theft ayudan a los administradores a proteger y localizar un dispositivo perdido. Las acciones se pueden desencadenar desde ESET PROTECT.

Al ejecutar comandos desde ESET PROTECT, el administrador recibe una confirmación en ESET PROTECT.

AL recibir la información de la ubicación (comando **Encontrar**), el administrador que usa ESET PROTECT recibe la información de la ubicación en forma de coordenadas de GPS.

Todos los comandos de Anti-Theft también pueden ser realizados desde ESET PROTECT. La nueva funcionalidad de administración de dispositivos móviles permite que los administradores realicen comandos Anti-Theft con unos pocos clics. Las tareas se envían inmediatamente para su ejecución a través un nuevo componente de procesamiento de comandos de empuje (Mobile Device Connector) que ahora es parte de la infraestructura de ESET PROTECT.

Contactos del administrador

Esta es la Lista de los números de teléfono del administrador protegidos por la contraseña de admin. Estos números también se usan para las notificaciones relacionadas con las acciones de Anti-Theft.

Cómo agregar contactos del administrador

Se deben ingresar un nombre de administrador y el número de teléfono durante el asistente de inicio de Anti-Theft. Si el contacto contiene más de un número de teléfono, todos los números asociados serán tomados en cuenta.

Los contactos de admin pueden ser agregados en la sección **Anti-Theft** > **Contactos de admin**.

Información de la pantalla de bloqueo

El administrador puede definir la información personalizada (nombre de la compañía, dirección de correo electrónico, mensaje) que se mostrará cuando el dispositivo esté bloqueado, con la opción de llamar a uno de los contactos predefinidos por admin.

Esta información incluye:

- Nombre de la empresa (opcional)
- Dirección de correo electrónico (opcional)
- Un mensaje personalizado

Tarjetas SIM de confianza

La sección **SIM de confianza** muestra la lista de tarjetas SIM de confianza que serán aceptadas por ESET Endpoint Security for Android. Si inserta una tarjeta SIM que no se encuentra definida en esta lista, se bloqueará la pantalla y se enviará un SMS de alerta al administrador.

Para agregar una tarjeta SIM nueva, toque el icono ➕. Ingrese un **Nombre** para la tarjeta SIM (por ejemplo, Hogar, Trabajo) y su número de IMSI (International Mobile Subscriber Identity). IMSI generalmente se presenta como un número de 15 dígitos impreso en la tarjeta SIM. En algunos casos, puede ser más corto.

Para eliminar una tarjeta SIM de la lista, pulse y mantenga la entrada, y luego toque el icono 🗑.

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

La característica de SIM de confianza no está disponible en dispositivos CDMA, WCDMA y solo con WiFi.

Comandos remotos

Los comandos remotos se pueden activar directamente desde la ESET PROTECT consola:

Buscar dispositivo

Recibirá un mensaje de texto con las coordenadas de GPS del dispositivo de destino, incluido un vínculo a dicha ubicación en Google Maps. Si hay una ubicación más precisa disponible luego de 10 minutos, el dispositivo enviará un nuevo SMS.

Bloquear dispositivo

Esto bloqueará el dispositivo. Podrá desbloquearlo con la contraseña del Administrador o con el comando remoto Desbloquear.

Desbloquear dispositivo bloqueado

El dispositivo se desbloqueará y se guardará la tarjeta SIM actual en el dispositivo como SIM de confianza.

Sonido de sirena/modo extraviado

El dispositivo se bloqueará y reproducirá un sonido muy fuerte durante 5 minutos (o hasta que se lo desbloquee). Una sirena muy fuerte comenzará a sonar, incluso si el dispositivo se encuentra en silencio.

Restablecimiento de fábrica mejorado

Reiniciará el dispositivo a su configuración predeterminada de fábrica. Se borrarán todos los datos accesibles y se eliminarán los encabezados de archivos. El proceso puede demorar unos minutos.

Control de aplicaciones

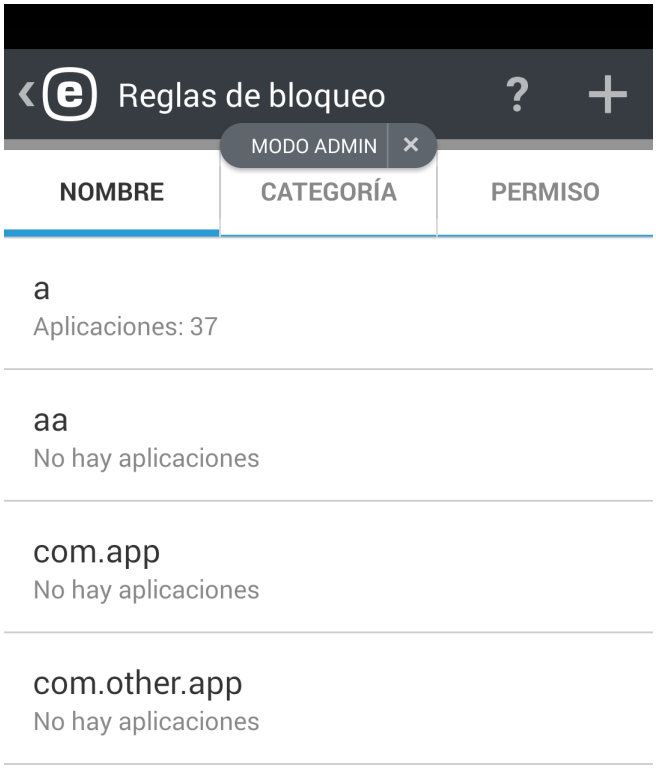
La característica **Control de aplicaciones** le ofrece a los administradores la opción de monitorear las aplicaciones instaladas, bloquear el acceso a aplicaciones definidas y reducir el riesgo de exposición instando a los usuarios a desinstalar determinadas aplicaciones. El administrador puede seleccionar entre varios métodos de filtración de aplicaciones:

- Definir manualmente las aplicaciones que deben ser bloqueadas
- Bloqueo según categoría (por ejemplo, juegos o social)
- Bloqueo según permisos (por ejemplo, aplicaciones que rastrean la ubicación)
- Bloquear por fuente (por ejemplo, aplicaciones instaladas desde fuentes que no sean de la tiendaGoogle Play)

Reglas de bloqueo

En la sección **Control de aplicaciones** > **Bloqueo** > **Reglas de bloqueo**, puede crear las reglas de bloqueo de la aplicación según los siguientes criterios:

- nombre de la aplicación o nombre del paquete
- categoría
- permisos



Bloquear aplicación

Bloqueo mediante nombre de la aplicación

ESET Endpoint Security for Android le otorga al administrador la opción de bloquear una aplicación según su nombre o el nombre del paquete. La sección**Reglas de bloqueo** proporciona una visión general de las reglas creadas y la lista de las aplicaciones bloqueadas.

Para modificar una regla existente, toque y mantenga la regla y luego pulse **Editar** . Para quitar algunas entradas de reglas de la lista, toque y mantenga una de las entradas, seleccione las que desea quitar y pulse **Quitar** . Para borrar la lista completa, pulse **SELECCIONAR TODO** y luego pulse Quitar .

Cuando bloquea una aplicación por nombre, ESET Endpoint Security for Android buscará la coincidencia exacta con un nombre de la aplicación iniciada. Si cambia la interfaz gráfica del usuario de ESET Endpoint Security for Android a un idioma diferente, debe volver a ingresar el nombre de la aplicación en ese idioma para continuar bloqueándola.

Para evitar cualquier problema con los nombres de las aplicaciones localizadas, recomendamos que bloquee dichas aplicaciones por los nombres de los paquetes: un identificador de aplicaciones único que no puede cambiarse durante el tiempo de ejecución o reutilizarse por otra aplicación.

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

Cómo bloquear una aplicación mediante su nombre

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

2.Elija si desea bloquear la aplicación de acuerdo a su nombre o al nombre del paquete.

3.Introduzca las palabras en base a las cuales se bloqueará la aplicación. Para dividir palabras múltiples, utilice una coma (,) como delimitador.

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

Bloqueo mediante la categoría de la aplicación

ESET Endpoint Security for Android otorga al admin. la opción de bloquear la aplicación de acuerdo a las categorías de aplicaciones predefinidas. La sección **Reglas de bloqueo** le proporciona una visión general de las reglas creadas y la lista de las aplicaciones bloqueadas.

Si desea modificar una regla existente, toque y mantenga presionada la regla y haga clic en **Editar**  .

Para quitar algunas entradas de reglas de la lista, toque y mantenga presionada una de las entradas, seleccione las que desea quitar y haga clic en **Quitar**  . Para borrar la lista completa, haga clic en **SELECCIONAR TODO**.

Cómo bloquear una aplicación en base a su categoría

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

2.Seleccione las categorías predefinidas a través de las casillas de verificación y toque **Bloquear**.

Bloqueo mediante los permisos de la aplicación

ESET Endpoint Security for Android otorga al administrador la opción de bloquear la aplicación de acuerdo a sus permisos. La sección **Reglas de bloqueo** le proporciona una visión general de las reglas creadas y la lista de las aplicaciones bloqueadas.

Si desea modificar una regla existente, toque y mantenga presionada la regla y haga clic en **Editar**  .

Para quitar algunas entradas de reglas de la lista, toque y mantenga presionada una de las entradas, seleccione las que desea quitar y haga clic en **Quitar**  . Para borrar la lista completa, haga clic en **SELECCIONAR TODO**.

Cómo bloquear una aplicación mediante sus permisos

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

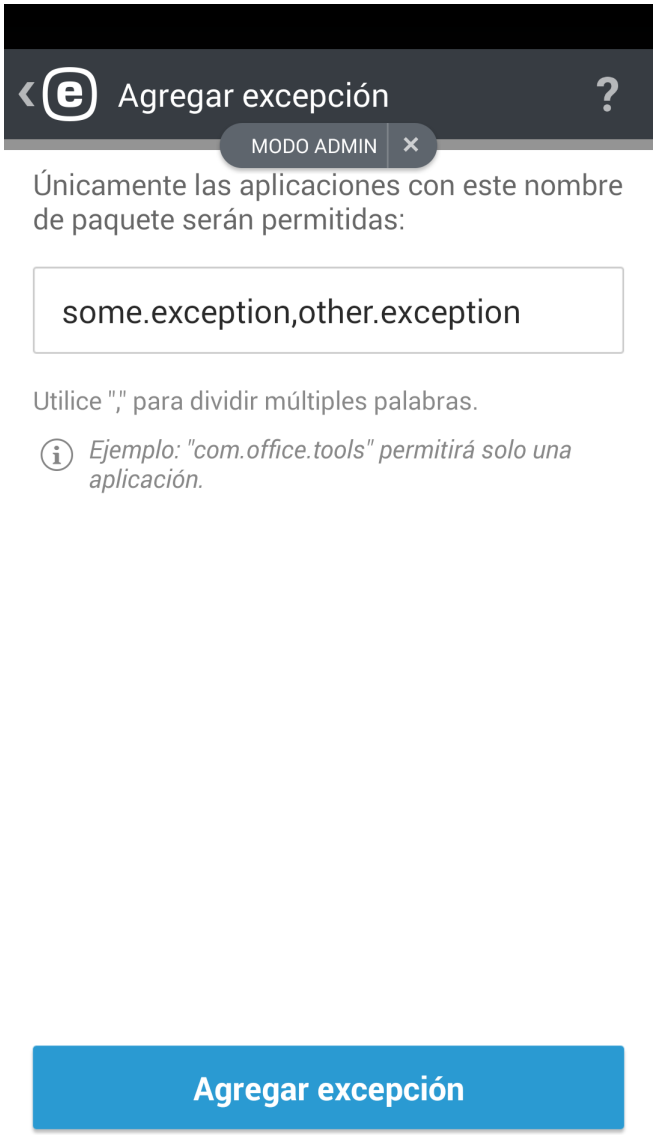
2.Seleccione los permisos a través de las casillas de verificación y toque **Bloquear**.

