ESET ENDPOINT SECURITY

PARA ANDROID

Manual de instalación y Guía del usuario

Haga clic aquí para descargar la versión más reciente de este documento

Contenido

1. Instalación de ESET Endpoint Security...3
1.1 Instalación....3
1.2 Desinstalación....4
2. Activación del producto....4
3. Antivirus....4
4. USSD Control....6
5. Antispam....7
6. Anti-Theft....8
7. Auditoría de seguridad....9
8. Remote Administration....10
9. Actualización....11
10. Contraseña....11
11. Resolución de problemas y asistencia técnica....12
11.1 Resolución de problemas....12
11.2 Asistencia técnica....12

ESET **ENDPOINT SECURITY**

Servicio de atención al cliente: www.eset.com/support

REV. 17. 12. 2012

1. Instalación de ESET Endpoint Security

Para instalar ESET Endpoint Security en Android, el dispositivo móvil debe cumplir los siguientes requisitos del sistema:

	Requisitos mínimos del sistema
Sistema operativo	Android 2.1 (Eclair) y posterior
CPU	600 MHz
RAM	256 MB
Espacio libre para almacenamiento interno	5 MB

NOTA: algunas funciones (p. ej., Antispam y Anti-Theft) no están disponibles en tablets Android 3.0 que no admiten llamadas ni mensajes. Puede encontrar más información en este artículo de la base de conocimientos (puede que no esté disponible en su idioma).

1.1 Instalación

Utilice uno de los métodos siguientes para instalar ESET Endpoint Security:

- Descargue el archivo de instalación de ESET Endpoint Security *(ees.apk)* desde el sitio web de ESET escaneando el código QR siguiente con una aplicación como QR Droid o Barcode Scanner:

- Descargue el archivo *ees.apk* en su ordenador desde el sitio web de ESET. Copie el archivo en su dispositivo por Bluetooth o USB. Toque en el icono de inicio en la pantalla de inicio de Android, o vaya a **Inicio** > **Menú** y toque en **Ajustes** > **Aplicaciones.** Asegúrese de que haya seleccionado la opción **Orígenes desconocidos**. Localice el archivo *ees.apk* mediante una aplicación similar a ASTRO File Manager o ES File Explorer. Abra el archivo y toque en **Instalar**. Una vez instalada la aplicación, toque en **Abrir**.

- Si desea instalar y activar ESET Endpoint Security en varios dispositivos, cree un archivo de configuración xml en ESET Configuration Editor.

  Abra ESET Configuration Editor bien desde ERA Console (**Herramientas** > ESET Configuration Editor) o bien haciendo clic en **Inicio** > **Todos los programas** > **ESET** > ESET Remote Administrator **Console >** ESET Configuration Editor. En el árbol de la izquierda, seleccione **Dispositivos móviles** > **Endpoint Security para Android** > **Actualizar** > **Configuración** > **Nombre de usuario**. Introduzca su nombre de usuario (datos de la licencia recibidos de ESET después de adquirir el producto) en el campo **Valor** a la derecha y haga clic en **Siguiente**. Haga clic en **Establecer contraseña** y vuelva a introducir la contraseña. Haga clic en **Aceptar** para confirmar. También puede definir otros ajustes de configuración (como Administración remota o Antivirus) que desee aplicar a todos los dispositivos móviles con ESET Configuration Editor. Cuando haya terminado de realizar cambios, haga clic en **Archivo** > **Guardar** (o pulse Ctrl+S) y guarde el archivo como *settings.xml*.

  Copie el archivo que acaba de guardar en la carpeta raíz de la tarjeta SD *(/mnt/sdcard)* junto con el archivo de instalación *ees.apk* de ESET Endpoint Security (disponible aquí). Abra el archivo *ees.apk* mediante una aplicación similar a ASTRO File Manager o ES File Explorer y pulse **Instalar**. Cuando finalice la instalación, toque en **Abrir**. ESET Endpoint Security se activará automáticamente con el nombre de usuario y la contraseña guardados en el archivo *settings.xml*.

Advertencia: ESET Endpoint Security debe instalarse en el almacenamiento interno del dispositivo. Algunos teléfonos permiten que los usuarios instalen aplicaciones en la tarjeta SD. Si instala ESET Endpoint Security en la tarjeta SD, no funcionarán las características Protección en tiempo real, Antispam ni Anti-Theft.

