ESET Endpoint Antivirus

Manual de usuario

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

ESET Endpoint Antivirus está 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

ESET Endpoint Antivirus

ESET Endpoint Antivirus representa un nuevo enfoque de la seguridad informática realmente integrada. La versión más reciente del motor de análisis ESET LiveGrid® garantiza la protección del ordenador gracias a su velocidad y precisión. Estas características lo convierten en un sistema inteligente que está constantemente en alerta frente a ataques y software malintencionado que puedan poner en peligro su ordenador.

ESET Endpoint Antivirus es una solución de seguridad integral que nació tras un gran esfuerzo por combinar el nivel máximo de protección con un impacto mínimo en el sistema. Las tecnologías avanzadas basadas en la inteligencia artificial son capaces de eliminar de forma proactiva la infiltración de virus, spyware, troyanos, gusanos, adware, rootkits y otros ataques que albergan en Internet sin dificultar el rendimiento del sistema ni interrumpir la actividad del ordenador.

ESET Endpoint Antivirus está diseñado principalmente para utilizarlo en estaciones de trabajo en empresas.

En la sección Instalación, los temas de ayuda se dividen en varios capítulos y subcapítulos con el fin de facilitar la orientación y la contextualización. Puede encontrar, por ejemplo, información relacionada con la Descarga, la Instalación y la Activación.

El uso de ESET Endpoint Antivirus con ESET PROTECT en un entorno empresarial le permitirá administrar fácilmente cualquier número de estaciones de trabajo cliente, aplicar políticas y reglas, controlar amenazas detectadas y configurar clientes de forma remota desde cualquier ordenador en red.

El capítulo Preguntas habituales abarca algunas de las preguntas más frecuentes y los problemas encontrados.

Características y ventajas

Interfaz de usuario rediseñada	La interfaz de usuario de esta versión se ha rediseñado y simplificado considerablemente en función de los resultados de las pruebas de usabilidad. Todos los textos y notificaciones de la GUI se han revisado cuidadosamente y la interfaz facilita actualmente asistencia para idiomas con escritura de derecha a izquierda, como hebreo y árabe. Se integra Ayuda en línea en ESET Endpoint Antivirus y ofrece contenido de asistencia actualizado dinámicamente.
Modo oscuro	Una extensión que le ayuda a cambiar rápidamente la pantalla a un tema oscuro. Puede elegir su esquema de colores preferido en Elementos de la interfaz de usuario.
Antivirus y antispyware	Detecta y desinfecta de forma proactiva más virus, gusanos, troyanos y rootkits, conocidos o no. La Heurística avanzada detecta incluso el código malicioso nunca visto hasta el momento, protegiéndole de amenazas desconocidas y neutralizándolas antes de que causen daños. La protección del tráfico de Internet y el Antiphishing funcionan supervisando la comunicación entre navegadores web y servidores remotos (incluido SSL). La protección del cliente de correo electrónico proporciona control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3(S) e IMAP(S).
Actualizaciones periódicas	La mejor manera de disfrutar del máximo nivel de seguridad en el ordenador es actualizar el motor de detección (anteriormente conocida como la "base de firmas de virus") y los módulos del programa de forma periódica.
ESET LiveGrid® (Reputación basada en la nube)	Puede comprobar la reputación de los procesos en ejecución y los archivos directamente desde ESET Endpoint Antivirus.

Administración remota	ESET PROTECT le permite administrar productos ESET en estaciones de trabajo, servidores y dispositivos móviles en un entorno de red desde una ubicación central. Con ESET PROTECT Consola Web (ESET PROTECT Consola Web) podrá implementar soluciones de ESET, administrar tareas, aplicar políticas de seguridad, supervisar el estado del sistema y responder rápidamente a problemas o amenazas que se produzcan en ordenadores remotos.
Protección contra ataques en la red	Analiza el contenido del tráfico de red y le protege contra posibles ataques de red. Se bloqueará todo el tráfico que se considere dañino.
Control de acceso web (solo ESET Endpoint Security)	Control de acceso web le permite bloquear las páginas web que puedan contener material que podría resultar ofensivo. Asimismo, los empleados o administradores del sistema pueden prohibir el acceso a más de 27 categorías de sitios web predefinidas y más de 140 subcategorías.

Novedades

Novedades de la versión 11 de ESET Endpoint Antivirus

Gestión de parches y vulnerabilidades

Función disponible en ESET PROTECT Cloud que analiza periódicamente una estación de trabajo para detectar cualquier software instalado vulnerable a riesgos de seguridad. La administración de revisiones comprueba el espacio disponible antes de iniciar la descarga (el valor predeterminado y mínimo es 2 GB) y ayuda a corregir estos riesgos con actualizaciones de software automatizadas, que garantizan mayor seguridad para los dispositivos.

Estados de los productos al fin de la vida útil

ESET Endpoint Antivirus en esta versión puede mostrar diferentes estados de los productos al fin de la vida útil. Puede configurar los estados de fin de la vida útil en Notificaciones.

Varias correcciones de errores y mejoras del rendimiento

Requisitos del sistema

Para un funcionamiento óptimo de ESET Endpoint Antivirus, el sistema debería cumplir con los siguientes requisitos de hardware y software (configuración predeterminada del producto):

Procesadores compatibles

Procesador Intel o AMD, de 32 bits (x86) con conjunto de instrucciones SSE2 o de 64 bits (x64), 1 GHz o más procesador de tipo ARM64, 1 GHz o superior

Sistemas operativos

Microsoft® Windows® 11

Microsoft® Windows® 10

Para obtener una lista detallada de las versiones compatibles con Microsoft® Windows® 10 y Microsoft® Windows® 11, consulte la política de compatibilidad con el sistema operativo Windows.

Intente siempre mantener actualizado su sistema operativo.

La compatibilidad con Azure Code Signing debe estar instalada en todos los sistemas operativos Windows para instalar o actualizar los productos ESET publicados a partir de julio de 2023. Más información.

Requisitos de las funciones de ESET Endpoint Antivirus

Consulte los requisitos del sistema para funciones de ESET Endpoint Antivirus concretas en la tabla que aparece a continuación:

Característica	Requisitos
Intel® Threat Detection Technology	Consulte los procesadores compatibles.
Limpiador especializado	Procesador que no está basado en ARM64.
Bloqueador de exploits	Procesador que no está basado en ARM64.
Análisis profundo de inspección de comportamiento	Procesador que no está basado en ARM64.

El instalador de ESET Endpoint Antivirus creado en ESET PROTECT es compatible con Windows 10 Enterprise para escritorios virtuales y el modo multisesión de Windows 10.

Otros

- Se cumplen los requisitos del sistema operativo y del resto de software instalado en el ordenador
- 0,3 GB de memoria libre en el sistema (consulte la nota 1)
- 1 GB de espacio libre en el disco duro (consulte la nota 2)
- Resolución de pantalla mínima de 1024 x 768
- Conexión a Internet o conexión de red de área local a una fuente (consulte la nota 3) de actualizaciones del producto
- La ejecución simultánea de dos programas antivirus en un mismo dispositivo provoca conflictos inevitables de recursos del sistema, como una ralentización del sistema que lo hace inservible

Aunque el producto podría instalarse y ejecutarse en sistemas que no cumplan estos requisitos, se recomienda realizar pruebas de usabilidad basadas en los requisitos de rendimiento.

(1): El producto podría utilizar más memoria si la memoria no se utiliza para otras tareas en un ordenador con muchas infecciones o al importar grandes listas de datos en el producto (p. ej. listas blancas de URL).
(2): El espacio en disco es necesario para descargar el instalador, instalar el producto, conservar una copia del paquete de instalación en los datos del programa y guardar copias de seguridad de las actualizaciones del producto para admitir la función de reversión. El producto puede utilizar más espacio en disco con configuraciones distintas (p. ej., cuando se almacenan más versiones de copia de seguridad de actualizaciones del producto, volcados de memoria o grandes cantidades de registros) o en un ordenador infectado (p. ej., debido a la función de cuarentena). Se recomienda mantener espacio en disco libre suficiente para permitir las actualizaciones del sistema operativo y del producto ESET.
(3): Aunque no se recomienda, puede actualizar el producto manualmente desde un medio extraíble.

Idiomas compatibles

ESET Endpoint Antivirus puede instalarse y descargarse en los idiomas que se indican a continuación.

Idioma	Código de idioma	LCID
Inglés (Estados Unidos)	en-US	1033
Árabe (Egipto)	ar-EG	3073
Búlgaro	bg-BG	1026
Chino simplificado	zh-CN	2052
Chino tradicional	zh-TW	1028
Croata	hr-HR	1050
Checo	cs-CZ	1029
Estonio	et-EE	1061
Finlandés	fi-FI	1035
Francés (Francia)	fr-FR	1036
Francés (Canadá)	fr-CA	3084
Alemán (Alemania)	de-DE	1031
Griego	el-GR	1032
*Hebreo	he-IL	1037
Húngaro	hu-HU	1038
*Indonesio	id-ID	1057
Italiano	it-IT	1040
Japonés	ja-JP	1041
Kazajo	kk-KZ	1087
Coreano	ko-KR	1042
*Letón	lv-LV	1062
Lituano	lt-LT	1063
Nederlands	nl-NL	1043
Noruego	nb-NO	1044
Polaco	pl-PL	1045
Portugués brasileño	pt-BR	1046
Rumano	ro-RO	1048
Ruso	ru-RU	1049
Español (Chile)	es-CL	13322
Español (España)	es-ES	3082
Sueco (Suecia)	sv-SE	1053
Eslovaco	sk-SK	1051
Slovenian	sl-SI	1060
Tailandés	th-TH	1054
Turco	tr-TR	1055

Idioma	Código de idioma	LCID
Ucraniano (Ucrania)	uk-UA	1058
*Vietnamita	vi-VN	1066

* ESET Endpoint Antivirus está disponible en este idioma, pero la guía del usuario en línea no está disponible (lo redirige a la versión en inglés).

Para cambiar el idioma de esta guía del usuario en línea, consulte la casilla de selección de idioma (en la esquina superior derecha).

Registro de cambios

Prevención

Cuando use el ordenador y, especialmente, cuando navegue por Internet, tenga en cuenta que ningún sistema antivirus puede eliminar completamente el riesgo de que se produzcan detecciones y ataques remotos. Para disfrutar de una protección y una comodidad máximas, se debe usar correctamente la solución antivirus y cumplir varias reglas útiles:

Actualización regular

De acuerdo con las estadísticas de ESET LiveGrid®, cada día se crean miles de nuevas amenazas únicas para burlar las medidas de seguridad existentes y proporcionar un beneficio a sus autores, todo ello a costa de otros usuarios. Los especialistas de ESET Virus Lab analizan estas amenazas diariamente, y preparan y publican actualizaciones para mejorar continuamente los niveles de protección para los usuarios. Para garantizar la máxima eficacia, las actualizaciones deben estar bien configuradas en el sistema. Para obtener más información sobre cómo configurar las actualizaciones, consulte el capítulo Configuración de actualizaciones.

Descarga de parches de seguridad

Los autores de software malintencionado con frecuencia explotan vulnerabilidades del sistema para aumentar la eficacia de la propagación de códigos malintencionados. Por ello, las empresas de software vigilan de cerca las nuevas vulnerabilidades en las aplicaciones y publican actualizaciones de seguridad para eliminar amenazas potenciales periódicamente. Es importante descargar estas actualizaciones de seguridad a medida que se publican. Microsoft Windows y los navegadores web como Microsoft Edge son dos ejemplos de software para los que se publican de forma periódica actualizaciones de seguridad.

Copia de seguridad de los datos importantes

Normalmente, a los autores de malware no les importan las necesidades de los usuarios y, con frecuencia, la actividad de los programas malintencionados provoca un fallo total del sistema operativo y la pérdida de datos importantes. Es esencial realizar copias de seguridad periódicas de los datos en una fuente externa, como un DVD o un disco duro externo. Estas precauciones facilitan y aceleran la recuperación de los datos en caso de fallo del sistema.

Análisis regular del ordenador en busca de virus

El módulo de protección del sistema de archivos en tiempo real se encarga de la detección de los virus, gusanos, troyanos y rootkits, conocidos o no. Esto significa que cada vez que entra en un archivo o lo abre, este se analiza en busca de actividad de código malicioso. Recomendamos que realice un análisis completo del ordenador al menos una vez al mes, ya que las firmas de códigos maliciosos pueden variar y el motor de detección se actualiza todos los días.

Seguimiento de las reglas de seguridad básicas

Esta es la regla más útil y eficaz de todas: sea siempre cauto. Actualmente, muchas amenazas requieren la intervención del usuario para su ejecución y distribución. Si es cauto a la hora de abrir archivos nuevos, se ahorrará mucho tiempo y esfuerzo en la desinfección de amenazas. Estas son algunas directrices útiles:

- No visite sitios web sospechosos con varios elementos y anuncios emergentes.
- Tenga cuidado al instalar programas gratuitos, paquetes codec, etc. Use únicamente programas seguros y solo visite sitios web seguros.
- Tenga cuidado a la hora de abrir archivos adjuntos de correo electrónico, especialmente los de mensajes masivos y de remitentes desconocidos.
- No use la cuenta de administrador para realizar su trabajo diario en el ordenador.

Estado de fin de la vida útil

ESET Endpoint Antivirus puede mostrar notificaciones o advertencias automatizadas para informarle sobre el próximo fin de la vida útil en varios lugares de la ventana principal del programa.

Más información acerca de:
- Política de fin de la vida útil (productos empresariales)
- Actualizaciones del producto
- Revisiones de seguridad y estabilidad

Para obtener más información sobre los cambios de ESET Endpoint Antivirus, lea el siguiente artículo de la base de conocimiento de ESET.

La siguiente tabla muestra algunos de los ejemplos de estados de productos y notificaciones con acciones basadas en categorías:

Categoría	Ventana de notificación o alerta	Página de actualización	Página de ayuda y asistencia técnica
Nueva actualización de funciones o mantenimiento disponible	Nueva versión de disponible Está disponible una actualización que contiene importantes correcciones de mantenimiento requeridas por ESET Endpoint Antivirus. Actualice ahora para garantizar la protección más actualizada. **Acción**: Más información	Hay una nueva versión de ESET Endpoint Antivirus disponible. Hay una nueva versión de ESET Endpoint Antivirus disponible. **Acciones**: actualizar ahora/activar actualizaciones automáticas	Hay una nueva versión de ESET Endpoint Antivirus disponible. Actualice ahora para obtener la versión más reciente con nuevas funciones y mejoras. Soporte hasta: dd/mm/aaaa
	Hay una actualización de mantenimiento disponible Hay una nueva versión de ESET Endpoint Antivirus disponible. Actualice ahora para obtener la versión más reciente con nuevas funciones y mejoras. **Acción**: Más información	Hay disponible una actualización de mantenimiento para ESET Endpoint Antivirus Número de versión instalada Soporte hasta: dd/mm/aaaa **Acción**: Más información	Está disponible una actualización que contiene importantes correcciones de mantenimiento requeridas por ESET Endpoint Antivirus. Actualice ahora para garantizar la protección más actualizada. Soporte hasta: dd/mm/aaaa
	Se recomienda reiniciar el dispositivo Está disponible una actualización que contiene importantes correcciones de mantenimiento requeridas por ESET Endpoint Antivirus. Actualice ahora para garantizar la protección más actualizada. **Acción**: Más información		Soporte hasta: dd/mm/aaaa
	Hay una actualización de mantenimiento crítica disponible Está disponible una actualización que contiene correcciones de mantenimiento críticas requeridas por ESET Endpoint Antivirus. Actualice ahora para garantizar la protección más actualizada. **Acción**: Más información	Hay disponible una actualización de mantenimiento crítica para ESET Endpoint Antivirus Número de versión instalada Soporte hasta: dd/mm/aaaa **Acción**: Más información	Está disponible una actualización que contiene correcciones de mantenimiento críticas requeridas por ESET Endpoint Antivirus. Actualice ahora para garantizar la protección más actualizada. Soporte hasta: dd/mm/aaaa
	Se necesita reiniciar el dispositivo Se ha descargado una actualización al número de versión, que contiene importantes correcciones de mantenimiento y estabilidad requeridas por su ESET Endpoint Antivirus. Actualice ahora para garantizar la protección más actualizada. **Acción**: Más información		Soporte hasta: dd/mm/aaaa

Categoría	Ventana de notificación o alerta	Página de actualización	Página de ayuda y asistencia técnica
Soporte próximo a caducar para la aplicación	El soporte para la versión de la aplicación instalada finaliza el dd/mm/aaaa, y el dispositivo pronto perderá la protección. Actualice ahora para mantener la protección. **Acción**: Actualizar ahora	Número de versión instalada/soporte hasta: dd/mm/aaaa **Acciones**: actualizar ahora/activar actualizaciones automáticas	El soporte para la versión instalada de ESET Endpoint Antivirus finaliza pronto y su equipo perderá la protección. Actualice ahora para mantener la protección. Soporte hasta: dd/mm/aaaa
	El soporte técnico ampliado de ESET con la versión de la aplicación instalada finaliza el dd/mm/aaaa, y su dispositivo pronto perderá la protección. Actualice ahora para mantener la protección. **Acción**: Actualizar ahora	Número de versión instalada/soporte hasta: dd/mm/aaaa **Acciones**: actualizar ahora/activar actualizaciones automáticas	El soporte extendido de ESET para la versión instalada de ESET Endpoint Antivirus finaliza pronto y su dispositivo perderá la protección. Actualice ahora para mantener la protección. Soporte hasta: dd/mm/aaaa
	El sistema operativo instalado está desactualizado, y el soporte para la versión de la aplicación instalada finaliza el dd/mm/aaaa. Actualice su sistema operativo para obtener la actualización de la aplicación más reciente y mantener la protección. **Acciones**: Más información	Número de versión instalada Soporte hasta: dd/mm/aaaa **Acción**: Más información	El soporte para la versión instalada de ESET Endpoint Antivirus finaliza pronto y su equipo perderá la protección. Actualice ahora para mantener la protección. Soporte hasta: dd/mm/aaaa
	El soporte extendido de ESET para la versión de la aplicación instalada finaliza pronto El sistema operativo instalado está desactualizado, y el soporte para la versión de la aplicación instalada finaliza el dd/mm/aaaa. Actualice su sistema operativo para obtener la actualización de la aplicación más reciente y mantener la protección. **Acción**: Más información	El soporte extendido de ESET para la versión instalada de ESET Endpoint Antivirus finaliza pronto Número de versión instalada Soporte hasta: dd/mm/aaaa **Acciones**: Más información	El soporte extendido de ESET para la versión instalada de ESET Endpoint Antivirus finaliza pronto y su dispositivo perderá la protección. Actualice ahora para mantener la protección. Soporte hasta: dd/mm/aaaa