Bloquear fuentes desconocidas

De forma predeterminada, ESET Endpoint Security for Android no bloquea las aplicaciones obtenidas de internet o cualquier otra fuente que no sea la tienda Google Play. La sección **Aplicaciones bloqueadas** le proporciona una visión general de las aplicaciones bloqueadas (nombre del paquete, regla aplicada) y la opción de desinstalar la aplicación o de agregarla a la lista blanca en la sección **Excepciones**.

Excepciones

Toque **Control de aplicaciones** > **Bloqueo** > **Excepciones** > **Agregar excepción** y podrá crear excepciones para excluir una aplicación específica de la lista de aplicaciones bloqueadas. Los administradores con gestión ESET Endpoint Security for Android remota pueden usar esta característica nueva para determinar si un dispositivo particular cumple con la política de la empresa sobre las aplicaciones instaladas.



Cómo agregar excepciones

Además de agregar la nueva excepción (ingresando el nombre del paquete de la aplicación), también se pueden agregar las aplicaciones a la lista blanca al excluirlas de la lista de **Aplicaciones bloqueadas**:

1. En su aplicación ESET Endpoint Security for Android, toque **Control de aplicaciones**.

2. Toque **Bloquo** > **Aplicaciones bloqueadas**.

3. Seleccione la aplicación que desee agregar a la lista blanca.

4. Toque el ícono de los tres puntos en la esquina superior derecha y, a continuación, toque **Agregar excepción**.

5. Ingrese la contraseña de admin y toque **Intro**.

Aplicaciones requeridas

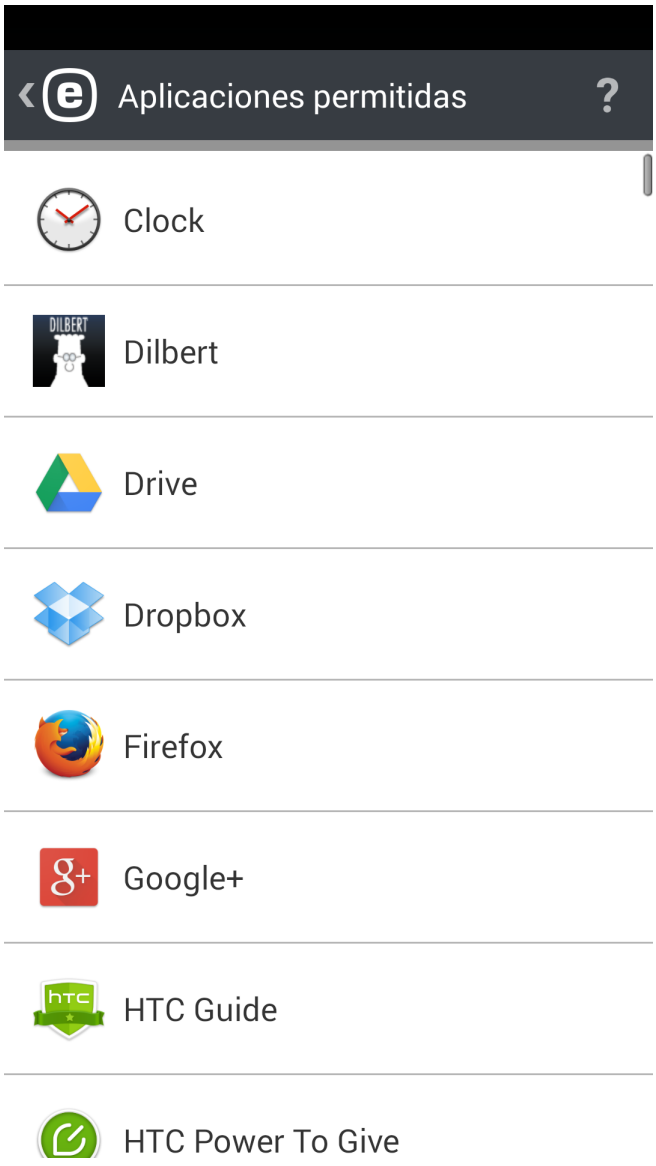
Si administra ESET Endpoint Security for Android de manera remota desde ESET PROTECT, tiene la opción de definir qué aplicaciones deben ser instaladas en los dispositivos de destino. La siguiente información es necesaria:

- nombre de la aplicación visible para el usuario
- nombre único del paquete de la aplicación, por ejemplo, *com.eset.ems2.gp*
- URL donde el usuario puede encontrar un enlace de descarga. También puede utilizar los enlaces de Google Play, por ejemplo, https://play.google.com/store/apps/details?id=com.eset.ems2.gp

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

Aplicaciones permitidas

Esta sección le proporciona una visión general de las aplicaciones instaladas que no están bloqueadas por reglas de bloqueo.

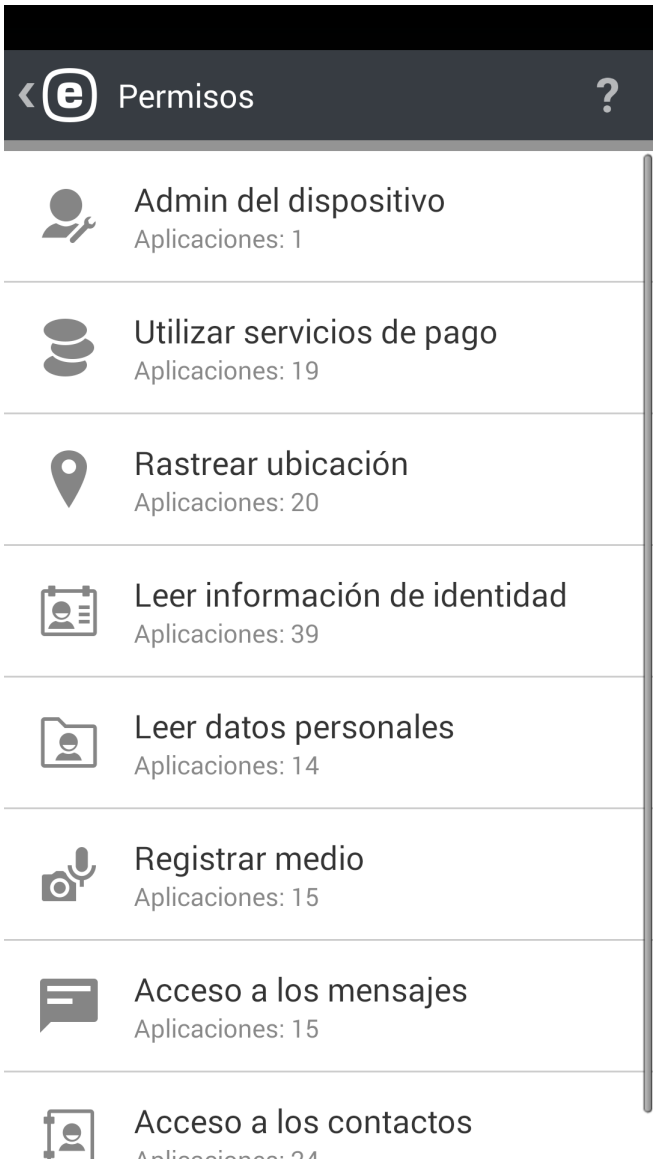


Permisos

Esta característica rastrea el comportamiento de las aplicaciones con acceso a los datos personales o de la empresa, y le permite al administrador monitorear el acceso de las aplicaciones en base a categorías predefinidas de permisos.

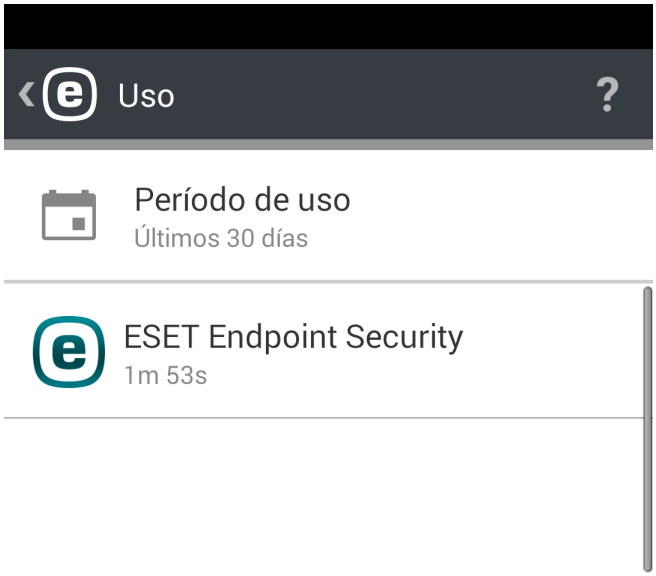
Es posible que algunas aplicaciones instaladas en su dispositivo tengan acceso a servicios que le cuestan dinero, rastrean su ubicación o leen su información de identidad, contactos o mensajes de texto. ESET Endpoint Security for Android proporciona una auditoría de estas aplicaciones.

En esta sección, puede ver la lista de aplicaciones clasificadas por categorías. Toque cada categoría para ver su descripción detallada. Se puede acceder a los detalles de los permisos de cada aplicación al tocar la aplicación específica.



Uso

En esta sección, el administrador puede controlar la cantidad de tiempo que un usuario utiliza para usar las aplicaciones específicas. Para filtrar la vista general por el período de uso, utilice la opción **Intervalo**.



Seguridad del dispositivo

La seguridad del dispositivo le brinda a los administradores las opciones para realizar lo siguiente:

- ejecutar las políticas de seguridad básicas a través de los dispositivos móviles y definir las políticas para las configuraciones importantes del dispositivo
- especificar la resistencia requerida para el bloqueo de pantalla
- restringir el uso de la cámara incorporada

Política de bloqueo de pantalla

En esta sección, el administrador puede:

- establecer un nivel de seguridad mínimo (patrón, PIN, contraseña) para el código de bloqueo de pantalla del sistema y definir la complejidad del código (por ejemplo, su longitud mínima)
- establecer el número máximo de intentos fallidos de desbloqueo (o el dispositivo volverá a la configuración predeterminada de fábrica)
- establecer la edad máxima del código de bloqueo de pantalla.
- establecer el temporizador del bloqueo de pantalla

ESET Endpoint Security for Android notifica automáticamente al usuario y al administrador si las configuraciones del dispositivo actuales cumplen con las políticas de seguridad corporativas. Si un dispositivo no cumple, la aplicación sugerirá automáticamente al usuario qué se debe cambiar para que vuelva a ser compatible.