Una vez que la instalación se haya realizado correctamente, active ESET Endpoint Security siguiendo los pasos que se describen en la sección Activación del producto 4.

1.2 Desinstalación

Para desinstalar ESET Endpoint Security del dispositivo, utilice el **Asistente de desinstalación**, al que se puede acceder desde el menú principal de ESET Endpoint Security, o siga estos pasos:

1. Toque en el icono de inicio en la pantalla de inicio de Android (o vaya a **Inicio** > **Menú**) y toque en **Ajustes** > **Ubicación y seguridad** > **Seleccionar administradores del dispositivo**, anule la selección de **ESET Security** y toque en **Desactivar**. Cuando se le solicite, escriba su contraseña de ESET Endpoint Security. (Si no ha establecido ESET Endpoint Security como Administrador de dispositivos, omita este paso.)
2. Vuelva a **Ajustes** y toque en **Aplicaciones** > **Administrar aplicaciones** > **ESET Security** > **Desinstalar**.

ESET Endpoint Security y la carpeta de cuarentena se eliminarán definitivamente del dispositivo móvil.

2. Activación del producto

Una vez que la instalación se haya realizado correctamente, es necesario activar ESET Endpoint Security. Toque en **Activar ahora** en el menú principal de ESET Endpoint Security.

Activar utilizando un Nombre de usuario y Contraseña: introduzca el nombre de usuario y la contraseña (datos de la licencia recibidos de ESET después de la adquisición del producto) en los campos correspondientes.

La activación es válida durante un período de tiempo fijo. Una vez la activación expire, se le pedirá que renueve la licencia del programa (el programa le informará al respecto de forma anticipada).

NOTA: durante la activación, el dispositivo debe estar conectado a Internet ya que se descargará una pequeña cantidad de datos.

De forma predeterminada, ESET Endpoint Security se instala con el idioma que su teléfono tiene establecido como configuración regional del sistema (dentro de la configuración del idioma y del teclado). Para cambiar el idioma de la interfaz de usuario de la aplicación, toque en **Idioma** en el menú principal de ESET Endpoint Security y seleccione el idioma que desee.

3. Antivirus

Analizar dispositivo

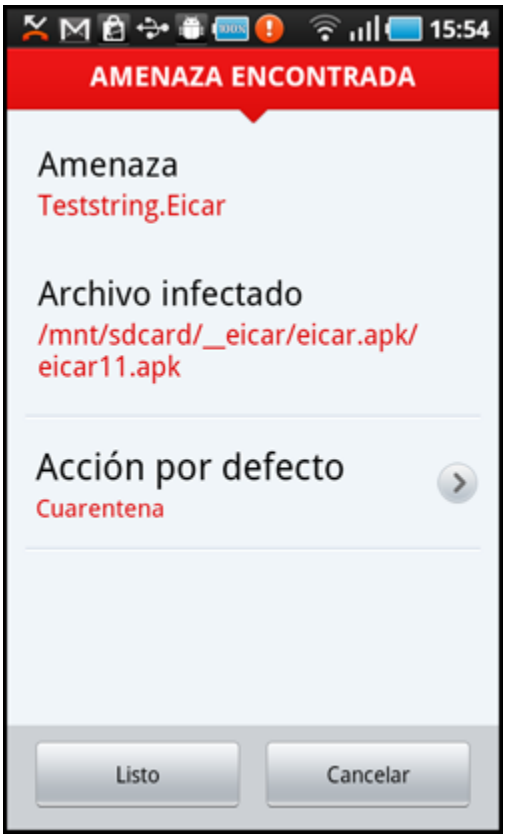
La opción **Analizar dispositivo** se puede utilizar para comprobar si hay amenazas en su dispositivo móvil.

Algunos tipos de archivos predefinidos se analizan de forma predeterminada. Un análisis completo del dispositivo comprueba la memoria, los procesos en ejecución, sus bibliotecas de vínculos dinámicos dependientes y los archivos que forman parte del almacenamiento interno y extraíble. Finalizado el análisis se muestra un resumen corto de los resultados (número de archivos infectados, número de archivos analizados, duración del análisis, etc.).

Para anular un análisis en curso, toque en **Cancelar**.

Analizar carpeta

Para analizar determinadas carpetas del dispositivo, toque en **Analizar carpeta**. Busque las carpetas que desee analizar, toque en sus casillas de verificación en la columna derecha y toque en **Analizar**.