Categoría	Ventana de notificación o alerta	Página de actualización	Página de ayuda y asistencia técnica
La versión de la aplicación ya no tiene soporte	⚠ La versión de la aplicación instalada ya no es compatible. El soporte para la versión de la aplicación instalada ha finalizado y es posible que el dispositivo no esté protegido. Actualice ahora para obtener protección. **Acción**: Actualizar ahora	⚠ La versión instalada de ESET Endpoint Antivirus ya no es compatible Número de versión instalada/soporte hasta: dd/mm/aaaa **Acciones**: actualizar ahora/activar actualizaciones automáticas	⚠ Soporte hasta: dd/mm/aaaa
	⚠ La versión de la aplicación instalada ya no es compatible. El sistema operativo instalado está desactualizado, y el soporte para la versión de la aplicación instalada ha finalizado. Su equipo no está protegido. Actualice su sistema operativo para recibir la actualización de la aplicación más reciente y obtener protección. **Acción**: Más información	⚠ La versión instalada de ESET Endpoint Antivirus ya no es compatible Número de versión instalada Soporte hasta: dd/mm/aaaa **Acción**: Más información	⚠ El soporte para la versión instalada de ESET Endpoint Antivirus ha finalizado y su equipo no está protegido. Actualice ahora para obtener protección. Soporte hasta: dd/mm/aaaa
Actualización del sistema operativo requerida	⚠ El sistema operativo instalado está desactualizado El sistema operativo instalado está desactualizado. Actualice su sistema operativo para obtener la actualización de la aplicación más reciente y mantener la protección. **Acción**: Más información	✓ ESET Endpoint Antivirus Número de versión instalada	Soporte hasta: dd/mm/aaaa

Páginas de Ayuda

Le damos la bienvenida a la guía del usuario de ESET Endpoint Antivirus. Esta información se proporciona para que presentarle el producto y como ayuda para que el ordenador sea más seguro.

Introducción

Antes de empezar a utilizar ESET Endpoint Antivirus, tenga en cuenta que el producto se puede gestionar de forma remota con ESET PROTECT. También le recomendamos que se familiarice con los diferentes tipos de amenazas detectadas y ataques remotos que puede encontrar al usar su ordenador.

Consulte las nuevas características para obtener más información sobre las características introducidas en esta versión de ESET Endpoint Antivirus. También hemos preparado una guía para ayudarle a configurar y personalizar las opciones básicas de ESET Endpoint Antivirus.

Cómo utilizar las páginas de Ayuda de ESET Endpoint Antivirus

Los temas de ayuda se dividen en varios capítulos y subcapítulos con el fin de facilitar la orientación y contextualización. Puede encontrar información relacionada en la estructura de páginas de Ayuda.

Pulse **F1** para obtener más información sobre cualquier ventana del programa. Aparecerá la página de Ayuda relacionada con la ventana que esté visualizando.

Las páginas de Ayuda admiten la búsqueda por palabra clave o por palabras o frases. La diferencia entre estos dos métodos es que una palabra clave puede estar relacionada de forma lógica con las páginas de Ayuda que no contienen esa palabra clave determinada en el texto. La búsqueda por palabras y frases se realiza en el contenido de todas las páginas y muestra únicamente las coincidencias que contienen la palabra o frase buscada.

Por motivos de coherencia y para ayudar a evitar confusiones, la terminología empleada en esta guía se basa en los nombres de parámetros de ESET Endpoint Antivirus. Además, utilizamos una serie de símbolos uniformes para destacar temas de interés o importancia especial.

Una nota es simplemente una breve observación. A pesar de que puede omitirlas, las notas contienen información valiosa como características específicas o un vínculo a un tema relacionado.

Este tipo de notas requieren su atención, y le recomendamos no omitir la información que incluyen. Normalmente contienen información que no resulta esencial, pero sí significativa.

Se trata de información que requiere más atención y cautela. Las advertencias se incluyen específicamente para evitar que cometa errores potencialmente peligrosos. Lea y comprenda el texto colocado en indicadores de advertencia, ya que hace referencia a una configuración del sistema muy delicada o a algún aspecto del sistema que conlleva ciertos riesgos.

Este es un caso o ejemplo práctico cuyo objetivo es ayudarle a comprender cómo se utiliza una determinada función o característica.

Convención	Significado
Negrita	Nombre de elementos de la interfaz, como recuadros y botones de opción.
Cursiva	Marcadores de posición de información que debe proporcionar. Por ejemplo, nombre de archivo o ruta de acceso significa que debe escribir la ruta de acceso real o un nombre de un archivo.
`Courier New`	Ejemplos de código o comandos.
Hipervínculo	Permite acceder de un modo rápido y sencillo a temas con referencias cruzadas o a una ubicación web externa. Los hipervínculos aparecen resaltados en color azul, y pueden estar subrayados.
%ProgramFiles%	El directorio del sistema Windows en el que se encuentran los programas instalados en Windows.

La **ayuda en línea** es la fuente principal de contenido de ayuda. Siempre que tenga una conexión a Internet activa se mostrará la versión más reciente de la ayuda en línea.

Documentación para equipos administrados de forma remota

Los productos para empresas de ESET, así como ESET Endpoint Antivirus, pueden administrarse de forma remota en las estaciones de trabajo cliente, servidores y dispositivos móviles en un entorno en red desde una ubicación central. Los administradores de sistemas que administran más de 10 estaciones de trabajo cliente pueden

considerar implementar una de las herramientas de administración remota de ESET para implementar soluciones de ESET, administrar tareas, aplicar políticas de seguridad, supervisar el estado del sistema y responder rápidamente a problemas o amenazas en ordenadores remotos desde una ubicación central.

Herramientas de administración remota ESET

ESET Endpoint Antivirus se puede administrar de forma remota con ESET PROTECT o ESET PROTECT Cloud.

- Introducción a ESET PROTECT
- Introducción a ESET PROTECT Cloud

- ESET HUB: vía de acceso centralizada a la plataforma de seguridad unificada ESET PROTECT. Proporciona administración centralizada de identidades, suscripciones y usuarios para todos los módulos de la plataforma ESET. Consulte Administración de licencias de ESET PROTECT para obtener instrucciones sobre cómo activar el producto. ESET HUB sustituye a ESET Business Account y ESET MSP Administrator por completo.

- ESET Business Account: es un portal de administración de licencias de los productos de ESET para empresas. Consulte Administración de licencias de ESET PROTECT para obtener instrucciones de activación del producto o consulte la Ayuda en línea de ESET Business Account para obtener más información sobre el uso de ESET Business Account. Si ya dispone de un nombre de usuario y una contraseña emitidos por ESET y desea convertirlos en una clave de licencia, consulte la sección Convertir credenciales de licencia heredada.

Productos de seguridad adicionales

- ESET Inspect: un completo sistema Endpoint de detección y respuesta que incluye funciones como las siguientes: detección de incidentes, administración de incidentes y respuesta, recopilación de datos, indicadores de detección de riesgo, detección de anomalías, detección de comportamientos e incumplimientos de políticas.
- ESET Endpoint Encryption: es una aplicación de seguridad integral diseñada para proteger sus datos en reposo y en tránsito. Con ESET Endpoint Encryption puede cifrar archivos, carpetas y correos electrónicos o crear discos virtuales cifrados, comprimir archivos e incluir una destructora de escritorio para la eliminación segura de archivos.

Herramientas de administración remota de terceros

- Supervisión y administración remotas (RMM)

Prácticas recomendadas

- Conectar todos los equipos con ESET Endpoint Antivirus a ESET PROTECT
- Proteger la Configuración avanzada en ordenadores cliente conectados para evitar modificaciones no autorizadas
- Aplicar una política recomendada para aplicar las funciones de seguridad disponibles
- Minimizar la interfaz de usuario: para reducir o limitar la interacción del usuario con ESET Endpoint Antivirus

Guías

- Cómo utilizar el modo de anulación
- Cómo implementar ESET Endpoint Antivirus con GPO o SCCM

Introducción a ESET PROTECT

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

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

ESET PROTECT lo conforman los siguientes componentes:

- ESET PROTECT Server: se ocupa de la comunicación con los agentes, y recopila y almacena datos de aplicaciones en la base de datos. ESET PROTECT Server se puede instalar en servidores Windows y Linux, y también está disponible como dispositivo virtual.
- ESET PROTECT Consola Web: es la interfaz principal que le permite administrar ordenadores cliente en su entorno. Muestra información general del estado de los clientes en la red y le permite implementar de forma remota soluciones de ESET en ordenadores no administrados. Tras instalar ESET PROTECT Server, puede acceder a la consola web a través del navegador web. Si configura el servidor web para que esté disponible desde Internet, puede utilizar ESET PROTECT desde prácticamente cualquier lugar o dispositivo con conexión a Internet.
- ESET Management Agent: facilita la comunicación entre ESET PROTECT Server y los ordenadores cliente. El agente debe instalarse en el ordenador cliente para establecer comunicación entre ese ordenador y ESET PROTECT Server. Como está en el ordenador cliente y puede almacenar varios contextos de seguridad, el uso de ESET Management Agent reduce considerablemente el tiempo de reacción a las nuevas detecciones. Con ESET PROTECT Web Console puede implementar ESET Management Agent en los ordenadores no administrados que identifica Active Directory o el Sensor de RD de ESET. También puede instalar de forma manual ESET Management Agent en los ordenadores cliente en caso de que sea necesario.
- ESET Rogue Detection Sensor: detecta los ordenadores no administrados presentes en su red y envía su información a ESET PROTECT Server. Esto le permite administrar ordenadores cliente nuevos en ESET PROTECT sin necesidad de buscarlos y agregarlos manualmente. El Rogue Detection Sensor recuerda los ordenadores que se han detectado y no envía la misma información dos veces.
- ESET Bridge: es un servicio que puede usarse en combinación con ESET PROTECT para:
    - Distribuir actualizaciones entre los ordenadores cliente y paquetes de instalación a ESET Management Agent.
    - Reenviar la comunicación de las instancias de ESET Management Agent a ESET PROTECT Server.
- Mobile Device Connector: es un componente que permite la administración de dispositivos móviles con ESET PROTECT, gracias a la que puede administrar dispositivos móviles (Android e iOS) y ESET Endpoint Security para Android.
- Dispositivo virtual de ESET PROTECT: está pensado para aquellos usuarios que quieren ejecutar ESET PROTECT en un entorno virtualizado.
- ESET PROTECT Virtual Agent Host: es un componente de ESET PROTECT que virtualiza entidades de agente

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

- Herramienta Mirror: es necesaria para las actualizaciones de módulos sin conexión. Si los ordenadores cliente no tienen conexión a Internet, puede utilizar la herramienta Mirror para descargar archivos de actualización de servidores de actualizaciones de ESET y almacenarlos localmente.
- ESET Remote Deployment Tool: implementa paquetes todo en uno creados en <%PRODUCT%> Web Console. Permite distribuir con facilidad ESET Management Agent con un producto de ESET por los ordenadores de una red.

Para obtener más información, consulte la ayuda 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 necesidad de tener un servidor físico o virtual como para ESET PROTECT o . Con (ESET PROTECT Cloud Consola Web), podrá implementar soluciones de ESET, administrar tareas, aplicar políticas de seguridad, supervisar el estado del sistema y responder rápidamente a problemas o amenazas que se produzcan en ordenadores remotos.

ESET PROTECT Cloud lo conforman los siguientes componentes:

- ESET PROTECT Cloud Instancia: se ocupa de la comunicación con los agentes, y recopila y almacena datos de aplicaciones en la base de datos.
- ESET PROTECT Cloud Consola Web: es la interfaz principal que le permite administrar ordenadores cliente en su entorno. Muestra información general del estado de los clientes en la red y le permite implementar de forma remota soluciones de ESET en ordenadores no administrados. Puede usar ESET PROTECT Cloud desde cualquier lugar o dispositivo en el que se disponga de conexión a Internet.
- ESET Management Agent: facilita la comunicación entre ESET PROTECT Cloud y los ordenadores cliente. El agente debe instalarse en el ordenador cliente para establecer comunicación entre ese ordenador y ESET PROTECT Cloud. Como está en el ordenador cliente y puede almacenar varios contextos de seguridad, el uso de ESET Management Agent reduce considerablemente el tiempo de reacción a las nuevas detecciones. Con ESET PROTECT Cloud Web Console puede implementar ESET Management Agent en los ordenadores no administrados. También puede instalar de forma manual ESET Management Agent en los ordenadores cliente en caso de que sea necesario.
- ESET Bridge: es un servicio que puede usarse en combinación con ESET PROTECT Cloud para:
    - Distribuir actualizaciones entre los ordenadores cliente y paquetes de instalación a ESET Management Agent.
    - Reenviar la comunicación de las instancias de ESET Management Agent a ESET PROTECT Cloud.
- Administración de dispositivos móviles: es un componente que permite la administración de dispositivos móviles con ESET PROTECT Cloud, gracias a la que puede administrar dispositivos móviles (Android e iOS) y ESET Endpoint Security para Android.
- Gestión de parches y vulnerabilidades: función disponible en ESET PROTECT Cloud que analiza periódicamente una estación de trabajo para detectar cualquier software instalado que pueda ser vulnerable a los riesgos de seguridad. Administración de revisiones ayuda a corregir estos riesgos mediante actualizaciones de software automatizadas, con lo que los dispositivos se mantienen más seguros.

Para obtener más información, consulte la ayuda en línea de ESET PROTECT Cloud.

Configuración protegida con contraseña

Debe configurar ESET Endpoint Antivirus correctamente para obtener la máxima seguridad para su sistema. Cualquier cambio o configuración incorrectos puede provocar que la seguridad y el nivel de protección del cliente disminuyan. Para limitar el acceso de usuarios a la configuración avanzada, el administrador puede protegerla con una contraseña.

El administrador puede crear una política para proteger con contraseña la Configuración avanzada de ESET Endpoint Antivirus en los ordenadores cliente conectados. Para crear una nueva política:

1. En ESET PROTECT Web Console, haga clic en **Políticas** en el menú principal de la izquierda.
2. Haga clic en **Nueva política**.
3. Escriba un nombre para su nueva política y, si lo desea, proporcione una descripción breve. Haga clic en el botón **Continuar**.
4. Seleccione **ESET Endpoint para Windows** en la lista de productos.
5. Haga clic en **Interfaz de usuario** en la lista **Configuración** y expanda **Configuración de acceso**.
6. Según la versión de ESET Endpoint Antivirus, haga clic en la alternar para activar **Contraseña para proteger la configuración**. Tenga en cuenta que la versión 7 y posteriores de los productos ESET Endpoint ofrece protección mejorada. Si dispone de la versión 7 y posteriores y de la versión 6 de productos Endpoint en la red, le recomendamos que cree dos políticas independientes con diferentes contraseñas para cada versión.
7. Cree una contraseña nueva en la ventana de notificación, confírmela y haga clic en **Aceptar**. Haga clic en **Continuar**.
8. Asigne la política a los clientes. Haga clic en **Asignar** y seleccione los ordenadores o los grupos de ordenadores que desea proteger con una contraseña. Haga clic en **Aceptar** para confirmar.
9. Compruebe que todos los ordenadores cliente que desea incluir estén en la lista y haga clic en **Continuar**.
10. Revise la configuración de la política en el resumen y haga clic en **Finalizar** para guardar la política nueva.

¿Qué son las políticas?

El administrador puede aplicar configuraciones específicas a productos de ESET que se ejecutan en ordenadores cliente con las políticas de ESET PROTECT consola web. Las políticas pueden aplicarse a ordenadores concretos o a grupos compuestos por varios ordenadores. También puede asignar varias políticas a un ordenador o a un grupo.

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

Las políticas se aplican en el orden de los grupos estáticos. En el caso de los grupos dinámicos, las políticas se aplican en primer lugar a los grupos dinámicos secundarios. Esto le permite aplicar políticas que tienen una mayor repercusión en la parte superior del árbol de grupos y políticas más específicas en los subgrupos. Con el uso de indicadores, un usuario de ESET Endpoint Antivirus con acceso a grupos que se sitúan en la parte superior del árbol puede anular las políticas de los grupos inferiores. Este algoritmo se explica en la ayuda en línea de ESET PROTECT.

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

Fusión de políticas

Una política que se aplica a un cliente suele ser el resultado de una fusión de varias políticas que terminan formando una política final. Las políticas se fusionan de una en una. Al fusionar políticas, la regla general es que la política más reciente siempre sustituye la configuración establecida por la más antigua. Si desea cambiar este comportamiento, puede utilizar los indicadores de políticas (disponibles para cada ajuste).

Al crear políticas, notará que algunos ajustes tienen reglas adicionales (sustituir, anexar, anteponer) que puede configurar.