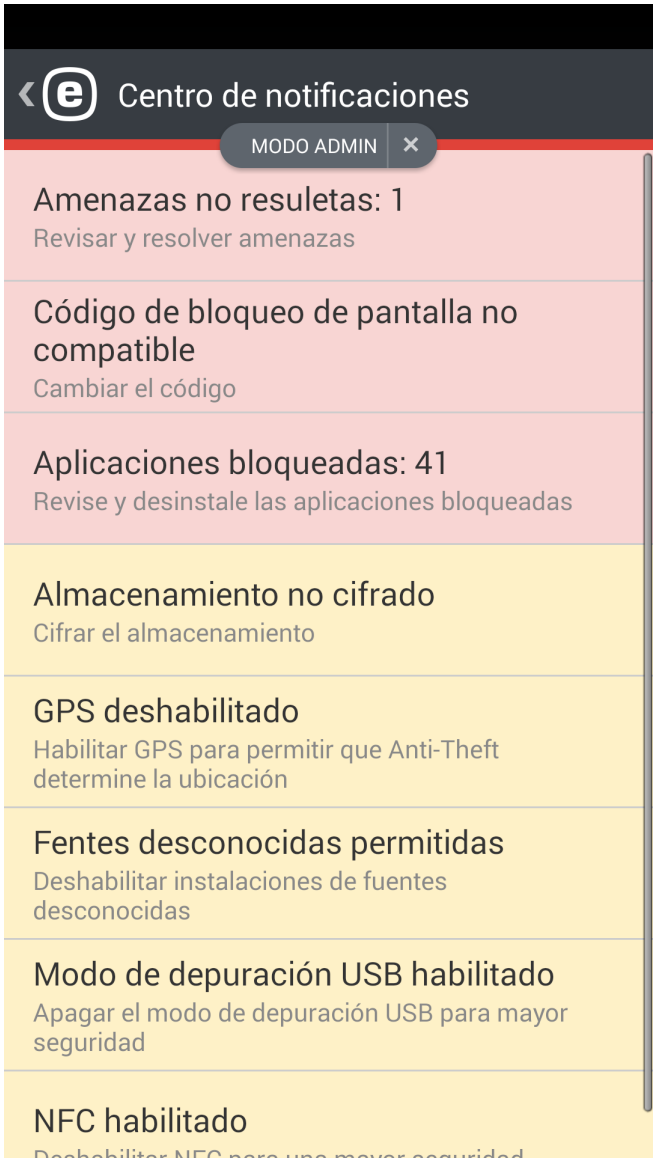
Política de configuraciones del dispositivo

La seguridad del dispositivo también incluye su **Política de configuraciones del dispositivo** (anteriormente una parte de la funcionalidad de la **Auditoría de seguridad**), que brinda al administrador del sistema la opción de

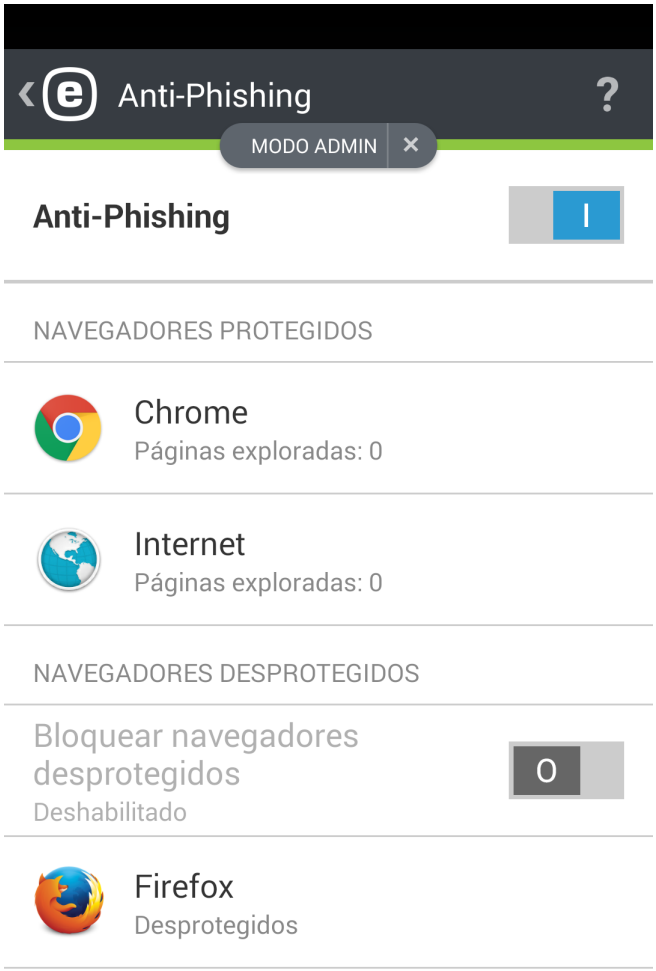
controlar las configuraciones predefinidas para determinar si se encuentran en el estado recomendado.

Las configuraciones del dispositivo incluyen:

- Wi-Fi
- Satélites de GPS
- Servicios de localización
- Memoria
- Itinerancia de datos
- Itinerancia de llamadas
- Fuentes desconocidas
- Modo de depuración
- NFC
- Cifrado del almacenamiento
- Dispositivo descifrado



Anti-Phishing



El *phishing* es una actividad delictiva que usa la ingeniería social (manipulación de usuarios para obtener información confidencial). Phishing es utilizado a menudo para obtener acceso a datos confidenciales tales como números de cuentas bancarias, números de tarjetas de crédito, números de PIN o usuarios y contraseñas.

Recomendamos que mantenga **Anti-Phishing** habilitado. ESET Endpoint Security for Android escanea direcciones URL: se bloquearán todos los posibles ataques phishing que provengan de sitios web o dominios que figuran en la base de datos de malware de ESET y se mostrará una notificación de advertencia que informa sobre el ataque.

IMPORTANTE: Anti-Phishing se integra a los navegadores Web más comunes disponibles en Android OS. En general, la protección antiphishing se encuentra disponible para navegadores Chrome, Firefox, Opera, Opera Mini, Dolphin, Samsung y stock preinstalados en dispositivos Android. Los demás navegadores figurarán como desprotegidos y se puede bloquear el acceso a ellos con el interruptor .

Para que ESET Anti-Phishing funcione de manera adecuada, se debe activar la función **Accesibilidad** en las configuraciones del sistema Android.

Otorgar permiso de acceso a ESET Endpoint Security for Android instalado 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 el acceso desinformado a estos permisos.

Cómo ESET Endpoint Security for Android usa 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.
El sitio web se bloquea cuando se detecta una amenaza para protegerlo a usted y a su información confidencial.
Los datos a los que se accede mediante permiso de accesibilidad no se comparten con terceros.

Para resolver el problema de accesibilidad:

1. Abra **Configuración** > **Accesibilidad** > **Aplicaciones descargadas** y ESET Endpoint Security for Android se pone gris.

2. Toque la aplicación ESET Endpoint Security for Android y se abrirá el cuadro de diálogo **Configuración restringida**.

3. Toque **'ACEPTAR'**.

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

5. Toque el ícono del menú de tres puntos ⋮ en la esquina superior derecha > **Permitir ajustes restringidos**.

El permiso de accesibilidad ya está habilitado y puede empezar a usar la aplicación.

Control Web

Use la configuración del control Web para proteger a su empresa del riesgo de responsabilidad legal. Por ejemplo, el control Web puede regular el acceso a sitios web que violan los derechos de propiedad intelectual. El objetivo es evitar que los empleados accedan a páginas con contenido inapropiado o perjudicial o páginas que puedan tener un impacto negativo en la productividad.

Los empleadores o los administradores de sistemas pueden prohibir el acceso a más de 27 categorías de sitios web predefinidas y a más de 140 subcategorías, y registrar estas visitas.

El control Web es una característica administrada. Toda la configuración se controla desde ESET PROTECT Cloud.

Para que el control Web funcione, un dispositivo administrado debe cumplir con los siguientes requisitos:
- Versión 3 o posterior de ESET Endpoint Security for Android.
- Versión 8 o posterior de Android.
- Inscripción en ESET PROTECT Cloud con permisos de administrador de dispositivos.

Navegadores protegidos

- Chrome
- Chrome Beta
- Firefox

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

Filtro de llamadas

Importante
La función Filtro de llamadas solo está disponible en la versión web de ESET Endpoint Security for Android.

Filtro de llamadas bloquea mensajes entrantes/salientes en base a reglas definidas por el usuario.

No se muestran notificaciones cuando se bloquea una llamada entrante. La ventaja que ofrece es que no se lo molestará con información no solicitada, pero siempre puede controlar los registros para ver si se bloqueó algún mensaje por equivocación.

Filtro de llamadas no funciona en tabletas que no admiten llamadas.

Para bloquear llamadas del último número de teléfono recibido, toque **Bloquear al último interlocutor**. Así, se creará una nueva regla.

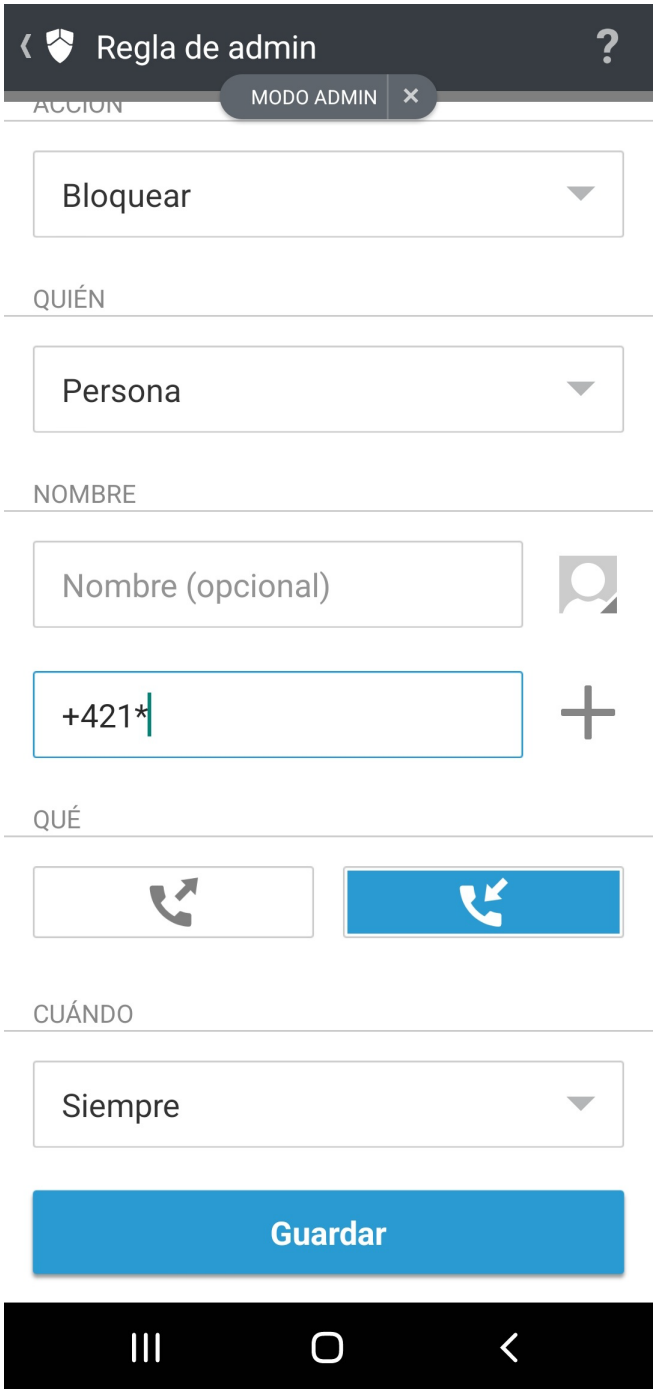
Bloquear números de teléfono con comodines

Puede bloquear un rango de números con 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 en particular, escriba el código del país y el carácter comodín ***** en el campo **Número de teléfono móvil**, de esta manera se bloquearán todas las llamadas entrantes del país que comiencen con este patrón de números. Cuando decida 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 realizadas desde Eslovaquia.