Amenaza detectada por ESET Endpoint Security

Analizar registros

La sección **Analizar registros** contiene registros que proporcionan información completa acerca de las tareas de análisis realizadas. Los registros se crean después de cada análisis activado manualmente (a petición) o cuando se detecta una amenaza durante el análisis en tiempo real.

Cada registro contiene:

- fecha y hora del suceso.
- número de archivos analizados.
- número de archivos infectados.
- nombre de la ruta de acceso completa de los archivos infectados.
- duración del análisis.
- acción realizada o errores detectados durante el análisis.

Cuarentena

La tarea principal de la cuarentena es almacenar los archivos infectados de forma segura. Los archivos deben ponerse en cuarentena si no es posible desinfectarlos, si no es seguro ni aconsejable eliminarlos o si ESET Endpoint Security los detecta incorrectamente como infectados.

Los archivos almacenados en la cuarentena se pueden ver en un registro que muestra el nombre y la ubicación original del archivo infectado, así como la fecha y la hora de la cuarentena.

Si desea restaurar un archivo en cuarentena a su ubicación original, toque en el archivo y seleccione **Restaurar**. No se recomienda esta opción.

Para eliminar definitivamente un archivo en cuarentena del dispositivo, toque en el archivo y seleccione **Eliminar**. Para eliminar todos los archivos almacenados en la cuarentena, pulse el botón **MENÚ** y toque en **Quitar todo**.

Configuración

La opción **A petición** le permite modificar los parámetros de análisis de un análisis activado manualmente (a petición).

La opción **Mostrar aviso de alerta** muestra las notificaciones de alerta de amenaza cada vez que el análisis a petición detecta una nueva amenaza.

Si desea analizar todas las aplicaciones (archivos *.apk*) instaladas en el dispositivo, seleccione la opción **Analizar aplicaciones**.

Protección proactiva es un método de detección basado en algoritmos que analiza el código y busca comportamientos habituales de los virus. Su ventaja principal es la capacidad de identificar software malicioso sin reconocer aún en la base de datos actual de firmas de virus. Si está activada la protección proactiva, se necesitará tiempo adicional para realizar el análisis.

La opción **Profundidad del análisis de archivos** le permite especificar la profundidad de los archivos anidados (archivos *.zip*) que se van a analizar. Cuanto más alto es el número, más profundo es el análisis.

La opción **Registros almacenados** le permite definir el número máximo de registros que se almacenarán en la sección **Analizar registros** 5.

Puede especificar una **Acción por defecto** que se realice automáticamente cuando se detecten archivos infectados. Puede definir las siguientes acciones como acciones por defecto:

- **Ignorar**: no se realizará acción alguna sobre el archivo infectado (no se recomienda esta opción).
- **Eliminar**: el archivo infectado se eliminará.
- **Cuarentena**: (por defecto) el archivo infectado se moverá a la **Cuarentena** 5.

La opción **Extensiones** muestra los tipos de archivos más comunes expuestos a amenazas en la plataforma Android. Seleccione los tipos de archivos que desea analizar o anule la selección de la extensiones para excluirlos del análisis. Esta configuración se aplica tanto al análisis a petición como al análisis en tiempo real:

- **Sensible a las extensiones**: si selecciona esta opción, solo se analizarán los archivos con las extensiones especificadas, lo que hará que los análisis se realicen más rápidamente. Recomendamos desactivar esta función de vez en cuando para que ESET Endpoint Security realice análisis para detectar cualquier tipo de amenaza posible, incluidas las amenazas ocultas por extensiones de archivo falsas.
- **DEX (archivo de código de aplicaciones)**: formato de archivo ejecutable que contiene código compilado escrito para el sistema operativo Android.
- **SO (bibliotecas)**: bibliotecas compartidas guardadas en lugares designados en el sistema de archivos y vinculadas mediante programas que requieren sus funciones.
- **Archivos (archivos comprimidos)**: archivos comprimidos con la compresión Zip.
- **Otros**: otros tipos de archivos conocidos.

En la opción **Tiempo real**, puede configurar los parámetros de análisis del análisis al acceder. El análisis al acceder comprueba los archivos con los que interactúa en tiempo real. Analiza automáticamente la carpeta *Descarga* en la tarjeta SD, los archivos de los archivos de instalación *.apk* y los archivos de la tarjeta SD una vez conectada (si está activada la opción **Analizar tarjeta SD conectada**). El análisis al acceder se inicia automáticamente al inicio del sistema.