- **Sustituir**: se sustituye la lista completa, se añaden valores nuevos y se quitan todos los anteriores.
- **Anexar**: se añaden elementos a la parte inferior de la lista aplicada en ese momento (debe ser otra política; la lista local siempre se sobrescribe).
- **Anteponer**: se añaden elementos a la parte superior de la lista (se sobrescribe la lista local).

ESET Endpoint Antivirus permite la fusión de ajustes locales y políticas remotas de una forma nueva. Si el ajuste es una lista (por ejemplo, una lista de sitios web bloqueados) y una política remota entra en conflicto con un ajuste local existente, la política remota la sobrescribe. Puede elegir cómo combinar listas locales y remotas si selecciona las distintas reglas de fusión para:

- Fusionar configuraciones para políticas remotas.
- Fusionar políticas remotas y locales y configuraciones locales con la política remota resultante.

Para obtener más información acerca de la fusión de políticas, consulte la guía del usuario de ESET PROTECT en línea y observe el ejemplo.

¿Cómo funcionan los indicadores?

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

Para cada ajuste puede seleccionar uno de los siguientes indicadores:

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

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

Instalación

Existen varios métodos para instalar ESET Endpoint Antivirus en una estación de trabajo cliente, a menos que implemente ESET Endpoint Antivirus de forma remota en estaciones de trabajo cliente a través de ESET PROTECT o ESET PROTECT Cloud.

Puede actualizar de ESET Endpoint Antivirus a ESET Endpoint Security al ejecutar el instalador de ESET Endpoint Security con ESET Endpoint Antivirus ya instalado. Sin embargo, debe instalar la misma versión o una versión posterior.

Métodos	Objetivo	Vínculo de descarga
Instalación con ESET AV Remover	La herramienta ESET AV Remover le ayudará a quitar casi todo el software antivirus que haya instalado anteriormente en su sistema antes de continuar con la instalación.	Descargar versión para 64 bits Descargar versión para 32 bits

Métodos	Objetivo	Vínculo de descarga
*** Instalación (.exe)	Proceso de instalación sin ESET AV Remover.	Descargar versión para 64 bits Descargar versión para 32 bits
Instalación (.msi)	En entornos empresariales, el instalador .msi es el paquete de instalación preferido. Esto se debe principalmente a las implementaciones sin conexión y remotas que utilizan diferentes herramientas, como ESET PROTECT.	Descargar versión para 64 bits Descargar versión para 32 bits
Instalación desde la línea de comandos	ESET Endpoint Antivirus puede instalarse localmente con la línea de comandos o de forma remota con una tarea de cliente de ESET PROTECT.	N/A
Implementación con GPO o SCCM	Use herramientas de administración como GPO o SCCM para implementar ESET Management Agent y ESET Endpoint Antivirus en estaciones de trabajo cliente.	N/A
Implementación con herramientas RMM	Los complementos de ESET DEM para la herramienta Remote Management and Monitoring (RMM) le permiten implementar ESET Endpoint Antivirus en las estaciones de trabajo cliente.	N/A

ESET Endpoint Antivirus está disponible en más de 30 idiomas.

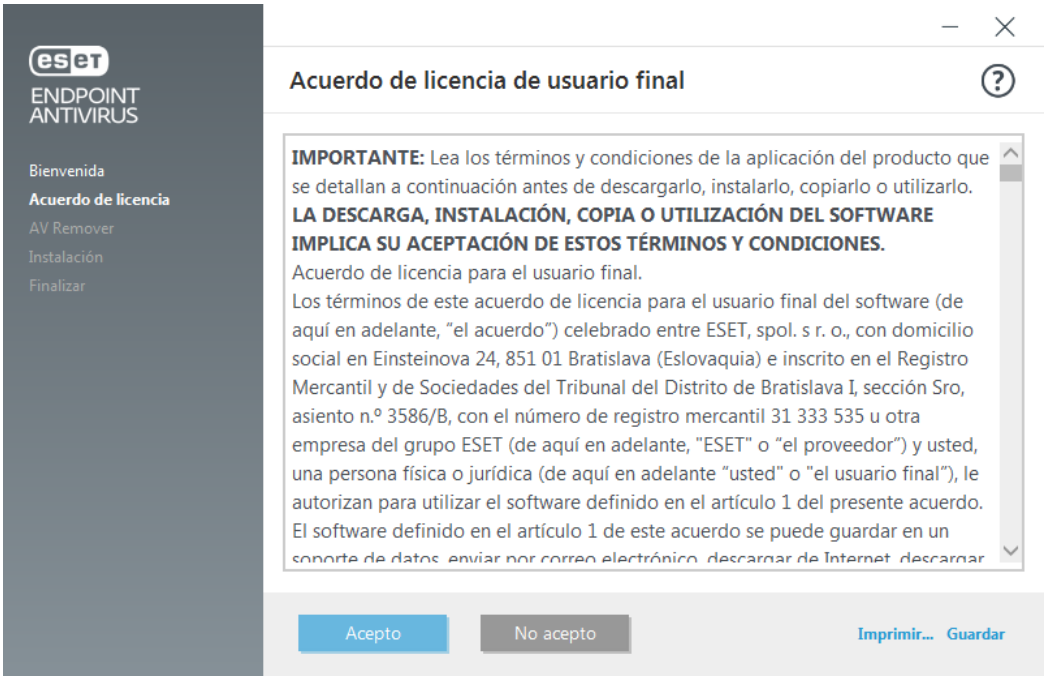
Instalación con ESET AV Remover

Antes de continuar con el proceso de instalación, es importante que desinstale las posibles aplicaciones de seguridad que tenga en el ordenador. Marque la casilla situada junto a **Quiero desinstalar aplicaciones antivirus con ESET AV Remover** para que ESET AV Remover analice el sistema y quite las aplicaciones de seguridad compatibles que tuviera instaladas. Mantenga la casilla desmarcada y haga clic en **Continuar** para instalar ESET Endpoint Antivirus sin ejecutar ESET AV Remover.

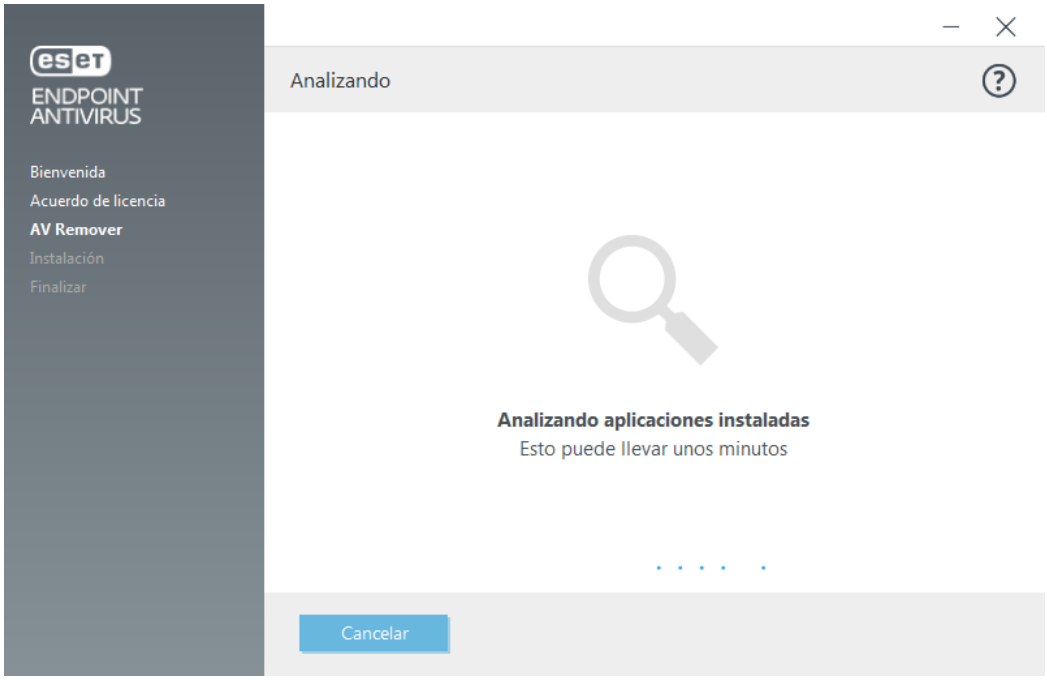
ESET AV Remover

La herramienta ESET AV Remover le ayudará a eliminar casi cualquier software antivirus que haya instalado anteriormente en el sistema. Siga las instrucciones expuestas a continuación para quitar un programa antivirus existente con ESET AV Remover:

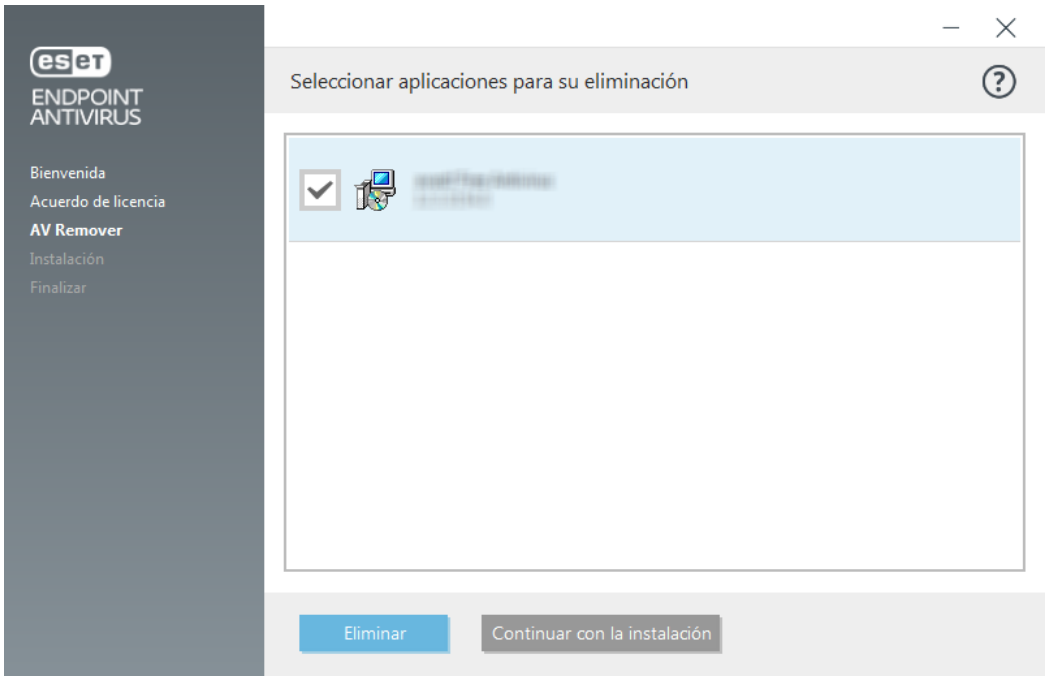
1. Para ver una lista del software antivirus que ESET AV Remover puede quitar, visite el artículo de la base de conocimiento de ESET.
2. Lea el Acuerdo de licencia para el usuario final y haga clic en **Aceptar** para confirmar que acepta dicho acuerdo. Si hace clic en **No acepto**, la instalación de ESET Endpoint Antivirus continuará sin la eliminación de las posibles aplicaciones de seguridad existentes en el ordenador.



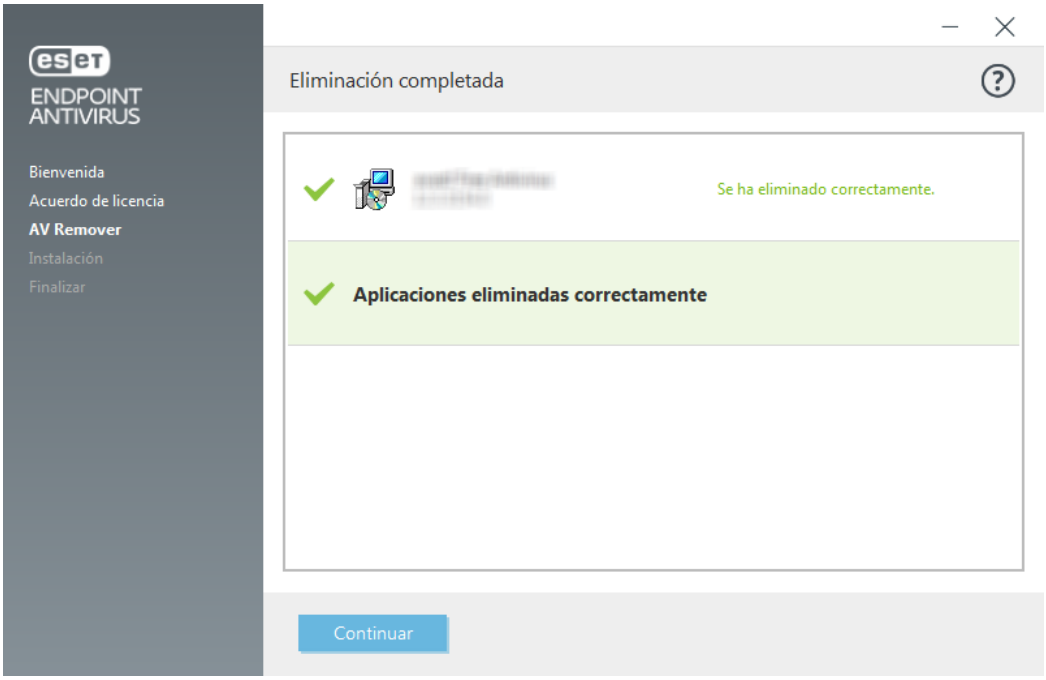
2. ESET AV Remover comenzará a buscar software antivirus en el sistema.



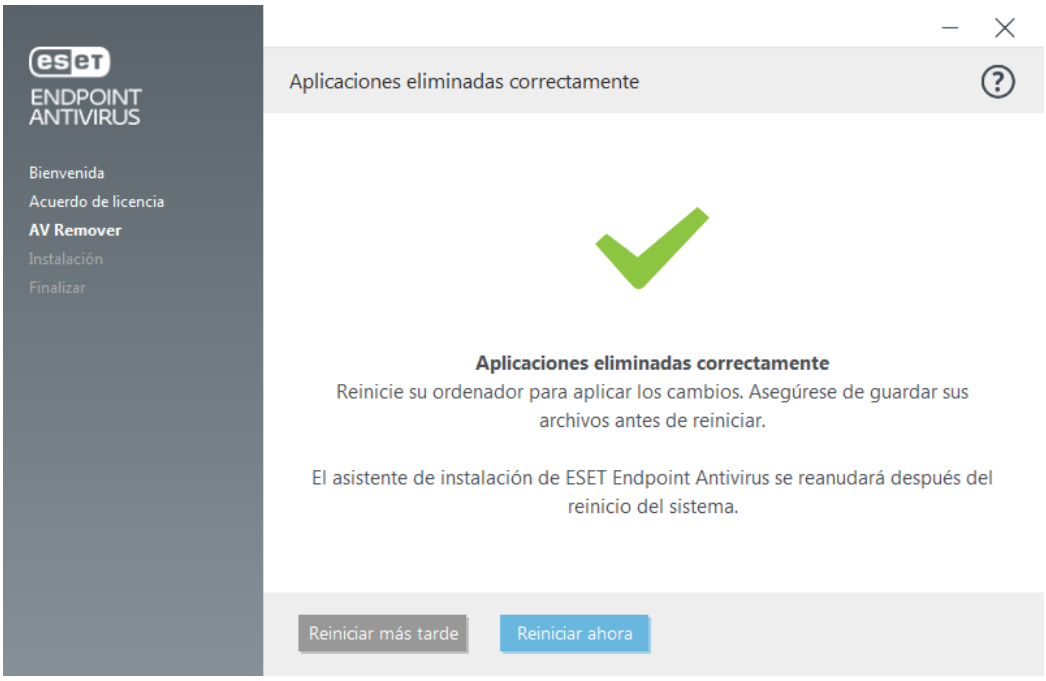
2. Seleccione las aplicaciones antivirus que aparezcan en la lista y haga clic en **Quitar**. Este proceso puede llevar unos minutos.



2. Una vez finalizado el procedimiento de desinstalación de aplicaciones, haga clic en **Continuar**.



6. Reinicie el ordenador para aplicar los cambios y continuar con la instalación de ESET Endpoint Antivirus. Si la desinstalación no ha finalizado correctamente, consulte el apartado La desinstalación mediante ESET AV Remover finalizó con un error de esta guía.



Desinstalación mediante ESET AV Remover finalizada con error

Si no puede quitar un programa antivirus con ESET AV Remover, recibirá una notificación en la que se le indica que la aplicación que está intentando quitar podría no ser compatible con ESET AV Remover. Consulte la lista de productos compatibles o acceda a los desinstaladores de software antivirus para Windows populares en la base de conocimiento de ESET para comprobar si el programa en cuestión puede quitarse.

Si la desinstalación del producto de seguridad no se pudo completar correctamente o alguno de sus componentes

se ha desinstalado solo de forma parcial, aparecerá la opción **Reiniciar y analizar de nuevo**. Confirme el control de cuentas de usuario tras el inicio y continúe con el proceso de análisis y desinstalación.

Si es necesario, póngase en contacto con el servicio de soporte técnico de ESET para abrir una solicitud de soporte y tenga a mano el archivo **AppRemover.log** para ayudar a los técnicos de ESET. El archivo **AppRemover.log** está en la carpeta **eset**. Vaya a *%TEMP%* en el Explorador de Windows para acceder a esta carpeta. El servicio de soporte técnico de ESET responderá lo más rápidamente posible para ayudarle a resolver el problema.