Reglas

Como usuario, puede crear reglas del usuario sin la necesidad de ingresar la Contraseña de admin. Las Reglas admin se pueden crear solo en el Modo admin. Las Reglas admin sobrescribirán cualquier regla del usuario.

Para obtener más información acerca de crear una regla nueva, consulte esta sección.

Si quiere eliminar una entrada de regla de la lista de **Reglas**, toque y mantenga la entrada y luego toque el ícono **Eliminar**.

Cómo agregar una nueva regla

Para agregar una nueva regla, toque **Agregar regla** o el ícono ➕ en la esquina superior derecha de la pantalla **Reglas**.

Especifique una persona o un grupo de números de teléfonos. ESET Endpoint Security for Android reconocerá los grupos de contactos guardados en sus Contactos (por ejemplo, Familia, Amigos o Trabajo). **Todos los números desconocidos** incluirán los números de teléfonos no guardados en su lista de contactos. Puede usar esta opción para bloquear llamadas de teléfono no bienvenidas (por ejemplo, “llamadas en frio”) o para evitar que los empleados marquen números desconocidos. La opción **Todos los números conocidos** se refiere a todos los números de teléfono guardados en su lista de contactos. **Números ocultos** se aplicará a llamadas cuyos números de teléfono estén ocultos intencionalmente por la Restricción de identificación de línea en llamada (CLIR).

Especifique qué debe bloquearse o permitirse:

- llamadas salientes
- llamadas entrantes

Para aplicar la regla solo por un tiempo especificado, toque **Siempre** > **Personalizar** y seleccione los días de la semana y un intervalo de tiempo durante el que quiera aplicar la regla. De manera predeterminada, se selecciona sábado y domingo. Esta funcionalidad puede ser útil si no quiere que lo molesten durante reuniones, viajes de negocios, por la noche o durante el fin de semana.

NOTA: Si está de viaje, todos los números de teléfono ingresados en esta lista deben incluir el código de marcado internacional seguido por el número real (por ejemplo, +1610100100).

Historial

En la sección **Historia**, puede ver las llamadas y mensajes bloqueados o permitidos por el Filtro de llamadas. Cada registro contiene el nombre de un evento, el número de teléfono correspondientes, la fecha y la hora del evento.

Si quiere modificar una regla relacionada con el número de teléfono o un contacto que fue bloqueado, selecciones la entrada de la lista tocándola y toque el ícono .

Para eliminar la entrada de la lista, selecciónela y toque el ícono . Para quitar más entradas, toque y mantenga una de las entradas, seleccione las que desea quitar y haga clic en el ícono .

Configuración

Idioma – De manera predeterminada, ESET Endpoint Security for Android está instalado en el idioma establecido en su dispositivo como configuración regional del sistema (en configuraciones del idioma y teclado del SO Android). Si desea cambiar el idioma de la interfaz del usuario de la aplicación, toque Idioma y elija el idioma que desee.

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

Actualización – Para lograr una protección máxima, es importante usar la última versión de ESET Endpoint Security for Android. Toque Actualizar para ver si hay una versión más reciente disponible para descargar desde el sitio Web de ESET.

Id del dispositivo – Establece o cambia el nombre de identificación del dispositivo para el administrador, en caso de que haya sido robado o extraviado.

Administración remota – Conecte su dispositivo a ESET PROTECT.

Configuración avanzada

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

Notificaciones de permisos: consulte la seccción Administración de permisos.

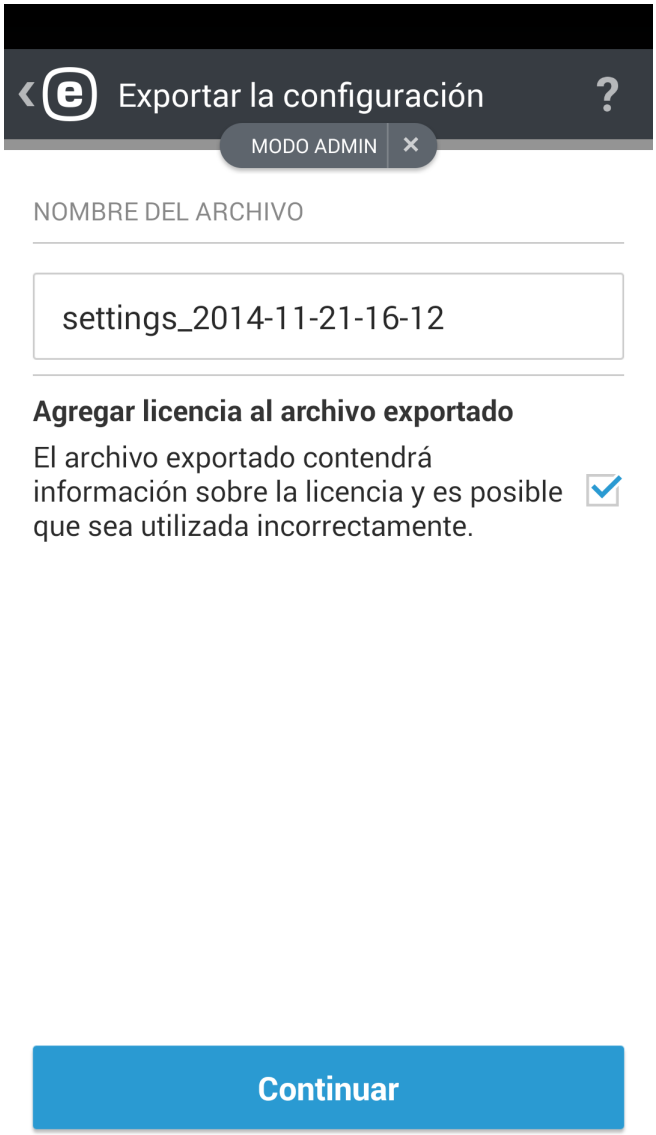
Enviar datos de uso – Esta opción ayuda a mejorar los productos de ESET mediante el envío de datos anónimos sobre el uso de la aplicación. No se enviará información sensible. Si no habilitó esta opción durante el asistente de inicio de instalación, puede hacerlo desde la sección Configuraciones > Configuración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

Contraseña de admin – Esta opción le permite configurar una nueva Contraseña de admin o cambiar la existente. Para obtener más información, consulte la sección Contraseña de admin de este documento.

Importar/Exportar configuraciones – Importa o exporta las configuraciones desde o hacia una aplicación ESET Endpoint.

Importar/Exportar configuraciones

Para compartir con facilidad las configuraciones de un dispositivo móvil con otro, si los dispositivos no son controlados por ESET PROTECT, ESET Endpoint Security for Android incluye la opción para exportar e importar la configuración del programa. El administrador puede exportar manualmente la configuración del dispositivo a un archivo que se puede compartir (por ejemplo, por correo electrónico) e importar a cualquier dispositivo ejecutándose en la aplicación del cliente. Cuando el usuario acepta el archivo de configuración recibido, define automáticamente todas las configuraciones y activa la aplicación (siempre que se haya incluido la información de la licencia). Todas las configuraciones estarán protegidas con la contraseña del administrador.



Exportar la configuración

Para exportar las configuraciones de ESET Endpoint Security for Android, especifique el nombre de archivo de las configuraciones: la fecha y hora actuales se completarán de manera automática. También puede agregar la información de la licencia (Clave de licencia o dirección de correo electrónico de admin de Seguridad y contraseña) al archivo exportado, pero tenga en cuenta que esta información no se cifrará y puede ser mal utilizada.

En el próximo paso, seleccione la manera en que desea compartir el archivo mediante:

- Red Wi-Fi
- Bluetooth
- Correo electrónico
- Gmail
- aplicación de exploración de archivos (por ejemplo, ASTRO File Manager o ES File Explorer)

Importar configuraciones

Para importar las configuraciones desde un archivo ubicado en el dispositivo, use una aplicación de exploración de archivos para localizar el archivo de configuraciones y elija ESET Endpoint Security for Android.

También se pueden importar las configuraciones seleccionando un archivo en la sección **Historia**.

Historial

La sección Historia le ofrece una lista de los archivos de configuración importados y le permite compartir, importar o eliminarlos.

Contraseña de admin

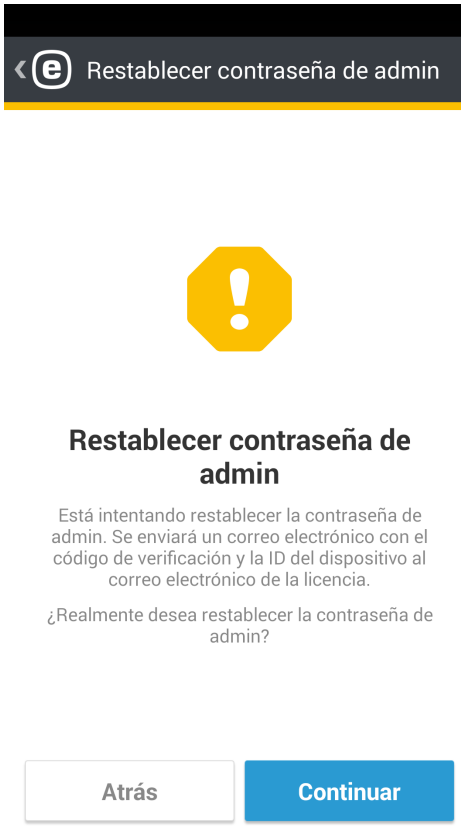
La **Contraseña de admin** es necesaria para desbloquear un dispositivo, enviar comandos Anti-Theft, acceder a funciones protegidas con contraseña y desinstalar ESET Endpoint Security for Android.

La creación de la **contraseña de administrador** impide que los usuarios cambien los ajustes y desinstalen ESET Endpoint Security for Android.

Elija la contraseña con cuidado. Para aumentar la seguridad, use una combinación de letras minúsculas, mayúsculas y números.

Para restablecer la Contraseña de admin en un dispositivo con una pantalla bloqueada:

1. Toque **¿Olvidó la contraseña?** > **Continuar** > **Solicitar código de verificación**. Si el dispositivo no está conectado a internet, toque el enlace **elegir restablecimiento sin conexión** en su lugar, y póngase en contacto con el 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 estará activo durante siete días. Escriba el código de verificación y una nueva contraseña en la pantalla bloqueada de su dispositivo.

Administración remota

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

Usar ESET PROTECT no solo aumenta su nivel de seguridad, sino que también brinda facilidad de uso en la administración de todos los productos ESET instalados en las estaciones de trabajo y los dispositivos móviles del cliente. Los dispositivos con ESET Endpoint Security for Android pueden conectarse a ESET PROTECT usando cualquier tipo de conexión a Internet (WiFi, LAN, WLAN, red celular (3G, 4G LTE, HSDPA, GPRS), etc.), siempre que sea una conexión a Internet regular (sin un proxy o firewall) y ambos puntos de conexión estén configuradas correctamente.

Al conectarse a ESET PROTECT por una red celular, una conexión exitosa depende del proveedor de red móvil y requiere una conexión a Internet con todas las funciones.