- **Protección en tiempo real**: si está activada (por defecto), el análisis al acceder se ejecuta en segundo plano.
- **Mostrar aviso de alerta**: muestra las notificaciones de alerta de amenaza cada vez que el análisis al acceder detecta una nueva amenaza.
- **Analizar tarjeta SD conectada**: analiza los archivos antes de abrirlos o guardarlos en la tarjeta SD.
- **Protección proactiva**: seleccione esta opción para aplicar técnicas de análisis heurísticas. La heurística identifica de forma proactiva nuevo malware no detectado aún por la base de datos de firmas de virus mediante el análisis del código y el reconocimiento del comportamiento habitual de los virus. Si está activada la protección proactiva, se necesitará tiempo adicional para realizar el análisis.
- **Profundidad del análisis de archivos**: esta opción le permite especificar la profundidad de los archivos anidados (archivos *.zip*) que se van a analizar. Cuanto más alto es el número, más profundo es el análisis.
- **Acción por defecto**: puede especificar una acción por defecto que se realice automáticamente cuando el análisis al acceder detecte archivos infectados. Si selecciona **Ignorar**, no se realizará acción alguna sobre el archivo infectado (no se recomienda esta opción). Si selecciona **Eliminar**, el archivo infectado se eliminará. Si selecciona**Cuarentena**, el archivo infectado se moverá a la **Cuarentena** 5.

ESET Endpoint Security muestra su icono de notificación  en la esquina superior izquierda de la pantalla (barra de estado de Android). Si no quiere que aparezca este icono, vaya al menú principal de ESET Endpoint Security, pulse el botón **MENÚ**, toque en **Configuración de notificaciones** y anule la selección de **Mostrar icono de la notificación**. Tenga en cuenta que esto no desactivará un icono de advertencia rojo con un signo de exclamación que informa acerca de un riesgo para la seguridad (p. ej., Análisis de virus en tiempo real desactivado, Comprobación de SIM desactivada, etc.).

4. USSD Control

La última versión de ESET Endpoint Security (1.2.103 y posterior) protege su dispositivo Android del borrado remoto y otros ataques USSD. Los códigos USSD (Unstructured Supplementary Service Data) se pueden ejecutar mediante mensajes de texto maliciosos, códigos QR o vínculos URL.

Si recibe una notificación de que hay una nueva versión de ESET Endpoint Security disponible para su descarga, ESET le recomienda que la instale lo antes posible.

No es posible acceder a USSD Control desde el menú principal, ya que se ejecuta en segundo plano y solo le avisa cuando se inicia un comando USSD. Para comprobar la vulnerabilidad de USSD de su dispositivo de forma segura, siga las instrucciones descritas en los pasos 4-6 de este artículo de la base de conocimientos.

5. Antispam

El módulo **Antispam** bloquea los mensajes SMS/MMS entrantes y las llamadas entrantes y salientes de acuerdo con unas reglas especificadas.

Los mensajes no solicitados incluyen anuncios de los proveedores de servicios de telefonía móvil o mensajes procedentes de usuarios desconocidos o sin especificar. El término *bloquear contactos* hace referencia a mover automáticamente un mensaje entrante a la sección **Registros de spam** 7. Cuando se bloquea un mensaje entrante, no se muestra notificación alguna. Esto tiene como ventaja que no se le molestará con información no solicitada, pero siempre puede comprobar los registros para ver si hay mensajes que se puedan haber bloqueado por error.

Para añadir una nueva regla de antispam, toque **Lista de reglas de llamadas y SMS** > **Agregar nueva**. Escriba el número de teléfono que desea bloquear o toque en el botón **+** para elegir el número de la lista de contactos. Personalice la regla permitiendo o bloqueando los mensajes y las llamadas; a continuación, toque en **Listo** .

Para editar o eliminar una entrada de regla existente, toque y mantenga presionada la entrada y, a continuación, elija la acción deseada. Si desea eliminar todas las reglas de antispam, pulse el botón **MENÚ** y toque en **Quitar todo**.

NOTA: el número de teléfono debe incluir el código de marcado internacional seguido del número real (p. ej., +16101001OO).

Lista de reglas del antispam

Configuración

Bloquear llamadas anónimas: active esta opción si desea bloquear a las personas que llaman cuyo número de teléfono se haya ocultado intencionadamente a través del servicio de restricción de identificación del número llamante (CLIR, Calling Line Identification Restriction).