Instalación (.exe)

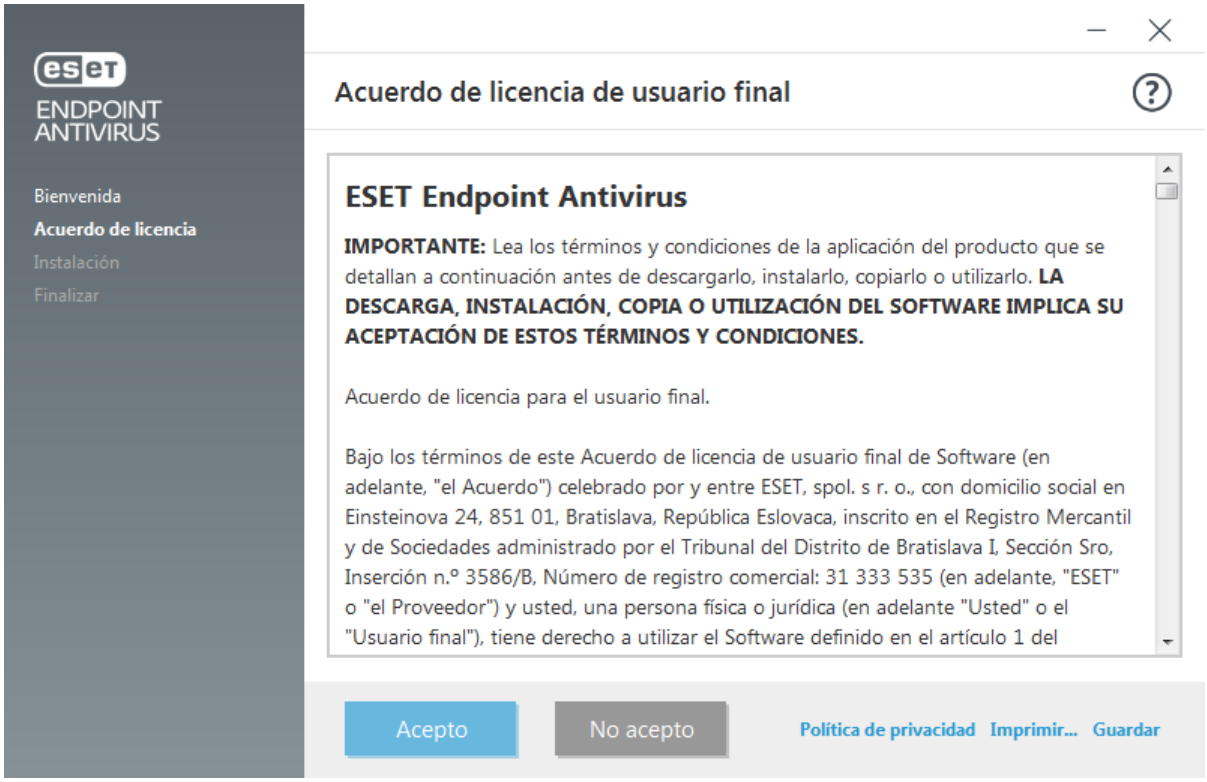
Cuando ejecute el instalador .exe, el asistente de instalación le proporcionará instrucciones para realizar la instalación.

Asegúrese de que no tiene instalados otros programas antivirus en el ordenador. Si instala más de dos soluciones antivirus en un solo ordenador, estas pueden entrar en conflicto. Le recomendamos que desinstale del sistema uno de los programas antivirus. Consulte nuestro artículo de la base de conocimiento para ver una lista de herramientas de desinstalación para software antivirus habitual (disponible en inglés y algunos otros idiomas).

1. Seleccione su preferencia para las siguientes funciones, lea el Acuerdo de licencia para el usuario final y la Política de privacidad, y haga clic en **Continuar**, o haga clic en **Permitir todo y continuar** para activar todas las funciones:

- Sistema de respuesta de ESET LiveGrid®
- Detección de aplicaciones potencialmente indeseables

Al hacer clic en **Continuar** o en **Permitir todo y continuar**, acepta el Acuerdo de licencia para el usuario final y la Política de privacidad. Puede instalar ESET Endpoint Antivirus en una carpeta concreta si hace clic en Cambiar la carpeta de instalación.



2. Una vez finalizada la instalación, se le pedirá que activar ESET Endpoint Antivirus.

Cómo cambiar la carpeta de instalación (.exe)

Puede **Cambiar la carpeta de instalación** durante la instalación. Seleccione una ubicación para la instalación de ESET Endpoint Antivirus. De forma predeterminada, el programa se instala en el directorio siguiente:

C:\Program Files\ESET\ESET Security

Puede especificar una ubicación para los datos y los módulos del programa. De forma predeterminada, estos se instalan en los directorios siguientes:

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

Haga clic en **Examinar** para cambiar estas ubicaciones (no recomendado).

Haga clic en **Atrás** y continúe con el proceso de instalación.

Instalación (.msi)

Cuando ejecute el instalador .msi, el asistente de instalación le proporcionará instrucciones para realizar la instalación.

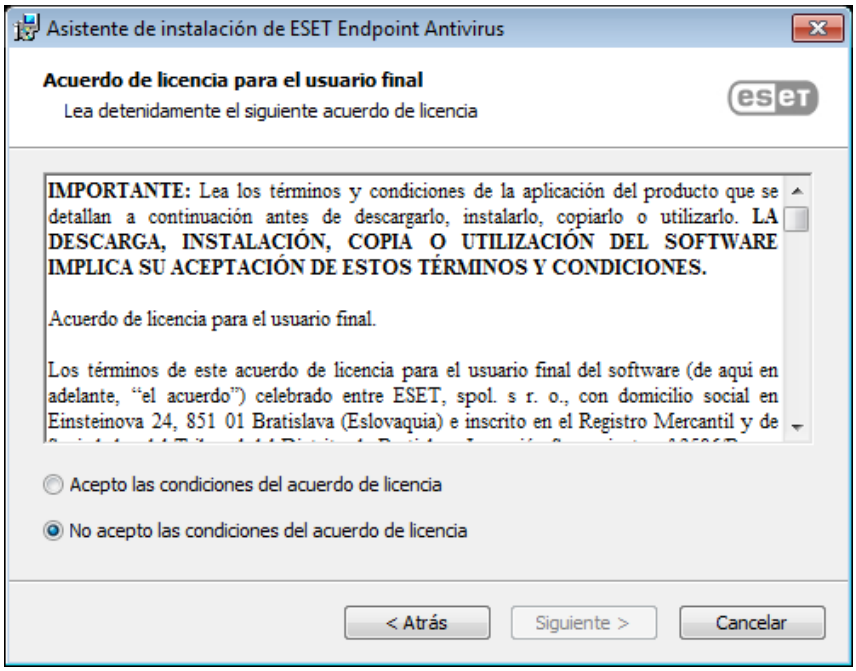
✓ En entornos empresariales, el instalador .msi es el paquete de instalación preferido. Esto se debe principalmente a las implementaciones sin conexión y remotas que utilizan diferentes herramientas, como ESET PROTECT.

Asegúrese de que no tiene instalados otros programas antivirus en el ordenador. Si instala más de dos soluciones antivirus en un solo ordenador, estas pueden entrar en conflicto. Le recomendamos que desinstale del sistema uno de los programas antivirus. Consulte nuestro artículo de la base de conocimiento para ver una lista de herramientas de desinstalación para software antivirus habitual (disponible en inglés y algunos otros idiomas).

El instalador de ESET Endpoint Antivirus creado en ESET PROTECT es compatible con Windows 10 Enterprise para escritorios virtuales y el modo multisesión de Windows 10.

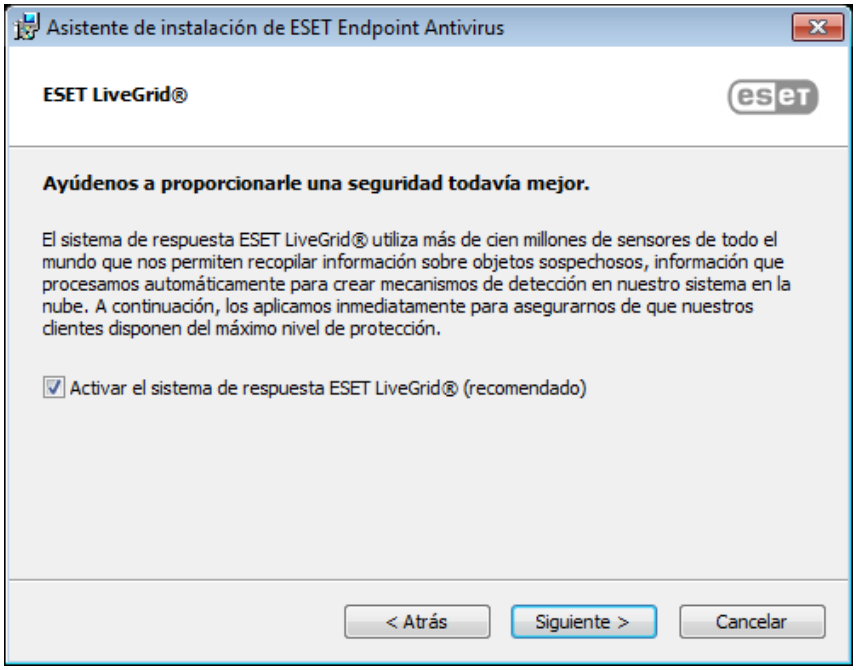
1. Seleccione el idioma que desee y haga clic en **Siguiente**.

2. Lea el Acuerdo de licencia para el usuario final y haga clic en **Acepto los términos del contrato de licencia** para confirmar su aceptación de dicho acuerdo. Haga clic en **Siguiente** después de aceptar los términos para continuar con la instalación.



3. Indique si desea activar el sistema de respuesta ESET LiveGrid®. ESET LiveGrid® garantiza que ESET recibe notificaciones inmediatas y continuas sobre nuevas infiltraciones, lo que le permite proteger mejor a sus

clientes. El sistema le permite enviar nuevas amenazas al laboratorio de virus de ESET, donde se analizan, procesan y agregan al motor de detección. Haga clic en **Configuración avanzada** para configurar parámetros de instalación adicionales.



4. El último paso es hacer clic en **Instalar**. Una vez finalizada la instalación, se le pedirá que active ESET Endpoint Antivirus.

Instalación avanzada (.msi)

La instalación avanzada le permite personalizar parámetros de instalación que no están disponibles durante el proceso de instalación típico.

1. Puede **Cambiar la carpeta de instalación** durante la instalación. Seleccione una ubicación para la instalación de ESET Endpoint Antivirus. De forma predeterminada, el programa se instala en el directorio siguiente:

C:\Program Files\ESET\ESET Security

Puede especificar una ubicación para los datos y los módulos del programa. De forma predeterminada, estos se instalan en los directorios siguientes:

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

Haga clic en **Examinar** para cambiar estas ubicaciones (no recomendado).

2. Elija los componentes de producto que desea instalar. Puede seleccionar su preferencia para el análisis del ordenador y todas las protecciones disponibles. El componente Mirror de actualización sirve para actualizar otros ordenadores de la red. Supervisión y administración remotas (RMM) es el proceso de supervisar y controlar los sistemas de software con un agente instalado localmente al que puede acceder un proveedor de servicios de administración.

3. Haga clic en **Instalar** para iniciar el proceso de instalación.

Instalación con el número mínimo de módulos

Para reducir el tráfico de red relacionado con el tamaño del instalador y ahorrar recursos, el producto ESET incluye un instalador con el número mínimo de módulos. El instalador solo contiene los módulos imprescindibles; el resto se descarga durante la actualización de los módulos iniciales tras la activación del producto. La principal ventaja es tener un instalador considerablemente más pequeño, y ESET Endpoint Antivirus descarga solo los módulos de la aplicación más recientes al activarse el producto.

El instalador con el número mínimo de módulos contiene los siguientes módulos:

- Cargadores
- Comunicación con Direct Cloud
- Compatibilidad con traducción
- Configuración
- SSL

Tras la activación del producto, verá el estado **Inicializando protección**, que le informará de las funciones que se están inicializando.

Si se produce un problema con la descarga de los módulos (p. ej., hay un error de configuración del proxy, no se detecta una red, etc.), se mostrará el estado de alerta de la aplicación **Se requiere atención**. En la ventana principal del programa, haga clic en **Actualizar** > **Buscar actualizaciones** para volver a iniciar el proceso de actualización.

Tras varios intentos sin éxito, se mostrará el estado de la aplicación **Error en la configuración de la protección** en rojo. Haga clic en Intentar de nuevo para volver a iniciar la configuración de la protección. Si el proceso de inicialización falla y sigue sin poder descargar los módulos, descargue los instaladores MSI completos.

Si los ordenadores cliente no tienen conexión a Internet o funcionan sin conexión y necesitan una actualización, utilice los siguientes métodos para descargar los archivos de actualización de los servidores de actualización de ESET:
- Actualización desde el servidor Mirror
- Uso de la herramienta Mirror

Instalación desde la línea de comandos

Puede instalar ESET Endpoint Antivirus localmente desde la línea de comandos o puede instalarlo de forma remota con una tarea del cliente desde ESET PROTECT.

Parámetros admitidos

APPDIR=<path>

- Ruta de acceso: ruta de acceso de un directorio válido
- Directorio de instalación de la aplicación.

APPDATADIR=<path>

- Ruta de acceso: ruta de acceso de un directorio válido

- Directorio de instalación de los datos de la aplicación.

MODULEDIR=<path>

- Ruta de acceso: ruta de acceso de un directorio válido
- Directorio de instalación del módulo.

ADDLOCAL=<list>

- Instalación de componentes: lista de características no obligatorias que se pueden instalar localmente.
- Uso con paquetes .msi de ESET: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Para obtener más información sobre la propiedad **ADDLOCAL**, consulte https://msdn.microsoft.com/es-es/library/aa367536(v=vs.85).aspx

ADDEXCLUDE=<list>

- La lista ADDEXCLUDE es una lista separada por comas de todos los nombres de características que no desea instalar, que sustituye a la función obsoleta REMOVE.
- Cuando seleccione una característica que no desee instalar, toda la ruta de acceso (es decir, todas sus subcaracterísticas) y las características invisibles relacionadas deben incluirse explícitamente en la lista.
- Uso con paquetes .msi de ESET: `ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

> **ADDEXCLUDE** no se puede usar junto con **ADDLOCAL**.

Consulte la documentación de la versión de **msiexec** usada para conocer los modificadores de la línea de comandos apropiados.

Reglas

- La lista **ADDLOCAL** es una lista separada por comas de los nombres de todas las características que se van a instalar.
- Al seleccionar una característica para instalarla, se debe incluir en la lista y de forma explícita toda la ruta de acceso (todas las características principales).
- Consulte las reglas adicionales para obtener la información sobre el uso correcto.

Componentes y funciones

> La instalación de componentes con los parámetros ADDLOCAL/ADDEXCLUDE no funciona con ESET Endpoint Antivirus.

Las funciones se dividen en 4 categorías:

- **Obligatoria**: la función se instalará siempre.
- **Opcional**: se puede anular la selección de la función para que no se instale.
- **Invisible**: característica lógica obligatoria para que otras características funcionen correctamente.
- **Marcador de posición**: característica que no tiene repercusión en el producto, pero que debe incluirse con características secundarias.

El conjunto de funciones de ESET Endpoint Antivirus es el siguiente:

Descripción	Nombre de la característica	Función principal	Presencia
Componentes del programa básicos	Computer		Marcador de posición
Motor de detección	Antivirus	Computer	Obligatoria
Motor de detección/Análisis de malware	Scan	Computer	Obligatoria
Motor de detección/Protección del sistema de archivos en tiempo real	RealtimeProtection	Computer	Obligatoria
Motor de detección/Análisis de malware/Protección de documentos	DocumentProtection	Antivirus	Opcional
Control de dispositivos	DeviceControl	Computer	Opcional
Protección de la red	Network		Marcador de posición
Protección de la red/Cortafuegos	Firewall	Network	Opcional
Protección de la red/Protección contra los ataques de red/...	IdsAndBotnetProtection	Network	Opcional
Navegador seguro	OnlinePaymentProtection	WebAndEmail	Opcional
Web y correo electrónico	WebAndEmail		Marcador de posición
Web y correo electrónico/Filtrado de protocolos	ProtocolFiltering	WebAndEmail	Invisible
Web y correo electrónico/Protección de acceso a la web	WebAccessProtection	WebAndEmail	Opcional
Web y correo electrónico/Protección del cliente de correo electrónico	EmailClientProtection	WebAndEmail	Opcional
Web y correo electrónico/Protección del cliente de correo electrónico/Clientes de correo electrónico	MailPlugins	EmailClientProtection	Invisible
Web y correo electrónico/Protección del cliente de correo electrónico/Antispam del cliente de correo electrónico	Antispam	EmailClientProtection	Opcional
Web y correo electrónico/Control de acceso web	WebControl	WebAndEmail	Opcional
Herramientas/ESET RMM	Rmm		Opcional
Actualización/Perfiles/Mirror de actualización	UpdateMirror		Opcional
Plugin ESET Inspect	EnterpriseInspector		Invisible

Conjunto de funciones de grupo:

Descripción	Nombre de la característica	Presencia de características
Todas las funciones obligatorias	_Base	Invisible
Todas las funciones disponibles	ALL	Invisible

Reglas adicionales

- Si se selecciona alguna de las funciones de **WebAndEmail** para la instalación, se debe incluir la función invisible **ProtocolFiltering** en la lista.
- Los nombres de las funciones distinguen entre mayúsculas y minúsculas, por ejemplo, UpdateMirror no es lo mismo que UPDATEMIRROR.