Para conectar un dispositivo a ESET PROTECT, añada el dispositivo a la lista de Equipos en la consola web de ESET PROTECT, inscriba el dispositivo con la tarea **Inscripción de dispositivo** e ingrese la **dirección del servidor del MDC**.

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

- **MDCserver:** el nombre completo del DNS o la dirección IP pública del servidor que ejecuta el Mobile Device Connector (MDC). Solo se puede utilizar el nombre de host si se conecta a través de una red Wi-Fi

interna.

- **Puerto:** el número de puerto usado para conectarse al Mobile Device Connector
- **Token:** cadena de caracteres generados por un administrador en la consola web de ESET PROTECT.

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

- Cómo administrar políticas
- Cómo crear tareas de clientes
- Obtenga información sobre informes

Id del dispositivo

El Id del dispositivo ayuda al administrador a identificar el dispositivo si lo pierde o se lo roban.

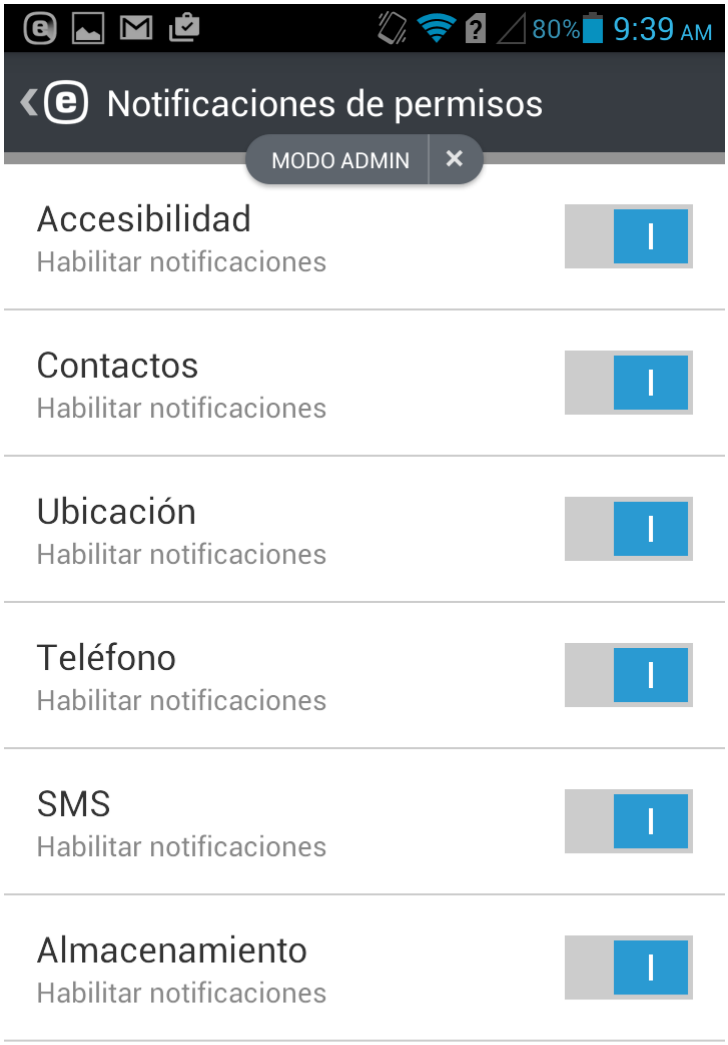
Administración de permisos

En Android 6 (Marshmallow), Google presento una nueva Administración de permisos y ESET Endpoint Security for Android es compatible. Las aplicaciones diseñadas para Android 6.0 solicitarán permisos una vez que haya comenzado a utilizarlas. En lugar de otorgar acceso a una aplicación durante la instalación, se le indicara que lo haga la primera vez que la aplicación quiera acceder a una función en particular del dispositivo.

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

- **Accesibilidad:** se requiere este permiso para que ESET Anti-Phishing funcione de manera adecuada
- **Contactos:** se requiere para Anti-Theft y Filtro de llamadas
- **Ubicación:** Anti-Theft
- **Teléfono:** Anti-Theft y Filtro de llamadas
- **SMS:** Anti-Theft y Filtro de llamadas
- **Almacenamiento:** antivirus y Anti-Theft

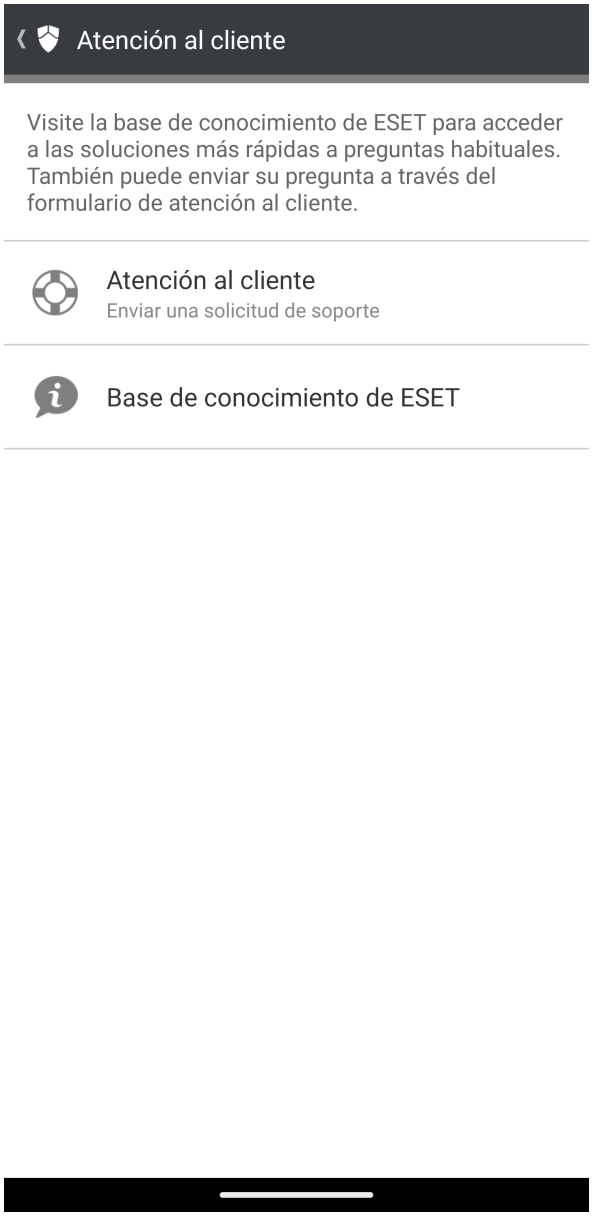
El administrador tiene permitido desactivar el monitoreo de estos permisos en **Configuraciones** > **Notificaciones de permisos**.



Atención al cliente

Los especialistas de Atención al cliente de ESET están disponibles para brindar ayuda administrativa o asistencia técnica relacionada con ESET Endpoint Security for Android o con cualquier otro producto de ESET.

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



ESET Endpoint Security for Android incluye la funcionalidad de registro avanzado para ayudar a diagnosticar problemas técnicos potenciales. Para proporcionar ESET con un registro de aplicación detallado, asegúrese de que la opción **Enviar registro de aplicación** esté seleccionada (predeterminado). Toque **Enviar** para enviar su solicitud. Un especialista de Atención al cliente lo contactará a la dirección de correo electrónico que usted proporcione.

Programa de mejora de la experiencia del cliente

Al unirse a nuestro Programa de mejora de la experiencia del cliente usted le provee a ESET información anónima relacionada con el uso de nuestros productos. Nuestra política de privacidad contiene información adicional sobre el procesamiento de datos.

Su consentimiento

La participación en el programa es voluntaria en función de su consentimiento. Tras unirse, la participación es pasiva, lo que significa que no tiene que hacer nada más. Puede revocar su consentimiento en cualquier momento al cambiar la configuración del producto. Esto nos impedirá el procesamiento de sus datos anónimos.

¿Qué tipo de información recolectamos?

Datos de la interacción con el producto

Estos datos nos informan sobre cómo se utilizan nuestros productos. Gracias a esto sabemos, por ejemplo, cuáles funcionalidades se utilizan frecuentemente, qué configuraciones modifican los usuarios o cuánto tiempo pasan utilizando nuestros productos.

Datos acerca de dispositivos

Recopilamos esta información para comprender en qué dispositivos y dónde se utilizan nuestros productos. Los más usuales son el modelo del dispositivo, el país y la versión y el nombre del sistema operativo.

Datos de diagnóstico de errores

También se recopilan datos acerca del error y de la situación de la falla. Por ejemplo, qué error se ha producido y qué acciones derivaron en él.

¿Por qué recopilamos esta información?

Estos datos anónimos nos hacen posible mejorar nuestros productos para usted, el usuario. Nos ayudan a convertirlos en más relevantes, fáciles de usar y sin fallas, en la medida de lo posible.

¿Quién controla esta información?

ESET, spol. s r.o. es el único controlador de los datos recopilados en el programa. Esta información no es compartida con terceros.

Acuerdo de licencia de usuario final

Vigente a partir del 19 de octubre de 2021.

IMPORTANTE: Lea los términos y las condiciones del producto de aplicación que se especifican abajo antes de descargarlo, instalarlo, copiarlo o usarlo. **AL DESCARGAR, INSTALAR, COPIAR O UTILIZAR EL SOFTWARE, USTED DECLARA SU CONSENTIMIENTO CON LOS TÉRMINOS Y CONDICIONES Y RECONOCE QUE HA LEÍDO LA POLÍTICA DE PRIVACIDAD.**

Acuerdo de Licencia de Usuario Final

Los términos de este Acuerdo de licencia para el usuario final ("Acuerdo") ejecutado por y entre ESET, spol. s r. o., con domicilio social en Einsteinova 24, 85101 Bratislava, Slovak Republic, registrado en el Registro Mercantil administrado por el tribunal de distrito de Bratislava I, sección Sro, n.° de entrada 3586/B, número de registro de negocio: 31333532 ("ESET" o el "Proveedor") y usted, una persona física o jurídica ("Usted" o el "Usuario final"), tienen derecho a usar el Software definido en el Artículo 1 de este Acuerdo. El Software definido en este artículo puede almacenarse en un soporte digital, enviarse mediante correo electrónico, descargarse de Internet, descargarse de servidores del Proveedor u obtenerse de otras fuentes bajo los términos y condiciones mencionados más adelante.

ESTO ES UN ACUERDO SOBRE LOS DERECHOS DEL USUARIO FINAL; NO UN CONTRATO DE COMPRA PARA ARGENTINA. El Proveedor sigue siendo el propietario de la copia del Software y del soporte físico en el que el

Software se suministra en paquete comercial, así como de todas las demás copias a las que el Usuario final está autorizado a hacer en virtud de este Acuerdo.

Al hacer clic en las opciones "Acepto" o "Acepto..." durante la instalación, descarga, copia o uso del Software, acepta los términos y condiciones de este Acuerdo y la Política de privacidad. Si no acepta todos los términos y condiciones de este Acuerdo o la Política de privacidad, de inmediato 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 LA UTILIZACIÓN DEL SOFTWARE INDICA QUE HA LEÍDO ESTE ACUERDO, QUE LO COMPRENDE Y QUE CONSIENTE OBLIGARSE POR SUS TÉRMINOS Y CONDICIONES.