Bloquear contactos conocidos: utilice esta opción para bloquear los mensajes y las llamadas de los contactos incluidos en la lista de contactos.

Bloquear contactos desconocidos: bloquea los mensajes y las llamadas de los contactos no incluidos en la lista de contactos. Puede utilizar esta opción para bloquear las llamadas telefónicas indeseadas (p. ej., "llamadas de venta") o para evitar que los niños marquen números desconocidos (para ello, se recomienda proteger con **contraseña** 11 la configuración del antispam).

En la sección **Registros de spam**, puede ver las llamadas y los mensajes bloqueados por el módulo Antispam. Cada registro contiene el nombre del evento, el número de teléfono correspondiente y la fecha y hora del evento. Los mensajes SMS bloqueados también contienen el cuerpo del mensaje.

6. Anti-Theft

La característica **Anti-Theft** protege el teléfono móvil del acceso no autorizado.

Si pierde el teléfono o alguien se lo roba y sustituye la tarjeta SIM por una nueva (que no sea de confianza), ESET Endpoint Security bloqueará el teléfono automáticamente. Se enviará un SMS de alerta a los números de teléfono definidos por el usuario. Este mensaje incluirá el número de teléfono de la tarjeta SIM actualmente insertada, el número IMSI (International Mobile Subscriber Identity) y el número de IMEI (International Mobile Equipment Identity) del teléfono. El usuario no autorizado no sabrá que este mensaje se ha enviado, puesto que se eliminará automáticamente de los hilos de **Mensajes**. También puede solicitar las coordenadas GPS del teléfono móvil perdido o borrar de forma remota todos los datos almacenados en el dispositivo.

Tarjetas SIM de confianza

Esta funcionalidad no está disponible en los dispositivos que no tienen tarjeta SIM (tablets y teléfonos CDMA).

Si la tarjeta SIM actualmente insertada en el teléfono móvil es la que desea guardar como de confianza, toque en el botón **Agregar**. Si utiliza más de una tarjeta SIM, puede que desee distinguirlas modificando su **Alias para la tarjeta SIM** (p. ej., *Trabajo*, *Casa* etc.).

Para editar o quitar una entrada de SIM existente, toque y mantenga presionada la entrada y, a continuación, elija **Editar** o **Quitar**. Si desea eliminar todas las entradas de la lista, pulse el botón **MENÚ** y toque en **Quitar todo**.

Contactos de administración

En la lista **Contactos de administración**, toque en **Agregar** para agregar los números de teléfono que recibirán un SMS de alerta cuando se inserte en el dispositivo una tarjeta SIM que no sea de confianza. Escriba un nombre en el campo **Nombre del contacto** y su número de teléfono en el campo **Número de teléfono**, o toque en el botón **+** para seleccionar el contacto de la lista de contactos. Si el contacto contiene más de un número de teléfono, se enviará un SMS de alerta a todos esos números.

Para editar o quitar una entrada existente, toque y mantenga presionada la entrada y, a continuación, elija **Editar** o **Quitar**. Si desea eliminar todas las entradas de la lista, pulse el botón **MENÚ** y toque en **Quitar todo**.

NOTA: el número de teléfono debe incluir el código de marcado internacional seguido del número real (p. ej., +16101001OO).

Configuración

Si no desea usar la comprobación de SIM, seleccione la opción **Ignorar comprobación de la SIM**. Esto desactivará las advertencias rojas *¡Riesgo de seguridad!* (*La comprobación de la SIM está desactivada* y *No se ha definido ninguna tarjeta SIM de confianza*) en el menú principal de ESET Endpoint Security. La opción Ignorar comprobación de la SIM aparece atenuada en los dispositivos CDMA.

Para activar la comprobación automática de la tarjeta SIM insertada (y el envío de SMS de alerta), seleccione la opción **Activar la comprobación de la SIM**.

En el campo **Texto de alerta SMS** puede modificar el mensaje de texto que se enviará a los números de teléfono predefinidos tras insertarse en el dispositivo una tarjeta SIM que no sea de confianza. También puede introducir otra cuenta de correo o bien un número de contacto alternativo.

Comandos SMS

Los comandos SMS remotos (wipe, lock y find) solo funcionan si está seleccionada la opción **Activar comandos SMS**.