Lista de propiedades de configuración

Propiedad	Valor	Característica
CFG_POTENTIALLYUNWANTED_ENABLED=	0: desactivado 1: activado	Detección de aplicaciones potencialmente no deseadas (PUA)
CFG_LIVEGRID_ENABLED=	Ver a continuación	Consulte la propiedad LiveGrid a continuación
FIRSTSCAN_ENABLE=	0: desactivado 1: activado	Programe y ejecute un Análisis del ordenador después de la instalación
CFG_PROXY_ENABLED=	0: desactivado 1: activado	Configuración del servidor Proxy
CFG_PROXY_ADDRESS=	<ip>	Dirección IP del servidor proxy
CFG_PROXY_PORT=	<port>	Número de puerto del servidor proxy
CFG_PROXY_USERNAME=	<username>	Nombre de usuario de autenticación
CFG_PROXY_PASSWORD=	<password>	Contraseña de autenticación
ACTIVATION_DATA=	Ver a continuación	Activación del producto, clave de licencia o archivo de licencia sin conexión
ACTIVATION_DLG_SUPPRESS=	0: desactivado 1: activado	Si se selecciona "1", no se muestra el cuadro de diálogo de activación del producto tras el primer inicio
ADMINCFG=	<path>	Ruta de acceso de la configuración XML exportada (valor predeterminado *cfg.xml*)

Propiedad de LiveGrid®

Cuando se instala ESET Endpoint Antivirus con`CFG_LIVEGRID_ENABLED`, el comportamiento del producto tras la instalación será:

Característica	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
Sistema de reputación ESET LiveGrid®	Activado	Activado
Sistema de respuesta ESET LiveGrid®	Desactivado	Activado
Enviar estadísticas anónimas	Desactivado	Activado

Propiedad ACTIVATION_DATA

Formato	Métodos
ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE	Activación con Clave de licencia de ESET (la conexión a Internet debe estar activa)

Formato	Métodos
`ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf`	Activación con un archivo de licencia sin conexión

Propiedades de idioma

Idioma de ESET Endpoint Antivirus (debe especificar ambas propiedades).

Propiedad	Valor
`PRODUCT_LANG=`	LCID Decimal (ID de configuración regional), por ejemplo, 1033 para inglés (Estados Unidos). Consulte la lista de códigos de idioma.
`PRODUCT_LANG_CODE=`	LCID String (nombre de referencia cultural del idioma) en minúsculas, por ejemplo, en-us para inglés (Estados Unidos). Consulte la lista de códigos de idioma.

Propiedades de reinicio

Especifique los parámetros siguientes para reiniciar el ordenador después de la instalación:

Propiedad	Valor	Característica
`REBOOT_WHEN_NEEDED=`	0: desactivado 1: activado	Si esta opción está activada, el ordenador se reiniciará tras la instalación.
`REBOOT_CANCELABLE=`	0: desactivado 1: activado	Si esta opción está activada, el usuario puede cancelar el reinicio del ordenador.
`REBOOT_POSTPONE=`	valor en segundos	Tiempo máximo en segundos para que el usuario posponga el reinicio del ordenador.

REBOOT_CANCELABLE y REBOOT_POSTPONE solo están disponibles si REBOOT_WHEN_NEEDED está activado.

Ejemplos de instalación desde la línea de comandos

Asegúrese de leer el Acuerdo de licencia de usuario final y de tener privilegios administrativos antes de ejecutar la instalación.

Excluya la sección **NetworkProtection** de la instalación (debe especificar también todas las funciones secundarias):
```
msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection
```

Si desea que ESET Endpoint Antivirus se configure automáticamente tras la instalación, puede especificar parámetros de configuración básicos en el comando de instalación.
Instale ESET Endpoint Antivirus con ESET LiveGrid® activado:
```
msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1
```

Instale en un directorio de instalación de aplicaciones distinto al predeterminado.
```
msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\
```

Instale y active ESET Endpoint Antivirus con la clave de licencia de ESET.
```
msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE
```

Instalación silenciosa con registro detallado (útil para la solución de problemas) y RMM solo con los componentes obligatorios:
`msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm`

Instalación completa silenciosa forzada con un idioma especificado.
`msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us`

Opciones de la línea de comandos tras la instalación

- CMD de ESET : importar un archivo de configuración de .xml o activar/desactivar una función de seguridad.
- Análisis de línea de comandos : ejecuta un análisis del ordenador desde la línea de comandos.

Implementación con GPO o SCCM

Además de instalar ESET Endpoint Antivirus directamente en una estación de trabajo cliente, también puede instalarlo mediante herramientas de administración como Objeto de política de grupo (GPO), Software Center Configuration Manager (SCCM), Symantec Altiris o Puppet.

Administrado (recomendado)

En los ordenadores administrados, primero instalamos el agente ESET Management, luego implementamos ESET Endpoint Antivirus a través de ESET PROTECT. Debe tener ESET PROTECT instalado en su red.

1. Descargue el instalador independiente para ESET Management Agent.
2. Prepare el script de implementación remota de GPO/SCCM.
3. Implemente ESET Management Agent con GPO o SCCM.
4. Asegúrese de que los ordenadores cliente se hayan agregado a ESET PROTECT.
5. Implemente y active ESET Endpoint Antivirus en sus ordenadores cliente.

Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:
- Implemente ESET Management Agent mediante SCCM o GPO
- Implementar ESET Management Agent con un Objeto de política de grupo (GPO)

No administrado

En los ordenadores no administrados, puede implementar ESET Endpoint Antivirus directamente en las estaciones de trabajo de cliente. Esto no se recomienda, ya que no podrá supervisar ni aplicar las políticas para todos sus productos ESET para equipos en las estaciones de trabajo.

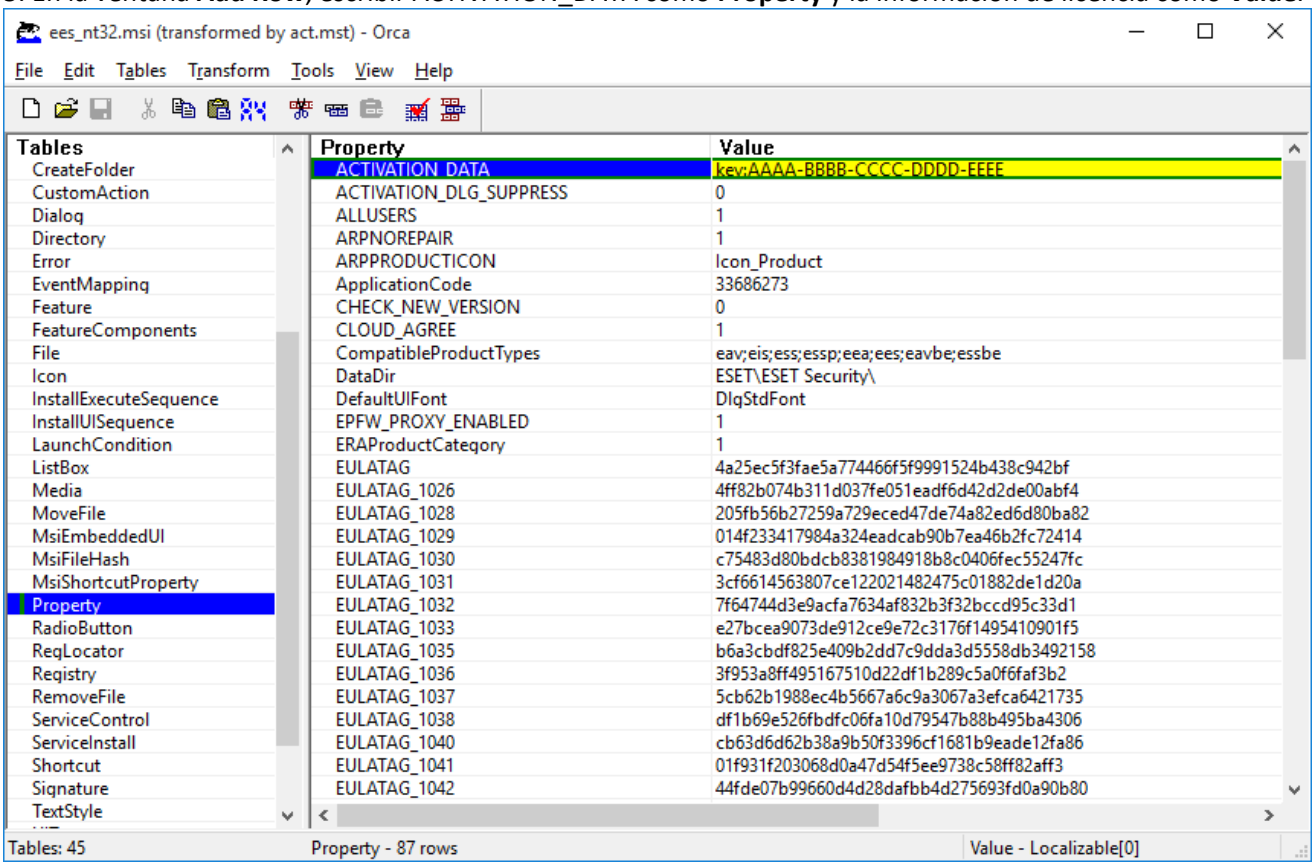
De forma predeterminada, ESET Endpoint Antivirus no se activa tras la instalación y, por lo tanto, no está funcional.

Opción 1 (instalación de software)

1. Descargue el instalador .msi para ESET Endpoint Antivirus.
2. Cree un paquete de transformación .mst a partir del archivo .msi (por ejemplo, mediante el editor de .msi Orca) para incluir la propiedad de activación del producto (consulte `ACTIVATION_DATA` en Instalación desde la línea de comandos).

Mostrar pasos para crear .mst en Orca

1. Abrir Orca
2. Cargar el instalador .msi haciendo clic en **File** > **Open**.
3. Hacer clic en **Transform** > **New Transform**.
4. Hacer clic en **Property** en la sección **Tables** y, a continuación, en el menú **Tables** > **Add row**.
5. En la ventana **Add Row**, escribir ACTIVATION_DATA como **Property** y la información de licencia como **Value**.



6. Hacer clic en **Transform** > **Generate Transform** para guardar el archivo .mst.

1. Opcional: Para importar su archivo de configuración ESET Endpoint Antivirus .xml personalizado (por ejemplo, para activar RMM o ajustar la configuración del servidor proxy), coloque el archivo cfg.xml en la misma ubicación que el instalador .msi.
2. Implemente el instalador .msi con el archivo .mst de forma remota con una GPO (mediante instalación de software) o SCCM.

Opción 2 (uso de una tarea programada)

1. Descargue el instalador .msi para ESET Endpoint Antivirus.
2. Prepare un script de Instalación desde la línea de comandos para incluir la propiedad de activación del producto (consulte `ACTIVATION_DATA`).
3. Haga el instalador .msi y el script .cmd accesibles en la red para todas las estaciones de trabajo.
4. Opcional: Para importar su archivo de configuración ESET Endpoint Antivirus .xml personalizado (por ejemplo, para activar RMM o ajustar la configuración del servidor proxy), coloque el archivo cfg.xml en la misma ubicación que el instalador .msi.
5. Aplique un script de instalación desde la línea de comandos preparado con GPO o SCCM.
    - Para GPO, use Preferencias de política de grupo > Tareas de programación de política de grupo > Tarea inmediata

Si no desea usar ESET PROTECT para administrar sus productos ESET para equipos de forma remota, ESET Endpoint Antivirus contiene el complemento de ESET para RMM que le permite supervisar y controlar los sistemas de software mediante un agente instalado de forma local al que se puede acceder a través de un proveedor de servicios de administración. Más información

Actualización a una versión más reciente

Las versiones nuevas de ESET Endpoint Antivirus implementan mejoras o solucionan problemas que no se pueden arreglar con las actualizaciones automáticas de los módulos de programa.

La actualización a una versión más reciente se puede realizar de varias maneras:

1. Automáticamente, con ESET PROTECT, o ESET PROTECT Cloud.
2. Automáticamente, con GPO o SCCM.
3. Automáticamente, mediante una actualización del programa.
   Las actualizaciones del programa se distribuyen a todos los usuarios y pueden afectar a determinadas configuraciones del sistema, de modo que se envían tras un largo período de pruebas para garantizar su funcionalidad en todas las configuraciones posibles del sistema. Si necesita instalar una versión más reciente en cuanto se publica, utilice uno de los métodos que se indican a continuación.
   Asegúrese de que ha activado el **Modo de actualización** en Configuración avanzada > **Actualización** > **Perfiles** > **Actualizaciones del producto**.
4. Actualización manual mediante la descarga e instalación de una versión más reciente sobre la instalación existente.

Escenarios de actualización recomendados

Administro o quiero administrar mis productos de ESET de forma remota

Si administra más de 10 productos de ESET Endpoint, puede gestionar las actualizaciones con ESET PROTECT o ESET PROTECT Cloud. Consulte la siguiente documentación:

- ESET PROTECT | Actualizar el software de ESET a través de una tarea del cliente
- ESET PROTECT | Guía para pequeñas y medianas empresas que administran hasta 250 productos de ESET para equipos Windows
- Introducción a ESET PROTECT Cloud

Actualización manual en una estación de trabajo cliente

Para actualizar ESET Endpoint Antivirus en estaciones de trabajo cliente específicas manualmente:

1. Compruebe que la versión que tiene instalada es compatible.
2. Compruebe que su sistema operativo sea compatible.

2. Descargue e instale la versión más reciente sobre la versión anterior.

No se garantiza la instalación correcta de la versión más reciente sobre la anterior en versiones con nivel de soporte "Fin de la vida útil". Consulte la Política sobre el fin de la vida útil para consultar su nivel de soporte de ESET Endpoint Antivirus.
Para actualizar desde versiones no compatibles, desinstale primero ESET Endpoint Antivirus. Lea el siguiente artículo de la base de conocimiento de ESET para obtener información adicional sobre la actualización de ESET Endpoint Antivirus en una estación de trabajo cliente.

Actualización automática de productos anteriores

La versión de su producto de ESET ya no es compatible y su producto se ha actualizado a la versión más reciente.

Problemas de instalación comunes

Cada nueva versión de productos de ESET contiene numerosas correcciones de errores y mejoras. Los clientes existentes que tengan una licencia válida para un producto de ESET pueden actualizar a la versión más reciente del mismo producto de forma gratuita.

Para finalizar la instalación:

1. Haga clic en **Aceptar y continuar** para aceptar Acuerdo de licencia para el usuario final y la Política de privacidad. Si no acepta el Acuerdo de licencia para el usuario final, haga clic en **Desinstalar**. No puede volver a la versión anterior.
2. Haga clic en **Permitir todo y continuar** para permitir el Sistema de comentarios de ESET LiveGrid® o haga clic en **Continuar** si no quiere participar.
3. Tras activar el nuevo producto de ESET con la clave de licencia, se mostrará la página de inicio. Si no se encuentra la información de su licencia, continúe con una nueva licencia de prueba. Si su licencia utilizada en el producto anterior no es válida, active su producto de ESET.
4. Es necesario reiniciar el dispositivo para completar la instalación.

Actualizaciones de seguridad y estabilidad

La actualización de ESET Endpoint Antivirus es una parte esencial para mantener una protección total frente a código malicioso. Cada nueva versión de ESET Endpoint Antivirus incluye muchas mejoras y correcciones de errores. Se recomienda encarecidamente actualizar ESET Endpoint Antivirus de forma periódica para evitar que se produzcan vulnerabilidades de seguridad y amenazas. ESET Endpoint Antivirus encaja en una etapa concreta del ciclo de vida del producto como cualquier otro producto de ESET.

Más información acerca de:
Política de fin de la vida útil (productos empresariales)
Actualizaciones del producto
Revisiones de seguridad y estabilidad
Para ver información adicional sobre los cambios en ESET Endpoint Antivirus, lea el siguiente artículo de la base de conocimiento de ESET.

Las actualizaciones automáticas garantizan la seguridad y la estabilidad máximas de su producto. No puede desactivar las actualizaciones de seguridad y estabilidad.

Activación del producto

Cuando haya finalizado la instalación, se le solicitará que active el producto.

Hay varios métodos para activar su producto. La disponibilidad de una opción concreta en la ventana de activación puede variar en función del país y del medio de distribución (página web de ESET, tipo de instalador .msi o .exe, etc.).

Puede activar ESET Endpoint Antivirus en la ventana principal del programa > **Ayuda y asistencia técnica** > **Activar el producto** o **Estado de protección** > **Activar producto**.

Puede utilizar cualquiera de estos métodos para activar ESET Endpoint Antivirus:

- **Utilizar la clave de licencia adquirida**: se trata de una cadena única que presenta el formato XXXX-XXXX-XXXX-XXXX-XXXX y sirve para identificar al propietario de la licencia y activar la licencia.
- **ESET HUB**: una cuenta de ESET HUB que usted deberá crear. ESET HUB es una vía de acceso centralizada a la plataforma de seguridad unificada ESET PROTECT. Proporciona administración centralizada de identidades, suscripciones y usuarios para todos los módulos de la plataforma ESET. Puede utilizar esta opción para activar ESET Endpoint Antivirus también con herramientas de administración de licencias más antiguas: ESET Business Account o ESET MSP Administrator.
- **Archivo de licencia sin conexión**: se trata de un archivo generado automáticamente que se transferirá al producto de ESET para proporcionar información sobre la licencia. Si una licencia le permite descargar un archivo de licencia (.lf) sin conexión, ese archivo se puede utilizar para realizar la activación sin conexión. El número de licencias sin conexión se restará del número total de licencias disponibles. Si desea obtener más información sobre la generación de un archivo sin conexión, consulte la Guía del usuario de ESET Business Account.

Haga clic en **Activar más tarde** si su ordenador es miembro de una red administrada y el administrador realizará la activación remota desde ESET PROTECT. Si desea activar este cliente más tarde, también puede usar esta opción.