1. **Software.** Tal como se utiliza en este Acuerdo, el término "Software" significa: (i) el programa informático que acompaña a este Acuerdo y todos sus componentes; (ii) todos los contenidos de los discos, CD-ROMs, DVDs, correos electrónicos y cualquier adjunto, u otros medios con los cuales se provee este Acuerdo, incluyendo el formulario del código objeto del software provisto en soporte digital, por medio de correo electrónico o descargado a través de la Internet; (iii) cualquier material escrito explicativo relacionado y cualquier otra documentación posible relacionada con el Software, sobre todo cualquier descripción del Software, sus especificaciones, cualquier descripción de las propiedades u operación del software, cualquier descripción del ambiente operativo en el cual se utiliza el Software, instrucciones de uso o instalación del Software o cualquier descripción del modo de uso del Software ("Documentación"); (iv) copias del Software, parches para posibles errores del Software, adiciones al Software, extensiones del Software, versiones modificadas del Software y actualizaciones de los componentes del Software, si existieran, con la autorización que le da a Usted el Proveedor con arreglo al Artículo 3 de este Acuerdo. El Software será provisto exclusivamente en la forma de código objeto ejecutable.

2. **Instalación, equipo y clave de licencia**. El Software suministrado en un soporte digital, enviado por correo electrónico, descargado de Internet, descargado de los servidores del Proveedor u obtenido de otras fuentes requiere instalación. El Software debe instalarse en un equipo correctamente configurado que cumpla, como mínimo, con los requisitos especificados en la Documentación. La metodología de instalación se describe en la Documentación. No puede haber ningún programa informático ni Hardware que pudiera afectar al Software instalado en el equipo en el que instala el Software. El equipo hace referencia al Hardware que incluye, pero no se limita, a equipos personales, equipos portátiles, estaciones de trabajo, equipos de bolsillo, teléfonos inteligentes, dispositivos electrónicos portátiles o cualquier otro dispositivo para el que se diseñe el Software y en el que vaya a instalarse y/o utilizarse. La clave de licencia se refiere a una secuencia única de símbolos, letras números o caracteres especiales que se le brinda al Usuario final para permitirle el uso del Software de manera legal, así como de una versión específica de este o para brindarle una extensión de los términos de la Licencia en conformidad con el presente 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.** Usted tendrá el derecho no exclusivo y no transferible de instalar el Software en el disco rígido de un equipo o soporte similar para un almacenamiento permanente de datos, instalar y almacenar el Software en la memoria de un sistema informático e implementar, almacenar y mostrar el Software.

b) **Disposición sobre la cantidad de licencias.** El derecho a utilizar el Software estará sujeto a la cantidad de Usuarios finales. Un "Usuario final" se refiere a lo siguiente: (i) instalación del Software en un sistema informático, o (ii) si el alcance de una licencia está vinculado a la cantidad de buzones de correo, un Usuario final se referirá a un usuario informático que acepta correo electrónico a través de un Agente de usuario de correo ("AUC"). Si un AUC acepta el correo electrónico y lo distribuye posteriormente en forma automática a varios usuarios, la cantidad de Usuarios finales se determinará conforme a la cantidad real de usuarios para los que se distribuyó el

correo electrónico. Si un servidor de correo cumple la función de una pasarela de correo, la cantidad de Usuarios finales será equivalente a la cantidad de usuarios de servidores de correo a los que dicha pasarela presta servicios. Si se envía una cantidad no especificada de direcciones de correo electrónico (por ejemplo, con alias) a un usuario y el usuario las acepta, y el cliente no distribuye automáticamente los mensajes a más usuarios, se requiere la Licencia únicamente para un equipo. No debe usar la misma Licencia en más de un equipo al mismo tiempo El Usuario final solo tiene derecho a introducir la Clave de licencia en el Software en la medida en que el Usuario final tenga derecho a usar el Software de acuerdo con la limitación derivada del número de Licencias otorgadas por el Proveedor. Se considera que la clave de Licencia es confidencial. No puede compartirla con terceros ni puede permitirles que la utilicen a menos que el presente Acuerdo o el Proveedor indique lo contrario. Si su clave de Licencia se encuentra en riesgo notifique al Proveedor de inmediato.

c) **Home/Business Edition.** La versión Home Edition del Software solo se usará en entornos privados o no comerciales para uso en el hogar y familiar exclusivamente. Debe obtener una versión Business Edition del software para poder usarla en un entorno comercial, así como en servidores, transmisores y puertas de enlace de correo o de Internet.

d) **Término de la Licencia.** El derecho a utilizar el Software tendrá un límite de tiempo.

e) **Software de OEM.** El software clasificado como "OEM" solo se puede usar en el equipo con el que se ha obtenido. No puede transferirse a otro equipo.

f) **Software NFR y versión de prueba.** Al Software clasificado como "No apto para la reventa", "NFR" o "Versión de prueba" no se le podrá asignar un pago y puede utilizarse únicamente para hacer demostraciones o evaluar las características del Software.

g) **Rescisión de la Licencia.** La Licencia se rescindirá automáticamente al finalizar el período para el cual fue otorgada. Si Usted no cumple con alguna de las disposiciones de este Acuerdo, el Proveedor tendrá el derecho de anular el Acuerdo, sin perjuicio de cualquier derecho o recurso judicial disponible para el Proveedor en dichas eventualidades. En el caso de cancelación de la Licencia, Usted deberá borrar, destruir o devolver de inmediato por su propia cuenta el Software y todas las copias de seguridad a ESET o al punto de venta donde obtuvo el Software. Tras la finalización de la Licencia, el Proveedor podrá cancelar el derecho del Usuario Final a utilizar las funciones del Software que requieran conexión a los servidores del Proveedor o de terceros.

4. **Funciones con recopilación de información y requisitos para la conexión a Internet.** Para que funcione de manera correcta, el Software requiere conexión a Internet y debe conectarse a intervalos regulares a los servidores del Proveedor o de terceros y debe recopilar información en conformidad con la Política de Privacidad. La conexión a Internet y la recopilación de datos son necesarias para llevar a cabo las siguientes funciones del Software:

a) **Actualizaciones del Software.** El Proveedor podrá publicar periódicamente actualizaciones o actualizaciones del Software ("Actualizaciones"), 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 aprovisionar Actualizaciones, es necesario verificar la autenticidad de la Licencia, lo que incluye información sobre el equipo o la plataforma en los que está instalado el Software, de acuerdo con la Política de Privacidad.

La entrega de todas las actualizaciones puede estar sujeta a la Política de fin de la vida útil ("Política EOL"), disponible en https://go.eset.com/eol_business. No se proporcionarán actualizaciones una vez que el Software o cualquiera de sus funciones lleguen a la fecha de fin de su vida útil, como se define en la Política EOL.

b) **Envío de infiltraciones e información al Proveedor**. El Software contiene funciones que reúnen muestras de virus informáticos, otros programas informáticos dañinos y objetos sospechosos, problemáticos, potencialmente no deseados o potencialmente no seguros como archivos, URL, paquetes de IP y marcos de Ethernet

(“Infiltraciones”) y luego los envía al Proveedor, incluidas, entre otras, la información sobre el proceso de instalación, el equipo o la plataforma en los cuales se instala el Software y la información sobre las operaciones y la funcionalidad del Software (“Información”). La Información y las Infiltraciones pueden contener datos (incluidos datos personales obtenidos aleatoriamente o accidentalmente) sobre el Usuario Final u otros usuarios del equipo en el cual se encuentra instalado el Software, y archivos afectados por Infiltraciones con metadatos asociados.

La Información y las Infiltraciones pueden ser recopiladas por las siguientes funciones del Software:

i. La función Sistema de reputación de LiveGride incluye la recopilación y el envío de hashes de una vía relacionados a Infiltraciones al Proveedor. Esta función se activa con la configuración estándar del Software.

ii. La función del sistema de comentarios de LiveGrid es recopilar información acerca de las infiltraciones con metadatos relacionados para enviársela al Proveedor. El Usuario final debe activar esta función durante la instalación del Software.

El proveedor solo debe hacer uso de la información y de las infiltraciones que recibe para analizar y para investigar las infiltraciones, para mejorar el Software y el proceso de verificación de la autenticidad de la Licencia. Asimismo, debe tomar las medidas correspondientes para garantizar la seguridad de las infiltraciones y de la información que recibe. Si se activa esta función del Software, el Proveedor deberá recopilar y procesar las infiltraciones y la información tal como se especifica en la Política de Privacidad y en conformidad con las normas legales vigentes. Puede desactivar estas funciones en cualquier momento.

A los efectos de este Acuerdo, es necesario recopilar, procesar y almacenar información que permita al Proveedor identificarlo en conformidad con la Política de Privacidad. Por medio del presente, reconoce que el Proveedor utiliza sus propios medios para verificar si Usted hace uso del Software de acuerdo con las disposiciones del Acuerdo. Asimismo, reconoce que, a los efectos de este Acuerdo, es necesario que su información se transfiera durante las comunicaciones entre el Software y los sistemas informáticos del Proveedor o de sus socios comerciales como parte de la red de distribución y soporte del Proveedor a fin de garantizar la funcionalidad del Software, de autorizar el uso del Software y proteger los derechos del Proveedor.

Tras la finalización de este Acuerdo, el Proveedor o cualquiera de sus socios comerciales tendrán el derecho de transferir, procesar y almacenar datos esenciales que lo identifiquen, con el propósito de realizar la facturación y para la ejecución del presente Acuerdo y para transmitir notificaciones a su equipo.

Los detalles sobre la privacidad, la protección de la información personal y sus derechos como parte interesada pueden encontrarse en la Política de Privacidad, disponible en el sitio web del Proveedor y a la que se puede acceder de manera directa desde el proceso de instalación. También puede acceder a ella desde la sección de ayuda del Software.

5. **Ejercicio de los derechos del 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 sistemas informáticos para los que ha obtenido una Licencia.

6. **Restricciones de los derechos.** No puede copiar, distribuir, extraer componentes o crear versiones derivadas del Software. Al usar el Software, Usted tiene la obligación de cumplir con las siguientes restricciones:

a) Puede crear una copia del Software en un soporte de almacenamiento permanente de datos como una copia de seguridad para archivar, siempre que su copia de seguridad para archivar no esté instalada ni se utilice en ningún equipo. Cualquier otra copia que realice del Software constituirá un incumplimiento de este Acuerdo.

b) No puede utilizar, modificar, traducir ni reproducir el Software, o transferir los derechos de su uso o copias realizadas del Software de ninguna otra forma a lo establecido en este Acuerdo.

c) No puede vender, sublicenciar, arrendar o alquilar el Software, ni usarlo para suministrar servicios comerciales.

d) No puede aplicar técnicas de ingeniería inversa, descompilar o desmontar el Software, ni intentar obtener el código fuente del Software de ninguna otra forma, salvo en la medida en que esta restricción esté explícitamente prohibida por la ley.

e) Usted acepta que solo usará el Software de forma que se cumplan todas las leyes aplicables en la jurisdicción en la que lo utilice, incluyendo, pero sin limitarse a, las restricciones aplicables relacionadas con el copyright y otros derechos de propiedad intelectual.

f) Usted acepta que solamente usará el Software y sus funciones de una manera que no limite las posibilidades de otros Usuarios finales para acceder a estos servicios. El Proveedor se reserva el derecho de limitar el alcance los servicios proporcionados a Usuarios finales individuales, para activar el uso de los servicios por parte de la mayor cantidad posible de Usuarios finales. La limitación del alcance de los servicios también significará la terminación completa de la posibilidad de usar cualquiera de las funciones del Software y la eliminación de los Datos y de la información de los servidores de los Proveedores o de los servidores de terceros relacionados con una función específica del Software.

g) Usted acepta no ejercer ninguna actividad que implique el uso de la clave de Licencia de manera contraria a los términos de este Acuerdo ni que implique proporcionar la clave de Licencia a personas que no estén autorizadas a hacer uso del Software, como la transferencia de la clave de Licencia usada o no. en cualquier forma, así como la reproducción no autorizada, o la distribución de claves de Licencia duplicadas o generadas. Asimismo, no utilizará el Software como resultado del uso de una clave de Licencia obtenida de una fuente que no sea el Proveedor.