La opción **Activar el reinicio de contraseña vía SMS** le permite restablecer la contraseña de seguridad mediante el envío de un mensaje SMS desde el móvil guardado en los **Contactos de administración** a su número de móvil. Este SMS debe tener el siguiente formato:
eset remote reset

Si pierde el teléfono y le gustaría bloquearlo, envíe un SMS de bloqueo remoto desde cualquier dispositivo móvil a su número de teléfono en el siguiente formato:
eset lock contraseña
Sustituya *contraseña* por su propia contraseña definida en la sección **Contraseña** 11. Los usuarios no autorizados no podrán usar su teléfono dado que se les pedirá que escriban su contraseña.

Si desea solicitar las coordenadas GPS de su teléfono móvil, envíe un SMS de búsqueda remota a su número de móvil o al número de móvil del usuario no autorizado (depende de si la tarjeta SIM ya se ha sustituido):
eset find contraseña
Recibirá un SMS con las coordenadas GPS junto con un vínculo a los mapas de Google con la ubicación exacta de su teléfono móvil. Tenga en cuenta que para recibir las coordenadas GPS, el módulo GPS del teléfono tiene que estar activado de forma anticipada.

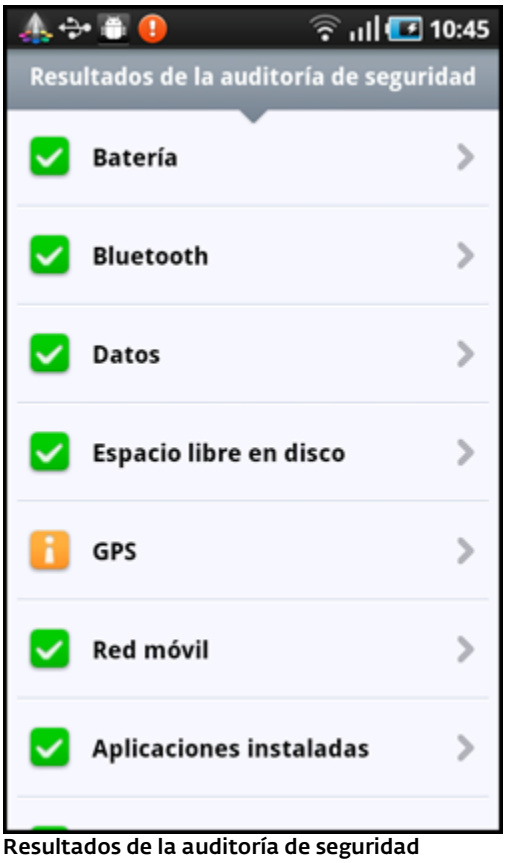
Si desea borrar todos los datos almacenados en el dispositivo y todos los soportes extraíbles actualmente insertados, envíe un SMS de borrado remoto:
eset wipe contraseña
Todos los contactos, mensajes, correos electrónicos, aplicaciones instaladas, su cuenta de Google y el contenido de la tarjeta SD se eliminarán definitivamente del dispositivo. Si ESET Endpoint Security no está establecido como Administrador de dispositivos, solo se borrarán los contactos, los mensajes y el contenido de la tarjeta SD.

NOTA: el campo de contraseña distingue entre mayúsculas y minúsculas. Asegúrese de escribir la contraseña exactamente como la ha definido en la sección Contraseña.

7. Auditoría de seguridad

La **Auditoría de seguridad** comprueba el estado del teléfono respecto a nivel de batería, estado de Bluetooth, espacio libre en disco, etc.

Para ejecutar la auditoría de seguridad manualmente, toque en **Auditar**. Se muestra un informe detallado.



Resultados de la auditoría de seguridad

Una marca de verificación verde junto a cada elemento indica que el valor se encuentra por encima del umbral o que el elemento no representa un riesgo para la seguridad.

Un icono amarillo significa que al menos uno de los elementos se encuentra por debajo del umbral o que el elemento puede representar un posible riesgo para la seguridad. Toque en el elemento para ver detalles de los resultados.

Un signo de exclamación rojo indica que el elemento está por debajo del umbral o que el elemento representa un riesgo para la seguridad y debe repararse.

Si desea corregir el estado del elemento resaltado en rojo, toque en el elemento y confirme tocando en **Sí**.

Configuración

Por defecto, la auditoría de seguridad está programada para ejecutarse periódicamente cada 24 horas. Si desea desactivar las auditorías periódicas, anule la selección de la opción **Auditar periódicamente**.