Si dispone de un nombre de usuario y una contraseña que utilizó para activar productos de ESET anteriores, convierta sus credenciales anteriores en una clave de licencia.

Puede cambiar la licencia del producto en cualquier momento en la ventana principal del programa > **Ayuda y asistencia técnica** > **Cambiar licencia**. Verá el ID de la licencia pública utilizado para identificar su licencia en el soporte de ESET.

ESET PROTECT puede activar ordenadores cliente de forma silenciosa con las licencias que le proporcione el administrador. Para obtener instrucciones, consulte la ayuda en línea de ESET PROTECT.

¿Se produjo un error durante la activación del producto?

Introducción de la clave de licencia durante la activación

Las actualizaciones automáticas son importantes para su seguridad. ESET Endpoint Antivirus solo recibirá las actualizaciones cuando se active con la **Clave de licencia**.

Si no introduce la clave de licencia tras la instalación del producto, este no se activará. Puede cambiar la licencia en la ventana principal del programa. Para ello, haga clic en **Ayuda y soporte técnico** > **Activar licencia**, e introduzca los datos de licencia que se le proporcionaron con el producto de seguridad de ESET en la ventana Activación del producto.

Cuando introduzca su **clave de licencia**, es importante que la escriba exactamente tal y como está escrita:

- La clave de licencia es una cadena única que presenta el formato XXXX-XXXX-XXXX-XXXX-XXXX y sirve para identificar al propietario de la licencia y activar la licencia.

Se recomienda copiar y pegar su clave de licencia desde el correo electrónico de registro para garantizar la exactitud.

Cuenta de ESET HUB

ESET HUB es una vía de acceso centralizada a la plataforma de seguridad unificada ESET PROTECT. Proporciona administración centralizada de identidades, suscripciones y usuarios para todos los módulos de la plataforma ESET. Con ESET HUB puede:

- Obtener información general sobre las suscripciones de seguridad
- Comprobar el uso y los estados de los servicios suscritos
- Asignar y controlar el acceso granular a plataformas ESET individuales
- Inicio de sesión único para todas las plataformas ESET vinculadas y accesibles

Puede utilizar esta opción de activación para activar ESET Endpoint Antivirus también con herramientas de administración de licencias más antiguas: ESET Business Account o ESET MSP Administrator.

Puede crear una cuenta de ESET HUB e iniciar sesión con su **dirección de correo electrónico** y **contraseña**.

Si ha olvidado su contraseña, haga clic en **He olvidado mi contraseña** para acceder al ESET HUB. Introduzca su dirección de correo electrónico y haga clic en **Iniciar sesión** para confirmar. A continuación, recibirá un mensaje con instrucciones sobre cómo restablecer la contraseña.

Procedimiento para usar credenciales de licencia antiguas para activar un producto ESET para equipos

Si ya tiene un nombre de usuario y una contraseña y desea recibir una clave de licencia, visite el portal de ESET Business Account, donde puede convertir sus credenciales en una nueva clave de licencia.

Error de activación

Si la activación de ESET Endpoint Antivirus no se realiza correctamente, las causas más habituales son:

- La clave de licencia ya está en uso.
- Ha introducido una clave de licencia no válida.
- La información en el formulario de activación no existe o no es válida.
- Error al establecer la comunicación con el servidor de activación.
- Sin conexión con los servidores de activación de ESET o con conexión desactivada.

Asegúrese de que ha introducido la clave de licencia adecuada o adjuntado una licencia sin conexión e intente activar el producto de nuevo.

Si no puede realizar la activación, nuestro paquete de bienvenida le servirá de guía por las preguntas frecuentes, los errores, los problemas de activación y las licencias (disponible en inglés y en otros idiomas).

- Iniciar solución de problemas de activación del producto ESET

Registro

Rellene los campos del formulario de registro y haga clic en **Continuar** para registrar su licencia. Los campos marcados entre paréntesis son obligatorios. La información se utilizará exclusivamente para cuestiones relacionadas con su licencia de ESET.

Progreso de la activación

ESET Endpoint Antivirus está en proceso de activación, esta operación puede tardar un tiempo.

La activación se ha realizado correctamente

ESET Endpoint Antivirus se ha activado correctamente. A partir de ahora, ESET Endpoint Antivirus recibirá actualizaciones periódicas para identificar las amenazas más recientes y proteger su ordenador. Haga clic en **Hecho** para finalizar la activación del producto.

Problemas de instalación comunes

Si se producen problemas durante la instalación, el asistente de instalación proporciona un solucionador de problemas que, si es posible, resuelve el problema.

Haga clic en **Ejecutar el solucionador de problemas** para iniciar el solucionador de problemas. Cuando termine el solucionador de problemas, siga la solución recomendada.

Si el problema persiste, consulte la lista de errores de instalación comunes y resoluciones.

Guía para principiantes

En este capítulo se proporciona una descripción general inicial de ESET Endpoint Antivirus y su configuración básica.

Icono en la bandeja del sistema

Algunas de las opciones y características de configuración más importantes están disponibles al hacer clic con el botón derecho del ratón en el icono de la bandeja del sistema  .

> Para acceder al menú de iconos de la bandeja del sistema (área de notificación de Windows), asegúrese de que el modo de inicio de los elementos de la interfaz de usuario esté configurado como Completo.

Pausar protección: muestra el cuadro de diálogo de confirmación que desactiva el Motor de detección, que protege contra ataques gracias al control de la comunicación realizada mediante archivos, por Internet y a través del correo electrónico. En el menú desplegable **Intervalo de tiempo** puede especificar durante cuánto tiempo se desactivará la protección.

Configuración avanzada: abre la configuración avanzada de ESET Endpoint Antivirus. Para abrir la configuración

avanzada desde la ventana principal del programa, pulse F5 en el teclado o haga clic en **Configuración** > **Configuración avanzada**.

Archivos de registro: los archivos de registro contienen información acerca de todos los sucesos importantes del programa y proporcionan información general acerca de las detecciones.

Abrir ESET Endpoint Antivirus: abre la ventana principal del programa de ESET Endpoint Antivirus desde el icono de la bandeja (área de notificación de Windows).

Restablecer disposición de la ventana: esta opción restablece el tamaño y la posición predeterminados de la ventana de ESET Endpoint Antivirus.

Modo de color: abre los ajustes de la interfaz de usuario, donde puede cambiar el color.

Buscar actualizaciones: inicia un módulo o una actualización del producto para garantizar su protección. ESET Endpoint Antivirus busca actualizaciones automáticamente varias veces al día.

Acerca de: contiene información del sistema y detalles acerca de la versión instalada de ESET Endpoint Antivirus, los módulos del programa instalados, el sistema operativo y los recursos del sistema.

Accesos directos del teclado

Para facilitar la navegación por ESET Endpoint Antivirus, puede utilizar los siguientes accesos directos del teclado:

Accesos directos del teclado	Acción
F1	abre las páginas de ayuda
F5	abre la Configuración avanzada
Flecha arriba/flecha abajo	Navegación por los elementos del menú desplegable
TAB	Ir al siguiente elemento de la interfaz gráfica de usuario en una ventana
Shift+TAB	Ir al elemento anterior de la interfaz gráfica de usuario en una ventana
ESC	cierra el cuadro de diálogo activo
Ctrl+U	muestra información sobre la licencia de ESET y su ordenador (detalles para el servicio de soporte técnico)
Ctrl+R	restablece la ventana del producto al tamaño y la posición predeterminados en la pantalla
ALT + Flecha izquierda	Volver
ALT + Flecha derecha	Ir hacia delante
ALT+Home	Ir a inicio

También puede utilizar los botones del ratón hacia atrás o hacia delante para la navegación.

Perfiles

El administrador de perfiles se utiliza en dos secciones de ESET Endpoint Antivirus: en **Análisis a petición** y en **Actualización**.

Exploración del equipo

Hay 4 perfiles de análisis predefinidos en ESET Endpoint Antivirus:

- **Análisis inteligente** – este es el perfil de análisis avanzado predeterminado. El perfil de análisis inteligente utiliza la tecnología de optimización inteligente, que excluye los archivos que se han comprobado estaban desinfectados en un análisis anterior y no se han modificado desde ese análisis. Esto permite reducir el tiempo de análisis y la repercusión en la seguridad del sistema.
- **Análisis del menú contextual** – puede iniciar un análisis a petición de cualquier archivo desde el menú contextual. El perfil de análisis del menú contextual le permite definir la configuración del análisis que se utilizará cuando active el análisis de esta forma.
- **Análisis exhaustivo** – De forma predeterminada, el perfil de análisis exhaustivo no utiliza la optimización inteligente, por lo que no se excluye ningún archivo del análisis con este perfil.
- **Análisis del ordenador** – este es el perfil predeterminado que se utiliza en el análisis estándar del ordenador.

Puede guardar sus parámetros de análisis preferidos para próximas sesiones de análisis. Le recomendamos que cree un perfil diferente (con varios objetos de análisis, métodos de análisis y otros parámetros) para cada uno de los análisis que realice con frecuencia.

Para crear un perfil nuevo, abra Configuración avanzada > **Motor de detección** > **Análisis de malware** > **Análisis a petición** > **Lista de perfiles** > **Editar**. En la ventana **Administrador de perfiles** encontrará el menú desplegable **Perfil seleccionado** con los perfiles de análisis existentes y la opción para crear uno nuevo. Si necesita ayuda para crear un perfil de análisis que se adecúe a sus necesidades, consulte la sección ThreatSense para ver una descripción de los diferentes parámetros de la configuración del análisis.

> Supongamos que desea crear su propio perfil de análisis y parte de la configuración de **Análisis del ordenador** es adecuada; sin embargo, no desea analizar los empaquetadores en tiempo real ni las aplicaciones potencialmente peligrosas y, además, quiere aplicar la opción **Reparar la detección siempre**. Introduzca el nombre del nuevo perfil en la ventana **Administrador de perfiles** y haga clic en **Agregar**. Seleccione un perfil nuevo en el menú desplegable **Perfil seleccionado**, ajuste los demás parámetros según sus requisitos y haga clic en **Aceptar** para guardar el nuevo perfil.

Actualización

El editor de perfiles de Configuración de actualizaciones le permite crear nuevos perfiles de actualización. Cree y utilice sus propios perfiles personalizados (es decir, distintos al predeterminado **Mi perfil**) únicamente si su ordenador utiliza varios medios para conectarse a servidores de actualización.

Por ejemplo, un ordenador portátil que normalmente se conecta a un servidor local (Mirror) de la red local, pero descarga las actualizaciones directamente desde los servidores de actualización de ESET cuando se desconecta de la red local (en viajes de negocios) podría utilizar dos perfiles: el primero para conectarse al servidor local y el segundo, a los servidores de ESET. Una vez configurados estos perfiles, seleccione **Herramientas** > **Planificador de tareas** y modifique los parámetros de la tarea de actualización. Designe un perfil como principal y el otro, como secundario.

Perfil de actualización: el perfil de actualización utilizado actualmente. Para cambiarlo, seleccione un perfil en el menú desplegable.

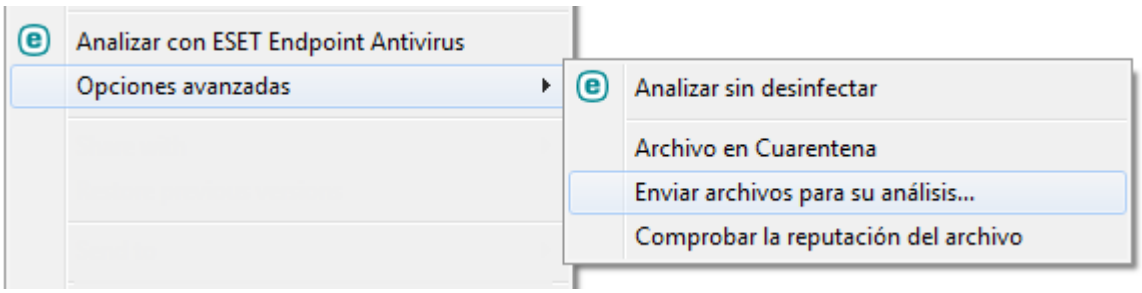
Lista de perfiles: cree perfiles de actualización nuevos o quite los actuales.

Menú contextual

El menú contextual aparece al hacer clic con el botón derecho en un objeto (archivo). En el menú se muestra una lista de todas las acciones que se pueden realizar en un objeto.

Puede integrar elementos de control de ESET Endpoint Antivirus en el menú contextual. La opción de configuración de esta funcionalidad está disponible en Configuración avanzada > **Interfaz de usuario** > **Elementos de la interfaz del usuario**.

Integrar en el menú contextual: integra los elementos de control de ESET Endpoint Antivirus en el menú contextual.

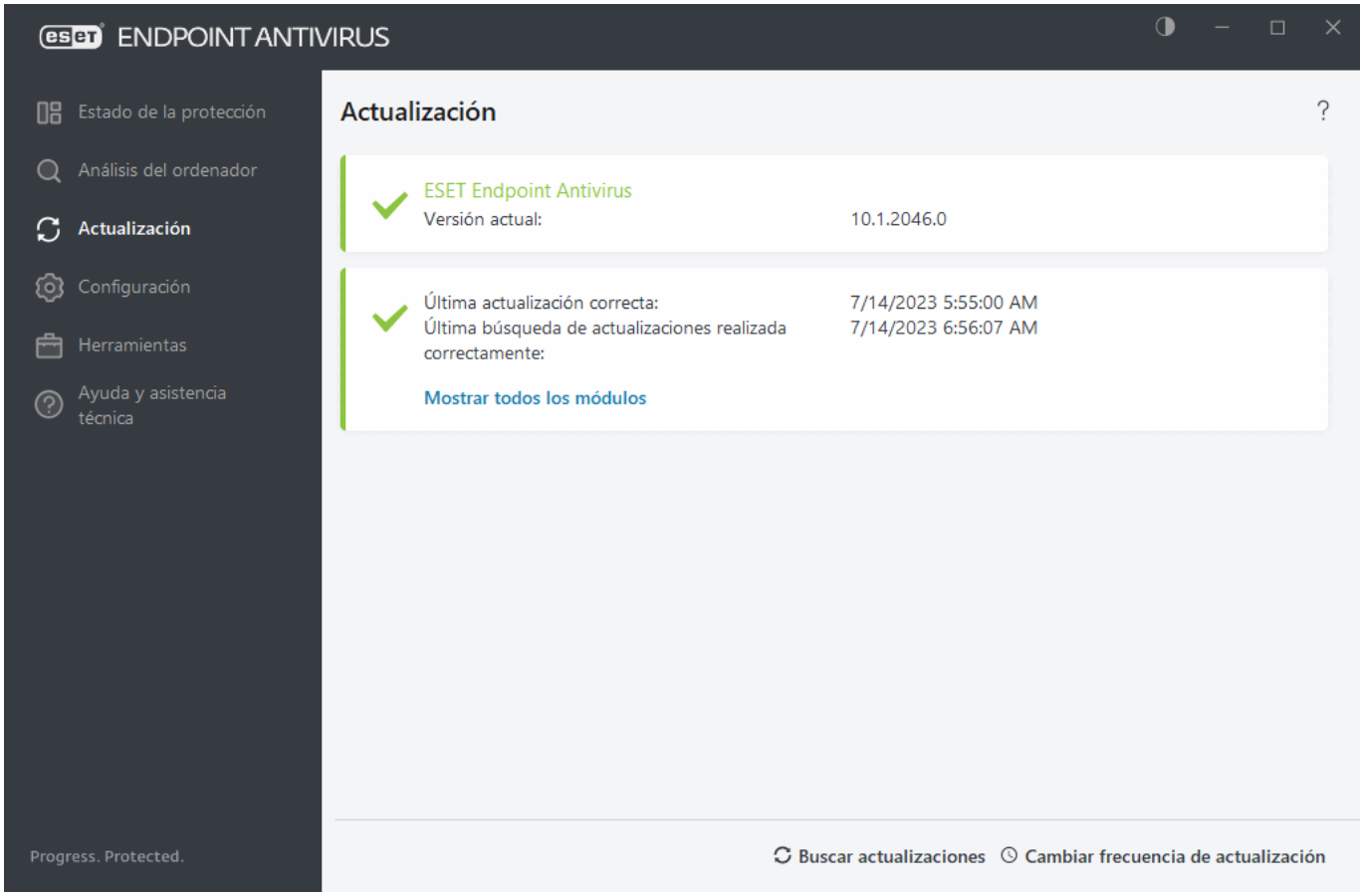


Configuración de actualizaciones

La mejor manera de disfrutar de la máxima seguridad en el ordenador es actualizar ESET Endpoint Antivirus periódicamente. El módulo de actualización garantiza que los módulos del programa y los componentes del sistema están siempre actualizados.