7. **Copyright**. El Software y todos los derechos, incluyendo, pero sin limitarse a, los derechos de propiedad y los derechos de propiedad intelectual, son propiedad de ESET y/o sus licenciatarios. Están protegidos por las disposiciones de tratados internacionales y por todas las demás leyes nacionales aplicables del país en el que se utiliza el Software. La estructura, la organización y el código del Software son valiosos secretos comerciales e información confidencial de ESET y/o sus licenciatarios. No puede copiar el Software, a excepción de lo especificado en el artículo 6 (a). Todas las copias que este Acuerdo le permita hacer deberán incluir el mismo copyright y los demás avisos legales de propiedad que aparezcan en el Software. Si aplica técnicas de ingeniería inversa, descompila o desmonta el Software, o intenta obtener el código fuente del Software de alguna otra forma, en incumplimiento de las disposiciones de este Acuerdo, por este medio Usted acepta que toda la información obtenida de ese modo se considerará automática e irrevocablemente transferida al Proveedor o poseída por el Proveedor de forma completa desde el momento de su origen, más allá de los derechos del Proveedor en relación con el incumplimiento 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 medios duales, varias copias**. En caso de que el Software sea compatible con varias plataformas o idiomas, o si Usted obtuvo varias copias del Software, solo puede usar el Software para la cantidad de sistemas informáticos y para las versiones correspondientes a la Licencia adquirida. 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 desde la fecha en que Usted acepta los términos de la Licencia. Puede poner fin a este Acuerdo en cualquier momento. Para ello, desinstale, destruya o devuelva permanentemente y por cuenta propia el Software, todas las copias de seguridad, y todos los materiales relacionados suministrados por el Proveedor o sus socios comerciales. Su derecho a usar el Software y cualquiera de sus funciones puede estar sujeto a la Política EOL. Cuando el Software o cualquiera de sus funciones lleguen a la fecha de fin de su vida útil definida en la Política EOL, se terminará su derecho a usar el Software. Más allá de la

forma de rescisión de este Acuerdo, las disposiciones de los artículos 7, 8, 11, 13, 19 y 21 seguirán siendo aplicables por tiempo ilimitado.

11. **DECLARACIONES DEL USUARIO FINAL**. COMO USUARIO FINAL, USTED RECONOCE QUE EL SOFTWARE SE SUMINISTRA EN UNA CONDICIÓN "TAL CUAL ES", SIN UNA GARANTÍA EXPRESA O IMPLÍCITA DE NINGÚN TIPO Y HASTA EL ALCANCE MÁXIMO PERMITIDO POR LAS LEYES APLICABLES. NI EL PROVEEDOR, SUS LICENCIATARIOS, SUS AFILIADOS NI LOS TITULARES DEL COPYRIGHT PUEDEN HACER NINGUNA REPRESENTACIÓN O GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS DE COMERCIABILIDAD O ADECUACIÓN PARA UN FIN ESPECÍFICO O GARANTÍAS DE QUE EL SOFTWARE NO INFRINJIRÁ UNA PATENTE, DERECHOS DE PROPIEDAD INTELECTUAL, MARCAS COMERCIALES U OTROS DERECHOS. NO EXISTE NINGUNA GARANTÍA DEL PROVEEDOR NI DE NINGUNA OTRA PARTE DE QUE LAS FUNCIONES CONTENIDAS EN EL SOFTWARE CUMPLIRÁN CON SUS REQUISITOS O DE QUE LA OPERACIÓN DEL SOFTWARE SERÁ ININTERRUMPIDA O ESTARÁ LIBRE DE ERRORES. USTED ASUME TODA LA RESPONSABILIDAD Y EL RIESGO POR LA ELECCIÓN DEL SOFTWARE PARA LOGRAR SUS RESULTADOS DESEADOS Y POR LA INSTALACIÓN, EL USO Y LOS RESULTADOS QUE OBTENGA DEL MISMO.

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

13. **LIMITACIÓN DE RESPONSABILIDAD**. EN LA MEDIDA EN QUE LO PERMITA LA LEGISLACIÓN APLICABLE, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O LICENCIADORES SERÁN RESPONSABLES DE PÉRDIDAS DE INGRESOS, GANANCIAS, VENTAS, DATOS O COSTOS DE ADQUISICIÓN DE BIENES O SERVICIOS SUSTITUIDOS, DAÑOS A LA PROPIEDAD, DAÑOS PERSONALES, INTERRUPCIÓN DEL NEGOCIO, PÉRDIDA DE INFORMACIÓN COMERCIAL O DE CUALQUIER VALOR ESPECIAL, DIRECTO, INSONDADO, ACCIDENTAL, ECONÓMICO, DE COBERTURA, DAÑOS PUNITIVOS, ESPECIALES O CONSECUENCIALES, QUE SIN EMBARGO DERIVEN O SURJAN POR CONTRATO, AGRAVIOS, NEGLIGENCIA U OTRA TEORÍA DE RESPONSABILIDAD QUE DERIVE DE LA INSTALACIÓN, EL USO O LA INCAPACIDAD DE USAR EL SOFTWARE, AUNQUE EL PROVEEDOR, SUS LICENCIADORES O FILIALES RECIBAN INFORMACIÓN DE 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. Nada de lo contenido en este Acuerdo perjudicará los derechos estatutarios de ninguna parte que actúe en calidad de consumidor si infringe dicho Acuerdo.

15. **Soporte técnico**. ESET o los terceros autorizados por ESET suministrarán soporte técnico a discreción propia, sin ninguna garantía ni declaración. Cuando el software o cualquiera de sus funciones lleguen a la fecha de fin de la vida útil definida en la Política EOL, no se proporcionará soporte técnico. El Usuario final deberá crear una copia de seguridad de todos los datos existentes, software y prestaciones de los programas en forma previa al suministro de soporte técnico. ESET y/o los terceros autorizados por ESET no pueden aceptar la responsabilidad por el daño o pérdida de datos, propiedad, software o hardware, o pérdida de beneficios debido al suministro de soporte técnico. ESET y/o los terceros autorizados por ESET se reservan el derecho de decidir si la solución del problema excede el alcance del soporte técnico. ESET se reserva el derecho de rechazar, suspender o dar por finalizado el suministro de soporte técnico a discreción propia. Se puede solicitar información sobre la Licencia y cualquier otro tipo de información a fin de brindar soporte técnico conforme a la Política de Privacidad.

16. **Transferencia de la Licencia**. El Software puede transferirse de un sistema informático a otro, a menos que esta acción infrinja los términos del presente Acuerdo. Si no infringe los términos del Acuerdo, el Usuario final solamente tendrá derecho a transferir en forma permanente la Licencia y todos los derechos derivados de este Acuerdo a otro Usuario final con el consentimiento del Proveedor, sujeto a las siguientes condiciones: (i) que el Usuario final original no se quede con ninguna copia del Software; (ii) que la transferencia de los derechos sea directa, es decir, del Usuario final original al nuevo Usuario final; (iii) que el nuevo Usuario final asuma todos los

derechos y obligaciones pertinentes al Usuario final original bajo los términos de este Acuerdo; (iv) que el Usuario final original le proporcione al nuevo Usuario final la Documentación que habilita la verificación de la autenticidad del Software, como se especifica en el artículo 17.

17. **Verificación de la autenticidad del Software.** El Usuario final puede demostrar su derecho a usar el Software en una de las siguientes maneras: (i) a través de un certificado de licencia emitido por el Proveedor o por un tercero designado por el Proveedor; (ii) a través de un acuerdo de licencia por escrito, en caso de haberse establecido dicho acuerdo; (iii) a través de la presentación de un correo electrónico enviado por el Proveedor donde se incluyan los detalles de la Licencia (nombre de usuario y contraseña). Se puede solicitar información sobre la Licencia y datos sobre el Usuario final a para llevar a cabo la verificación de la autenticidad del Software conforme a la Política de Privacidad.

18. **Licencias para autoridades públicas y el gobierno de los Estados Unidos**. Se deberá suministrar el Software a las autoridades públicas, incluyendo el gobierno argentino, con los derechos de la Licencia y las restricciones descritas en este Acuerdo.

19. **Cumplimiento del control comercial**.

a) Usted no podrá, ya sea directa o indirectamente, exportar, reexportar o transferir el Software, o de alguna otra forma ponerlo a disposición de ninguna persona, o utilizarlo de ninguna manera, o participar de ningún acto, que pueda ocasionar que ESET o sus compañías controladoras, sus empresas subsidiarias y las subsidiarias de cualquiera de sus compañías controladoras, así como también las entidades controladas por sus compañías controladoras ("Afiliadas") violen, o queden sujetas a las consecuencias negativas de las Leyes de Control Comercial, las cuales incluyen

i. toda ley que controle, restrinja o imponga requisitos de licencia a la exportación, reexportación o transferencia de productos, software, tecnología o servicios, establecida o adoptada por cualquier gobierno, estado o autoridad reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados Miembro, o cualquier país donde deban cumplirse las obligaciones conforme al Acuerdo, o donde ESET o cualquiera de sus Afiliadas operen o estén constituidas y

ii. cualquier sanción, restricción, embargo, prohibición de exportación o importación, prohibición de transferencia de fondos o activos o prohibición de prestación de servicios, ya sea de índole económica, financiera, comercial o de otro tipo, o toda medida equivalente impuesta por cualquier gobierno, estado o autoridad reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados Miembro, o cualquier país donde deban cumplirse las obligaciones conforme al Acuerdo, o donde ESET o cualquiera de sus Afiliadas operen o estén constituidas.

(actos legales mencionados en los puntos i y ii. anteriormente, denominados "Leyes de control comercial").

b) ESET tendrá el derecho de suspender sus obligaciones conforme a estos Términos o terminar el Acuerdo, con efecto inmediato, en los siguientes casos:

i. ESET determina que, en su razonable opinión, el Usuario ha violado o podría violar la disposición del Artículo 19 a) del Acuerdo; o

ii. el Usuario final o el Software quedan sujetos a las Leyes de Control Comercial y, en consecuencia, ESET determina que, en su razonable opinión, el cumplimiento continuo de sus obligaciones conforme al Acuerdo podría ocasionar que ESET o sus Afiliadas incurriesen en la violación de las Leyes de Control Comercial o quedasen sujetas a las consecuencias negativas de estas.

c) Ninguna de las estipulaciones del Acuerdo tiene por objeto inducir o exigir, ni debe interpretarse como una intención de inducir o exigir a ninguna de las partes actuar o abstenerse de actuar (o acordar actuar o abstenerse

de actuar) de ninguna manera que resulte inconsistente con las Leyes de Control Comercial aplicables, o se encuentre penalizada o prohibida por estas.