Si la opción **Reparar automáticamente** está activada, ESET Endpoint Security intentará corregir automáticamente los elementos en riesgo (p. ej., el estado de Bluetooth) sin la intervención del usuario. Esta opción solo se aplica a una auditoría periódica (programada).

La opción **Registros almacenados** le permite definir el número máximo de registros que se almacenarán en la sección **Registros de auditoría**.

La opción **Período de auditoría** le permite definir la frecuencia con que se realizará la auditoría periódica (programada).

Para ajustar el valor del límite en el que el espacio en disco disponible y el nivel de batería se consideran bajos, utilice las opciones **Límite de espacio libre en disco** y **Límite del nivel de batería**.

En la pestaña **Elementos que auditar**, seleccione los elementos que se comprobarán durante la auditoría periódica (programada).

La sección **Registros de auditoría** contiene registros que proporcionan información completa acerca de las auditorías activadas manualmente y periódicas realizadas. Cada registro contiene la fecha y la hora del suceso y resultados detallados de cada elemento.

El **Administrador de tareas** proporciona una visión general de todos los procesos, servicios y tareas que se ejecutan en su dispositivo. ESET Endpoint Security le permite detener los procesos, servicios y tareas que no ejecute el sistema. Estos se indica con un icono rojo (**x**).

8. Remote Administration

ESET Remote Administrator (ERA) permite gestionar ESET Endpoint Security en un entorno de red directamente desde una ubicación central.

Los administradores pueden realizar las siguientes acciones de forma remota:

- Crear una tarea de configuración remota en ERA y enviar los ajustes a ESET Endpoint Security.
- Activar un análisis a petición.
- Instalar actualizaciones de la base de datos de firmas de virus.
- Comprobar los archivos de registro.
- Enviar mensajes de administración a dispositivos móviles.

El uso de ERA no solo aumenta el nivel de seguridad, sino que además facilita la administración de todos los productos de ESET instalados en estaciones de trabajo cliente y dispositivos móviles. Los dispositivos móviles que tienen ESET Endpoint Security pueden conectarse a ERA mediante cualquier tipo de conexión a Internet — LAN, WLAN, red de móvil (3G, HSDPA, GPRS), etc.—, siempre que sea una conexión normal (sin un proxy, cortafuegos, etc.) y ambos puntos finales estén configurados correctamente. Cuando se realiza la conexión a ERA mediante una red móvil, el éxito de la conexión depende del proveedor de GSM y se requiere una conexión a Internet completa. Por ejemplo, si solo se permite la navegación web a través de HTTP con el puerto 8O, la conexión fallará porque el puerto 2222 es necesario para la comunicación con el servidor ERA.

Configuración

El menú principal de ESET Endpoint Security incluye opciones de configuración de administración remota. Toque en **Remote Administration** > **Ajustes**.

Active la administración remota seleccionando la opción **Conectar con el servidor de ESET Remote Administration**.

Intervalo entre conexiones al servidor: esta opción indica con qué frecuencia ESET Endpoint Security tratará de conectarse a ERA Server para enviar los datos.

Servidor principal, **Servidor secundario**: por lo general, solo es necesario configurar el servidor principal. Si está ejecutando varios servidores ERA en la red, puede optar por añadir una conexión ERA Server secundaria. Servirá como solución de reserva. Si no es posible acceder al servidor principal, ESET Endpoint Security tratará de contactar de forma automática con el ERA Server secundario. Al mismo tiempo, tratará de restablecer la conexión con el servidor principal. Una vez que esté activa la conexión, ESET Endpoint Security cambiará al servidor principal. La configuración de dos perfiles de servidor de administración remota es más apropiada para clientes que se conectan tanto desde la red local como desde fuera de la red.

Dirección del servidor: especifique el nombre DNS o la dirección IP del servidor que esté ejecutando ERA Server.

Puerto: este campo contiene un puerto de servidor predefinido que se utiliza para la conexión. Recomendamos que deje ajustado el puerto predeterminado como 2222.

Si ESET Remote Administrator requiere autenticación mediante contraseña, seleccione la opción **El servidor de Remote Administrator requiere autenticación** e introduzca su contraseña en el campo **Contraseña**.

NOTA: Para obtener más orientación sobre cómo gestionar su red con ESET Remote Administrator, consulte el Manual de instalación y Guía del usuario de ESET Remote Administrator (este documento puede no estar disponible en su idioma).