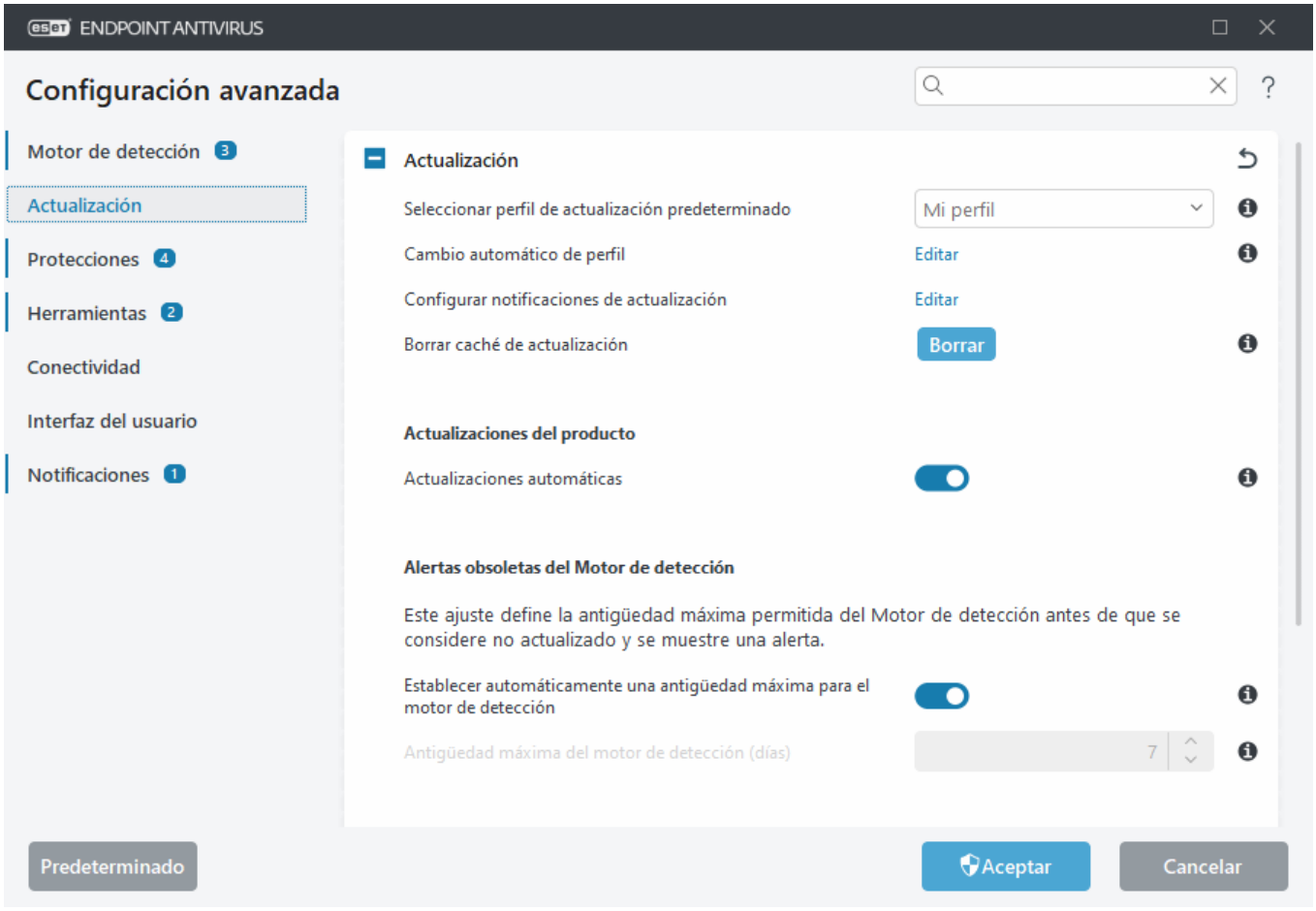
Haga clic en **Actualizar** en la ventana principal del programa para consultar el estado de la actualización, la fecha y la hora de la última actualización, y si es necesario actualizar el programa.

Además de las actualizaciones automáticas, puede hacer clic en **Buscar actualizaciones** para activar una actualización manual.



Configuración avanzada > **La actualización** contiene opciones de actualización adicionales como el modo de actualización, el acceso al servidor proxy y las conexiones LAN.

Si está experimentando problemas con una actualización, haga clic en **Borrar** para borrar la caché de actualización. Si aún así no puede actualizar los módulos del programa, consulte la sección Solución de problemas para el mensaje "Error de actualización de los módulos".

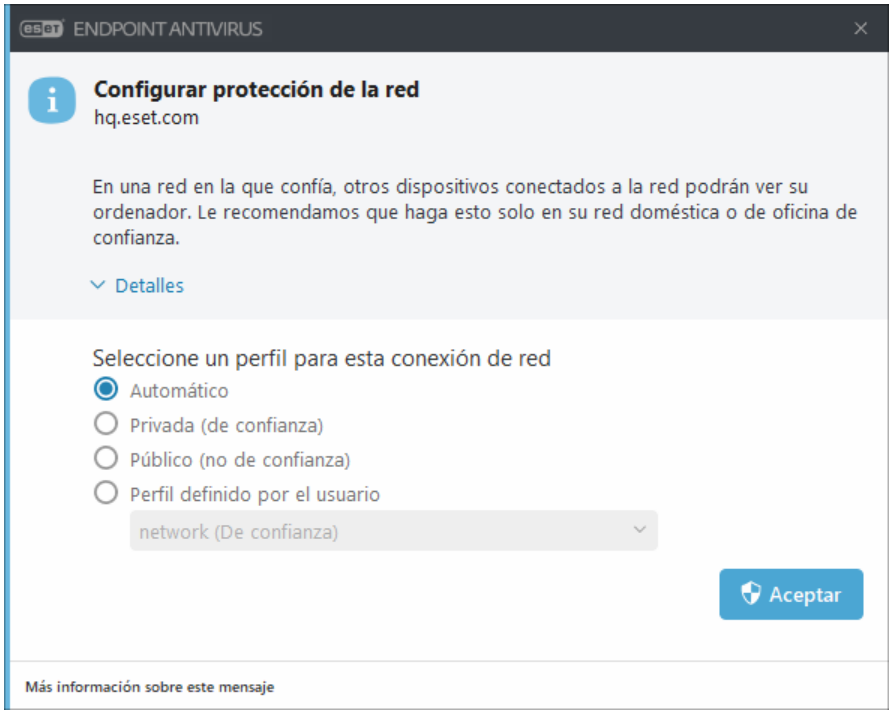


La opción **Elegir automáticamente** de Configuración avanzada > **Actualizaciones** > **Perfiles** > **Actualizaciones** > **Actualizaciones de los módulos** está activada de forma predeterminada. Si se usa un servidor de actualización de ESET para recibir actualizaciones, se recomienda que mantenga la opción tal cual está.

Para lograr una funcionalidad óptima, el programa debe actualizarse automáticamente. Las actualizaciones automáticas solo están disponibles si se introduce la clave de licencia correcta en **Ayuda y asistencia técnica** > **Activar producto**. Si no introdujo la clave de licencia tras la instalación, puede hacerlo en cualquier momento. Para obtener información detallada sobre la activación, consulte Cómo activar ESET Endpoint Antivirus.

Configurar protección de la red

De forma predeterminada, ESET Endpoint Antivirus utiliza la configuración de Windows cuando se detecta una nueva red. Para mostrar una ventana de diálogo cuando se detecta una nueva red, cambie la asignación del perfil de protección de red a **Preguntar**. La configuración de la protección de la red se muestra siempre que su ordenador se conecta a una red nueva.



Puede seleccionar entre los siguientes Perfiles de conexión de red:

Automático:ESET Endpoint Antivirus seleccionará el perfil automáticamente, en función de los activadores configurados para cada perfil.

Privado: para una red de confianza (red doméstica o de oficina). El ordenador y los archivos compartidos almacenados en el ordenador son visibles para otros usuarios de la red, y los recursos del sistema están disponibles para otros usuarios de la red (el acceso a los archivos y las impresoras compartidos está activado, la comunicación RPC entrante está activada y el escritorio remoto compartido está disponible). Se recomienda utilizar esta configuración al acceder a una red local segura. Este perfil se asigna automáticamente a una conexión de red si está configurado como Dominio o Red privada en Windows.

Pública: para una red que no es de confianza (red pública). Los archivos y las carpetas de su sistema no se comparten ni son visibles para otros usuarios de la red, y el uso compartido de recursos del sistema está desactivado. Se recomienda utilizar esta configuración al acceder a las redes inalámbricas. Este perfil se asigna automáticamente a cualquier conexión de red que no esté configurada como Dominio o Red privada en Windows.

Perfil definido por el usuario: puede seleccionar un perfil que haya creado en el menú desplegable. Esta opción solo está disponible si ha creado al menos un perfil personalizado.

⚠ Una configuración de red incorrecta puede exponer su ordenador a riesgos para la seguridad.

Hashes bloqueados

Usar ESET Inspect en el entorno permite a los administradores bloquear el acceso a los ejecutables especificados según el hash. Si el administrador bloquea el acceso a un archivo ejecutable y usted intenta acceder a él, ESET Endpoint Antivirus muestra esta notificación:

Acceso al archivo bloqueado: la aplicación (se muestra el nombre de la aplicación) intentó acceder a un archivo que el administrador no permite.

Si usted es el administrador y desea permitir el acceso a la aplicación especificada en la notificación, consulte Hashes bloqueados en la ayuda en línea de ESET Inspect. Si usted es un usuario y desea cambiar el comportamiento de la aplicación, póngase en contacto con el administrador.

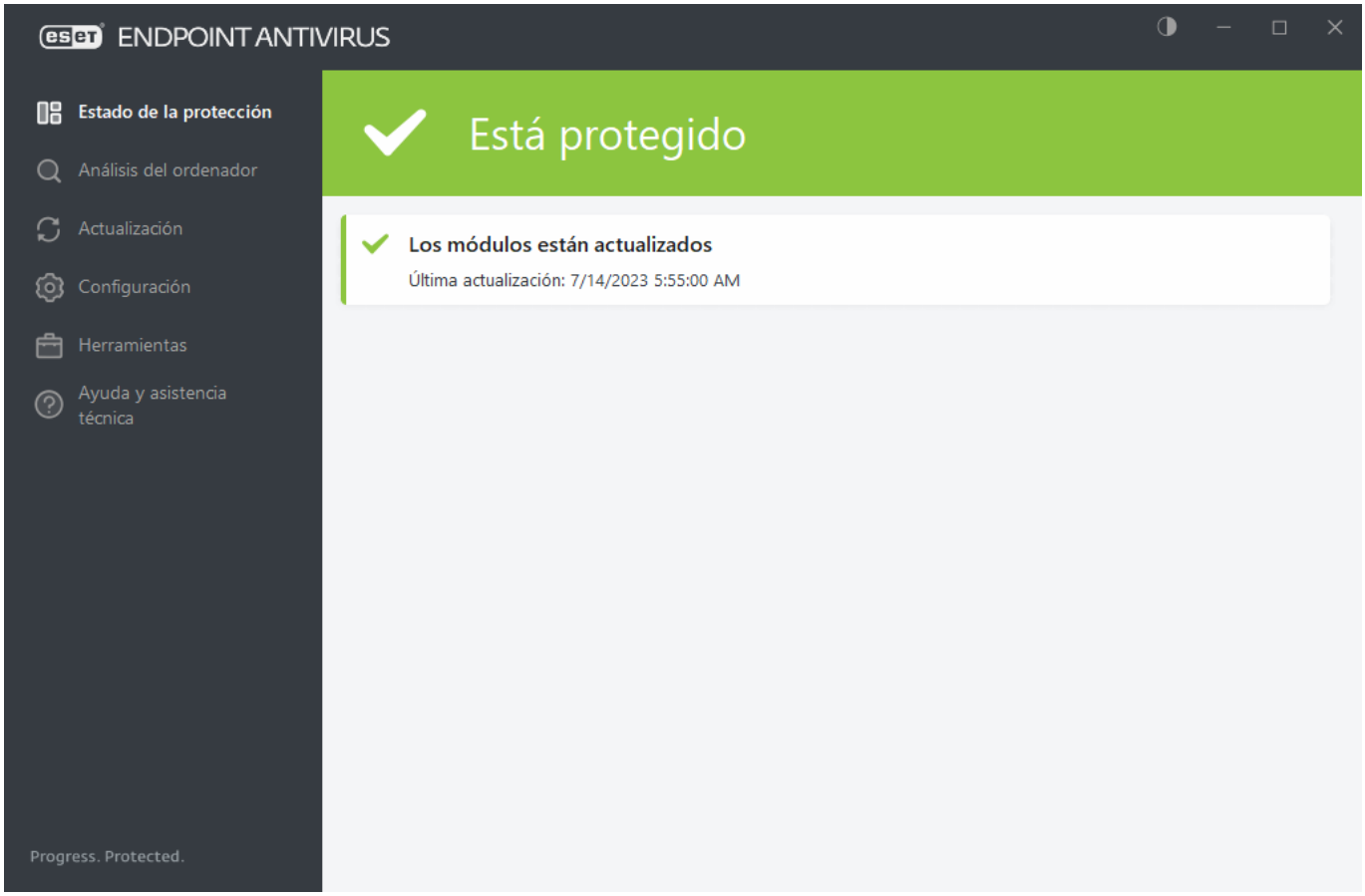
Trabajo con ESET Endpoint Antivirus

La ventana principal del programa de ESET Endpoint Antivirus está dividida en dos secciones principales. En la ventana principal, situada a la derecha, se muestra información relativa a la opción seleccionada en el menú principal de la izquierda.

> **Instrucciones con ilustraciones**
> Consulte Abrir la ventana principal del programa de los productos de ESET para Windows para obtener instrucciones con ilustraciones disponibles en inglés y en otros idiomas.

Puede seleccionar el esquema de colores de la interfaz gráfica de usuario de ESET Endpoint Antivirus en la esquina superior derecha de la ventana principal del programa. Haga clic en el icono **Esquema de colores** (el icono cambia en función del esquema de colores seleccionado actualmente) junto al icono **Minimizar** y seleccione el esquema de colores en el menú desplegable:

- **Igual que el color del sistema**: define el esquema de colores de ESET Endpoint Antivirus según la configuración del sistema operativo.
- **Oscuro**: ESET Endpoint Antivirus tendrá un esquema de colores oscuros (modo oscuro).
- **Claro**: ESET Endpoint Antivirus tendrá un esquema de colores estándar y claro.



Opciones del menú principal:

Estado de la protección: proporciona información sobre el estado de protección de ESET Endpoint Antivirus.

Análisis del ordenador: configure e inicie un análisis de su ordenador o cree un análisis personalizado.

Actualización: muestra información sobre las actualizaciones del módulo y el motor de detección.

Herramientas – Funciones que ayudan a simplificar la administración del programa y ofrecen opciones adicionales para usuarios avanzados.

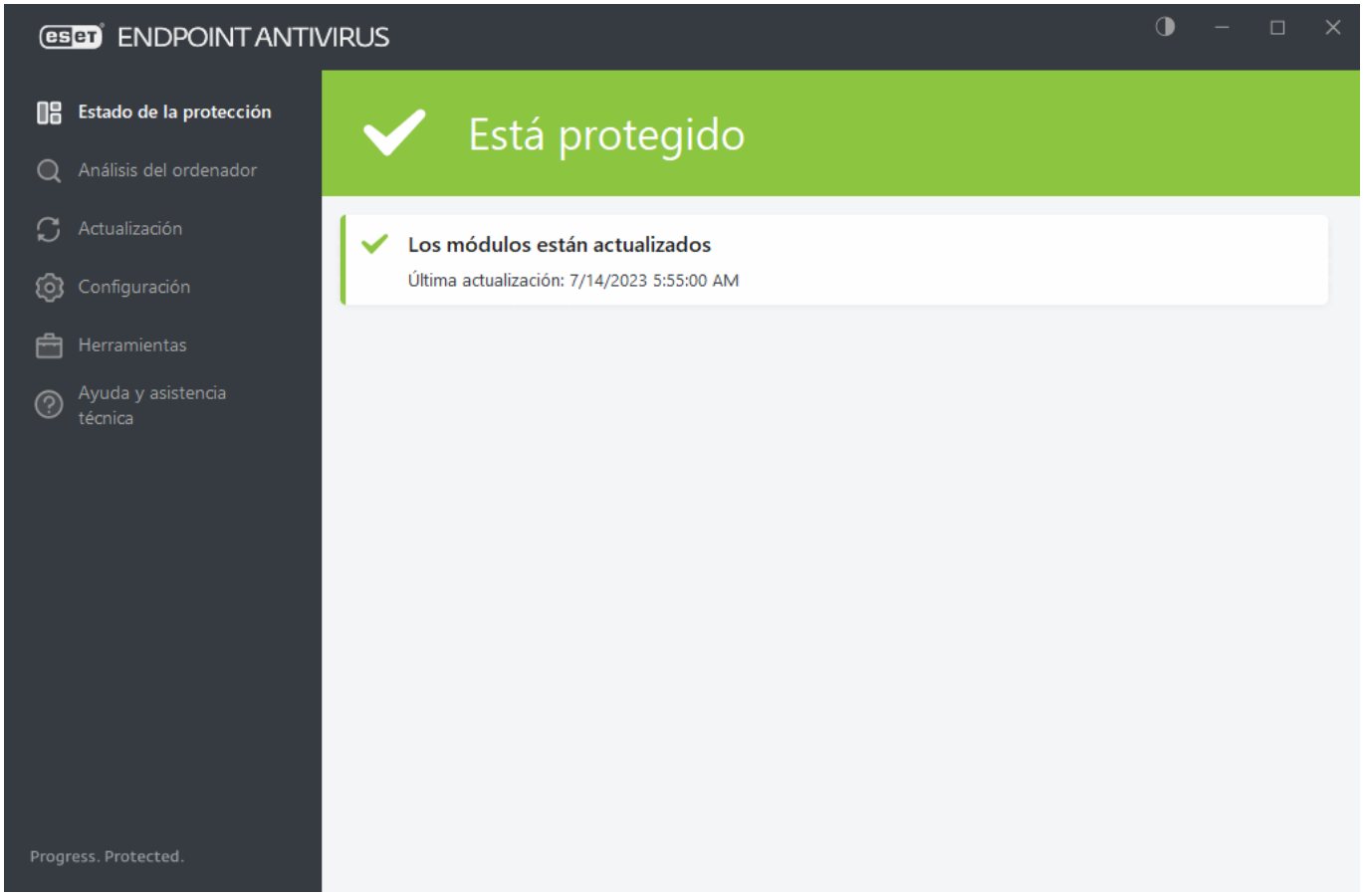
Configuración: ofrece opciones de configuración para las funciones de protección de ESET Endpoint Antivirus y acceso a la Configuración avanzada.