20. **Avisos**. Todos los avisos y devoluciones de software o documentación deben entregarse a: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, sin perjuicio del derecho de ESET a comunicarle cualquier cambio de este Acuerdo, las Políticas de privacidad, la Política de EOL y la Documentación de acuerdo con el artículo. 22 del Acuerdo. ESET puede enviarle correos electrónicos, notificaciones en la aplicación a través del Software o publicar la comunicación en nuestro sitio web. Acepta recibir comunicaciones legales de ESET de forma electrónica, lo que incluye comunicaciones sobre cambios de Términos, Términos especiales o Políticas de privacidad, cualquier contrato de trabajo o aceptación o invitación a tratar, 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 conforme a la legislación de la República Eslovaca. En el presente Acuerdo, el Usuario final y el Proveedor aceptan que los principios del conflicto de leyes y la Convención de las Naciones Unidas sobre los Contratos de Venta Internacional de Bienes no serán aplicables. Acepta expresamente que cualquier disputa o demanda derivada del presente Acuerdo con respecto al Proveedor o relativa al uso del Software deberá resolverse por el Tribunal del Distrito de Bratislava I., Eslovaquia; asimismo, Usted acepta expresamente el ejercicio de la jurisdicción del Tribunal mencionado.

22. **Disposiciones generales**. Si alguna disposición de este Acuerdo no es válida o aplicable, no afectará la validez de las demás disposiciones del Acuerdo, que seguirán siendo válidas y ejecutables bajo las condiciones aquí estipuladas. Este acuerdo se ha ejecutado en inglés. En el caso de que se prepare cualquier traducción del acuerdo para su comodidad o con cualquier otro fin, o en caso de discrepancia entre las versiones en diferentes idiomas de este acuerdo, prevalecerá la versión en inglés.

ESET se reserva el derecho de realizar cambios en el Software, así como de revisar los términos de este Acuerdo, sus Anexos, la Política de privacidad, la Política y la Documentación de EOL o cualquier parte de ellos, en cualquier momento mediante la actualización del documento pertinente (i) para reflejar cambios del Software o el comportamiento comercial de ESET, (ii) por cuestiones legales, normativas o de seguridad; o (iii) para evitar abusos o daños. Se le notificará cualquier revisión del Acuerdo por correo electrónico, notificación en la aplicación o por otros medios electrónicos. Si no está de acuerdo con los cambios de texto del Acuerdo, puede rescindirlo de acuerdo con el Artículo 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 de texto se considerarán aceptados y estarán vigentes para Usted a partir de la fecha en que reciba un aviso del cambio.

Este es el acuerdo entero entre el proveedor y Usted relacionado con el Software y reemplaza a cualquier representación, discusión, garantía, comunicación o publicidad previa relacionadas con el Software.

EULAID: EULA-PRODUCT-LG; 3537.0

Política de privacidad

La protección de los datos personales reviste especial importancia para ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, Slovak Republic, Número de registro comercial: 31333532 como Controlador de datos ("ESET" o "Nosotros"). Queremos cumplir con el requisito de transparencia de acuerdo con el Reglamento General de Protección de Datos de la Unión Europea (“RGPD”). A fin de cumplir con el objetivo, publicamos la presente Política de privacidad con el único propósito de informar a nuestros clientes (“Usuario final” o “Usted”), en carácter de interesados, acerca de los siguientes temas relativos a la protección de los datos personales:

- Fundamento jurídico para el procesamiento de datos personales.

- Intercambio y confidencialidad de los datos.
- Seguridad de los datos.
- Sus derechos como interesado.
- Procesamiento de sus datos personales,
- Información de contacto.

Procesamiento de sus datos personales

Los servicios prestados por ESET implementados en nuestro producto se prestan de acuerdo con los términos del Acuerdo de licencia de usuario final ("EULA"), pero algunos pueden requerir atención especial. Quisiéramos brindarle más detalles sobre la recolección de datos relacionada a la provisión de nuestros servicios. Prestamos diversos servicios descritos en el Acuerdo de licencia de usuario final (EULA) y la documentación del producto Para hacer que todo funcione, necesitamos recolectar 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.
- Funciones hash unidireccionales relativas a infiltraciones como parte del sistema de reputación de ESET LiveGrid®, que mejora la eficiencia de nuestras soluciones de protección frente a programas malignos comparando archivos analizados con una base de datos de elementos puestos en listas blancas y negras en la nube.
- Muestras y metadatos sospechosos de la circulación, parte del sistema de realimentación de ESET LiveGrid®, que permite a ESET reaccionar de forma inmediata ante las necesidades de sus usuarios finales y responder a las amenazas más recientes. Nosotros dependemos de que Usted nos envíe:
    - infiltraciones como muestras potenciales de virus y otros programas malignos y sospechosos; objetos problemáticos o potencialmente no deseados o inseguros, como archivos ejecutables, mensajes de correo electrónico que haya clasificado, como correo no deseado o que nuestro producto haya marcado;
    - 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 IP, URL y marcos de Ethernet;
    - archivos de volcado de memoria y la información que contienen.

No necesitamos recopilar datos por fuera de este ámbito. Sin embargo, en algunas ocasiones no podemos evitarlo. Los datos recopilados accidentalmente pueden incluirse como malware y Nosotros no pretendemos que sean parte de nuestros sistemas o procesarlos para el cumplimiento de los objetivos detallados en la presente Política de privacidad.

- Para fines de facturación, verificación de autenticidad de la licencia y prestación de nuestros servicios, se requiere información de licencia como identificación de licencia y datos personales, como nombre, apellido, dirección y dirección de correo electrónico.
- Pueden ser necesarios datos de contacto y datos contenidos en sus solicitudes de soporte para el servicio técnico. Basados en el medio que Usted eligió para comunicarse con Nosotros, podemos recopilar su correo electrónico, número de teléfono, datos de licencia, detalles del producto y descripción de su caso de asistencia. Podemos solicitarle que proporcione información adicional para facilitar la prestación del servicio de soporte.

Intercambio y confidencialidad de los datos

No compartimos sus datos con terceros. Sin embargo, ESET es una compañía que opera globalmente a través de entidades afiliadas o socios como parte de nuestra red de venta, servicio y soporte. La información sobre licencias, facturación y soporte técnico que procesa ESET puede ser transferida desde las entidades afiliadas o los socios o hacia ellos a fin de ejecutar el EULA, por ejemplo, para la prestación de servicios o soporte.

ESET prefiere procesar sus datos en la Unión Europea (UE). Sin embargo, según su ubicación (el uso de nuestros productos o servicios fuera de la UE) o el servicio que elija, puede que sea necesario transmitir sus datos a un país ubicado fuera de la UE. Por ejemplo, usamos servicios de terceros en conexión con la informática en la nube. En estos casos, seleccionamos cuidadosamente a nuestros proveedores de servicios y garantizamos un nivel adecuado de protección de los datos mediante medidas contractuales, técnicas y organizativas. Por regla general, pactamos las cláusulas contractuales estándar de la UE, si es necesario, con normas contractuales complementarias.

En el caso de algunos países fuera de la UE, como Reino Unido y Suiza, la UE ya ha determinado un nivel de protección de datos equivalente. Debido a este nivel de protección de datos equivalente, la transferencia de datos hacia estos países no requiere ninguna autorización ni acuerdo especial.

Derechos de la persona registrada

Los derechos de los Usuarios finales son importantes. Queremos informarle que cada Usuario final (de cualquier país, dentro y fuera de la Unión Europea) tiene los siguientes derechos, que ESET garantiza. Para ejercer los derechos de los interesados, puede comunicarse con nosotros a través del formulario de soporte o por correo electrónico a la siguiente dirección: dpo@eset.sk. A fin de poder identificarlo, le solicitamos la siguiente información: Nombre, dirección de correo electrónico y, de estar disponible, clave de licencia o número de cliente y empresa de afiliación. No debe enviarnos ningún otro dato personal, como la fecha de nacimiento. Queremos señalar que, para poder procesar su solicitud, así como con fines de identificación, procesaremos sus datos personales.

Derecho a retirar el consentimiento. El derecho a retirar el consentimiento resulta aplicable únicamente cuando nuestro procesamiento requiera su consentimiento. Si procesamos sus datos personales en razón de su consentimiento, tiene derecho a retirarlo en cualquier momento sin expresión de causa. Solo podrá retirar su consentimiento con efectos para el futuro, lo que no afectará la legitimidad de los datos procesados con anterioridad.

Derecho a oponerse. El derecho a oponerse al procesamiento resulta aplicable únicamente cuando nuestro procesamiento esté basado en el interés legítimo de ESET o un tercero. Si procesamos sus datos personales en pos de un interés legítimo, Usted, como interesado, tiene derecho a oponerse, en cualquier momento, al interés legítimo que designemos y al procesamiento de sus datos personales. Solo podrá oponerse al procesamiento con efectos para el futuro, lo que no afectará la legitimidad de los datos procesados con anterioridad. Si procesamos sus datos personales con fines de marketing directo, no es necesario que exprese los motivos de su objeción. Esto también se aplica a la elaboración de perfiles, ya que se relaciona con el marketing directo. En todos los demás casos, le solicitamos que nos informe, de forma breve, sus quejas en contra del interés legítimo de ESET para el procesamiento de sus datos personales.

Tenga en cuenta que, en algunos casos, a pesar de que haya retirado su consentimiento o el procesamiento de la objeción, tenemos derecho a continuar procesando sus datos personales en función de algún otro fundamento jurídico, por ejemplo, para el cumplimiento de un contrato.

Derecho de acceso. En carácter de interesado, Usted tiene derecho a obtener información de los datos que almacene ESET sobre usted de forma gratuita, en cualquier momento.

Derecho a solicitar una rectificación. En caso de que procesemos de forma involuntaria datos personales incorrectos sobre Usted, tiene derecho a que se corrija esta información.

Derecho de borrar. En carácter de interesado, Usted tiene derecho a solicitar el borrado de sus datos personales o una restricción en su procesamiento. Si procesamos sus datos personales, por ejemplo, con su consentimiento, Usted lo retira y no hay ningún otro fundamento jurídico (como un contrato), eliminaremos sus datos personales de inmediato. También eliminaremos sus datos personales en cuanto ya no sean necesarios para los fines indicados cuando finalice nuestro período de retención.

Derecho a la restricción del procesamiento. Si usamos sus datos personales únicamente con el fin de marketing directo y Usted ha retirado su consentimiento o se ha opuesto al interés legítimo subyacente de ESET, restringiremos el procesamiento de sus datos personales, lo que implicará que sus datos de contacto se incluyan en nuestra lista negra interna para evitar el contacto no solicitado. De lo contrario, sus datos personales serán eliminados.

Tenga en cuenta que podemos tener la obligación de almacenar sus datos hasta que finalicen los períodos y las obligaciones de retención determinados por el legislador o las autoridades supervisoras. La legislación eslovaca también podría determinar períodos y obligaciones de retención. A partir de su finalización, los datos correspondientes se eliminarán de forma rutinaria.

Derecho a la portabilidad de datos. Nos complace proporcionarle a Usted, en carácter de interesado, los datos personales que procese ESET en formato xls.

Derecho a presentar una queja. Como interesado, Usted tiene el derecho de presentar una queja a una autoridad supervisora en cualquier momento. ESET se encuentra sujeto a la regulación de las leyes eslovacas y Nosotros cumplimos con la ley de protección de datos como parte de la Unión Europea. La autoridad supervisora competente en materia de datos es la Oficina de Protección de Datos Personales de la República de Eslovaquia, con sede en Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Información de contacto

Si desea ejercer su derecho como persona registrada o tiene una consulta o preocupación, envíenos un mensaje a:

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