9. Actualización

ESET Endpoint Security se puede actualizar fácilmente con la última versión del producto para garantizar la protección del dispositivo móvil frente a las últimas amenazas y ataques maliciosos. Si recibe una notificación de que hay una nueva versión de ESET Endpoint Security disponible para su descarga, ESET le recomienda que la instale lo antes posible.

Por defecto, ESET Endpoint Security se instala con una tarea de actualización para garantizar que el programa se actualice periódicamente. Para ejecutar la actualización manualmente, toque en **Actualizar ahora**.

Configuración

La opción **Actualización automática** le permite definir el intervalo de tiempo para la descarga automática de las actualizaciones de la base de datos de virus.

NOTA: para evitar el uso innecesario de ancho de banda, las actualizaciones se emiten en caso necesario, cuando se agrega una nueva amenaza. Aunque las actualizaciones se incluyen de forma gratuita con la licencia activa, puede que el proveedor de servicios de telefonía móvil le cobre las transferencias de datos.

10. Contraseña

La contraseña de seguridad protege la configuración frente a los cambios no autorizados. La contraseña es necesaria en los siguientes casos:

- Para acceder a características protegidas con contraseña de ESET Endpoint Security (Antivirus, Antispam, Anti-Theft y Auditoría de seguridad).
- Para acceder al teléfono cuando está bloqueado.
- Para enviar comandos SMS al dispositivo.
- Para desinstalar ESET Endpoint Security.

NOTA: La protección frente a la desinstalación solo está disponible en Android 2.2 y posterior.

Para definir una nueva contraseña de seguridad, escríbala en los campos **Contraseña** y **Vuelva a escribir la contraseña**. La opción **Frase recordatoria** (si está establecida) muestra una sugerencia en caso de que no recuerde la contraseña.

IMPORTANTE: Proceda con cuidado cuando elija su contraseña ya que se le pedirá para desbloquear el dispositivo o desinstalar ESET Endpoint Security.

En la pestaña **Aplicar a**, puede especificar los módulos que estarán protegidos por la contraseña.

Si olvida la contraseña, puede enviar un SMS desde el número de móvil guardado en la lista **Contactos de administración** a su número de móvil. Este SMS debe tener el siguiente formato:
eset remote reset
Se restablecerá su contraseña.

11. Resolución de problemas y asistencia técnica

11.1 Resolución de problemas

ESET Endpoint Security proporciona una funcionalidad de registro avanzada que ayuda a diagnosticar posibles problemas técnicos. Antes de ponerse en contacto con el servicio de atención al cliente de ESET, le recomendamos encarecidamente que busque una posible solución a su problema en la base de conocimientos de ESET. Si aun así necesita ponerse en contacto con el servicio de atención al cliente de ESET, siga los pasos siguientes:

1. Vaya al menú principal de ESET Endpoint Security, pulse el botón **MENÚ** y toque en **Configuración de inicio de sesión**.
2. Seleccione un componente de programa adecuado con el que esté relacionado el problema.
3. Reproduzca el problema. La información se debe escribir dentro de un archivo de registro de la aplicación.
4. Vaya al menú principal de ESET Endpoint Security, pulse el botón **MENÚ** y toque en **Atención al cliente**.
5. Si no encuentra una solución en nuestra base de conocimientos, toque en **Continuar**.
6. Rellene toda la información y pulse **Enviar** en la parte inferior de la pantalla. Asegúrese de que la opción **Registro de la aplicación** esté seleccionada (lo está de forma predeterminada).

11.2 Asistencia técnica

Nuestros especialistas del servicio de atención al cliente están disponibles para proporcionarle ayuda con aspectos administrativos y asistencia técnica relacionada con ESET Endpoint Security o con cualquier otro producto de ESET.

Para encontrar respuestas a las preguntas más frecuentes, acceda a la base de conocimientos de ESET en:
http://kb.eset.com/android

La base de conocimientos contiene abundante información útil para resolver la mayoría de los problemas más comunes, con acceso fácil por categorías o mediante una herramienta de búsqueda avanzada.

Para ponerse en contacto con el servicio de atención al cliente de ESET, utilice el formulario de solicitud de asistencia disponible en:
http://eset.com/support/contact

Para solicitar asistencia directamente desde el teléfono móvil, vaya al menú principal de ESET Endpoint Security, pulse el botón **MENÚ** y toque en **Atención al cliente**. Rellene todos los campos obligatorios. Para incluir un **registro de la aplicación** completo, siga los pasos que se describen en la secciónResolución de problemas 12.