Ayuda y asistencia técnica: muestra información sobre la licencia, el producto de ESET instalado y vínculos a la ayuda en línea, la base de conocimiento de ESET y el soporte técnico.

Estado de protección

La ventana **Estado de protección** muestra información sobre la protección actual del ordenador y la última actualización. El icono de estado verde de **Máxima protección** indica que se garantiza la protección máxima.

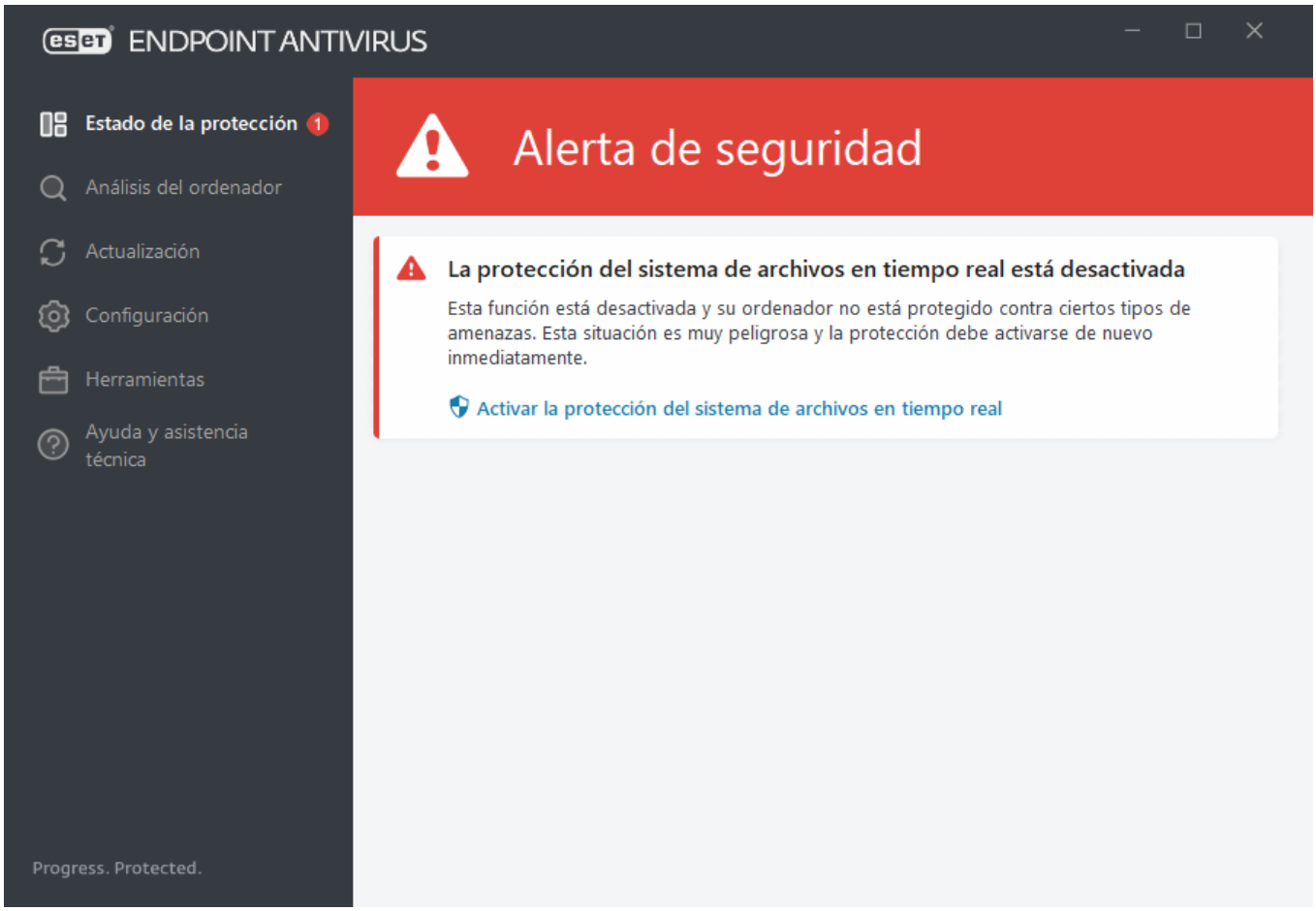
En la ventana **Estado de protección** se muestran notificaciones con información detallada y soluciones recomendadas para mejorar la seguridad de ESET Endpoint Antivirus, activar funciones adicionales o garantizar la máxima protección.



El icono de color verde y el estado **Está protegido** verde indican que se garantiza la máxima protección.

Qué hacer si el programa no funciona correctamente

Una marca de verificación verde aparecerá junto a todos los módulos del programa que estén totalmente operativos. Si un módulo necesita atención, aparecerá un signo de exclamación rojo o un icono de notificación naranja. En la parte superior de la ventana aparecerá información adicional sobre el módulo, incluyendo nuestra recomendación sobre cómo restaurar todas las funcionalidades. Para cambiar el estado de un módulo, haga clic en **Configuración** en el menú principal y, a continuación, en el módulo deseado.



El icono del signo de exclamación rojo (!) indica que no se garantiza la protección máxima del ordenador. Podría encontrarse con este tipo de notificación en las siguientes situaciones:

- **La protección antivirus y antiespía está en pausa**: haga clic en **Iniciar todos los módulos de protección antivirus y antispyware** para volver a activar la protección antivirus y antiespía en el panel **Estado de protección** o **Activar la protección antivirus y antiespía** en el panel **Configuración** en la ventana principal del programa.
- La protección antivirus no está operativa: se ha producido un error al inicializar el análisis de virus. La mayoría de los módulos de ESET Endpoint Antivirus no funcionarán correctamente.
- **La protección Anti-Phishing no está operativa**: esta función no está operativa porque otros módulos necesarios del programa no están activos.
- **El Motor de detección no está actualizado**: este error aparecerá tras varios intentos sin éxito de actualizar el motor de detección (llamado antes base de firmas de virus). Le recomendamos que compruebe la configuración de actualización. La causa más frecuente de este error es la introducción incorrecta de los datos de autenticación o una mala configuración de la conexión.
- **El producto no está activado** o **Su licencia está vencida**: esto se indica mediante un icono de estado de protección. Una vez que caduque la licencia, el programa no se puede actualizar. Siga las instrucciones de

la ventana de alerta para renovar la licencia.

- **El sistema de prevención de intrusiones basado en el host (HIPS) está desactivado**: este problema se indica cuando HIPS está desactivado. Su ordenador no está protegido contra ciertos tipos de amenazas y la protección debería volver a activarse de forma inmediata haciendo clic en **Activar HIPS**.
- **No hay actualizaciones regulares programadas**: ESET Endpoint Antivirus no buscará ni recibirá actualizaciones importantes a menos que programe la tarea de actualización.
- **Acceso a la red bloqueado**: se muestra cuando se activa la tarea del cliente **Aislar ordenador de la red** de esta estación de trabajo desde ESET PROTECT. Póngase en contacto con el administrador del sistema si desea más información.
- **La protección del sistema de archivos en tiempo real está en pausa**: el usuario desactivó la protección en tiempo real. Su ordenador no está protegido frente a amenazas. Haga clic en Activar protección en tiempo real para volver a activar esta funcionalidad.

 La "i" naranja indica que un problema no grave del producto de ESET requiere su atención. Los posibles motivos son:

- **La protección del tráfico de Internet está desactivada**: haga clic en la notificación de seguridad para volver a activar la protección del tráfico de Internet y, a continuación, haga clic en **Activar la protección del acceso a la Web**.
- **La licencia caduca en breve/Su licencia caduca hoy**: esto se indica mediante el icono de estado de la protección, que muestra un signo de exclamación junto. Cuando expire la licencia, el programa no se podrá actualizar y el icono del estado de la protección se volverá rojo.
- **El antispam del cliente de correo electrónico correo electrónico está en pausa**: haga clic en **Activar Antispam del cliente de correo electrónico de correo electrónico** para volver a activar esta función.
- **El Control web está en pausa**: haga clic en **Habilitar control de acceso web para volver a activar esta función**.
- **Anulación de política activa**: la configuración definida por la política está anulada temporalmente, posiblemente hasta que finalice la solución de problemas. Solo el usuario autorizado podrá anular la configuración de la política. Para obtener más información, consulte Cómo utilizar el modo de anulación.
- **Se pausó el control de dispositivos**: haga clic en **Activar el control de dispositivos** para volver a activar esta función.

Para ajustar los estados de visibilidad en el producto en el primer panel de ESET Endpoint Antivirus, consulte Estados de la aplicación.

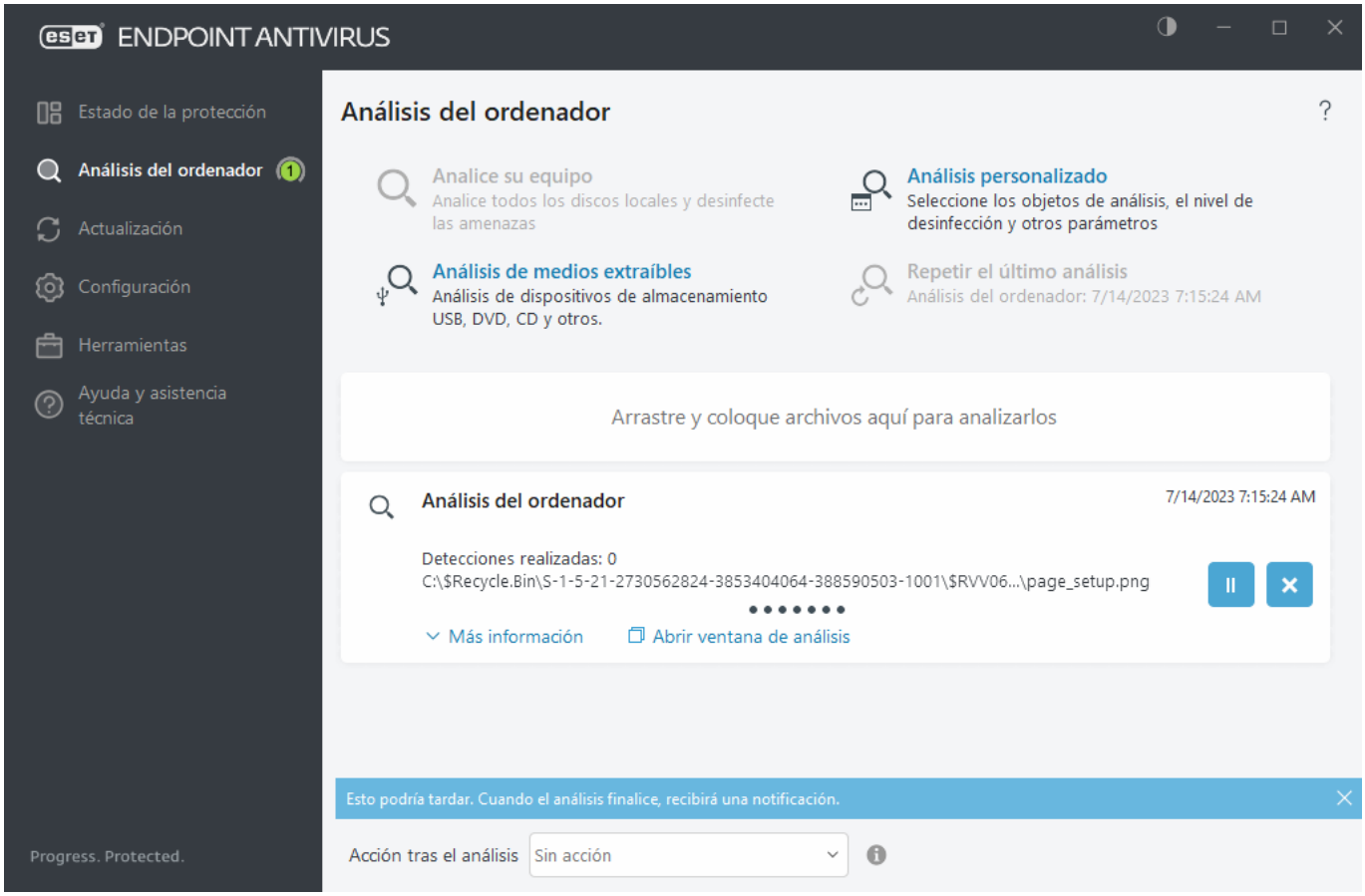
Si no consigue solucionar el problema con estas sugerencias, haga clic en **Ayuda y soporte** para acceder a los archivos de ayuda o realice una búsqueda en la base de conocimiento de ESET. Si todavía necesita ayuda, puede enviar una solicitud de soporte. El servicio de soporte técnico de ESET responderá a sus preguntas y le ayudará a encontrar una solución rápidamente.

> Si un estado pertenece a una función bloqueada por la política de ESET PROTECT, no podrá hacer clic en el enlace.

Exploración del equipo

El análisis a petición es una parte importante de ESET Endpoint Antivirus. Se utiliza para realizar análisis de archivos y carpetas en su ordenador. Desde el punto de vista de la seguridad, es esencial que los análisis del ordenador no se ejecuten únicamente cuando se sospecha que existe una infección, sino que se realicen periódicamente como parte de las medidas de seguridad rutinarias. Le recomendamos que realice un análisis en

profundidad de su sistema periódicamente (por ejemplo, una vez al mes) para detectar virus que la Protección del sistema de archivos en tiempo real no haya detectado. Este fallo puede deberse a que la protección del sistema de archivos en tiempo real no estaba activada en ese momento, a que el motor de detección estaba obsoleto o a que el archivo no se detectó como un virus cuando se guardó en el disco.



Están disponibles dos tipos de **Análisis del ordenador**. **Análisis del ordenador** analiza el sistema rápidamente, sin necesidad de configuración adicional de los parámetros de análisis. **Análisis personalizado** le permite seleccionar cualquiera de los perfiles de análisis predefinidos y definir objetos de análisis específicos.

Consulte Progreso del análisis para obtener más información sobre el proceso de análisis.

Analice su equipo

Análisis del ordenador le permite iniciar rápidamente un análisis del ordenador y desinfectar los archivos infectados sin la intervención del usuario. La ventaja de este tipo de **análisis del ordenador** es su sencillo funcionamiento, sin configuraciones de análisis detalladas. El análisis comprueba todos los archivos de las unidades locales y desinfecta o elimina automáticamente las amenazas detectadas. El nivel de desinfección se establece automáticamente en el valor predeterminado. Para obtener más información detallada sobre los tipos de desinfección, consulte Desinfección.

También puede utilizar la función **Análisis mediante arrastrar y colocar** para analizar un archivo o una carpeta manualmente al hacer clic en el archivo o la carpeta, desplazar el cursor del ratón hasta la zona marcada mientras se mantiene pulsado el botón del ratón, para después soltarlo. Después, la aplicación pasa al primer plano.

En **Análisis avanzados** están disponibles las siguientes opciones de análisis:

Análisis personalizado

La opción **Análisis personalizado** le permite especificar parámetros de análisis como, por ejemplo, objetos y métodos de análisis. La ventaja del **Análisis personalizado** es que puede configurar los parámetros detalladamente. Las diferentes configuraciones se pueden guardar en perfiles de análisis definidos por el usuario, que pueden resultar útiles si el análisis se realiza varias veces con los mismos parámetros.

Análisis de medios extraíbles

Al igual que **Análisis del ordenador**, inicia rápidamente el análisis de medios extraíbles (como CD/DVD/USB) que están actualmente conectados al ordenador. Esto puede resultar útil cuando conecta una unidad flash USB a un ordenador y desea analizar su contenido por si contiene código malicioso u otras posibles amenazas.

Este tipo de análisis también se puede iniciar haciendo clic en **Análisis personalizado**, en **Medios extraíbles** en el menú desplegable **Objetos de análisis** y, a continuación, en **Analizar**.

Repetir el último análisis

Permite iniciar rápidamente el análisis realizado previamente con los mismos ajustes con los que se ejecutó.

En el menú desplegable **Acción tras el análisis** puede establecer la acción que desea efectuar automáticamente cuando concluya el análisis:

- **Sin acciones**: cuando el análisis concluya no se realizará ninguna acción.
- **Apagar**: el ordenador se apaga cuando finaliza el análisis.
- **Reiniciar si es necesario**: el ordenador se reinicia solo si es necesario para completar la desinfección de las amenazas detectadas.
- **Reiniciar**: cierra todos los programas abiertos y reinicia el ordenador cuando concluye el análisis.
- **Forzar reinicio si es necesario**: el ordenador fuerza el reinicio solo si es necesario para completar la desinfección de las amenazas detectadas.
- **Forzar reinicio**: fuerza el cierre de todos los programas abiertos sin esperar la intervención del usuario y reinicia el ordenador cuando concluye el análisis.
- **Suspender**: guarda la sesión y establece el ordenador en un estado de bajo consumo para que pueda retomar su trabajo rápidamente.
- **Hibernar**: recopila todos los programas y archivos que se encuentran en ejecución en la RAM y los guarda en un archivo especial de su disco duro. El ordenador se apaga, pero la próxima vez que lo encienda presentará el estado anterior al apagado.

> **i** Las acciones **Suspender** o **Hibernar** estarán disponibles según la configuración de las opciones de encendido y suspensión del sistema operativo de su ordenador o las prestaciones correspondientes. Debe tener en cuenta que cuando el ordenador está en suspensión sigue en funcionamiento. Sigue ejecutando funciones básicas y utilizando electricidad si funciona con la alimentación de la batería. Si desea ahorrar carga de la batería, por ejemplo al salir de la oficina, le recomendamos utilizar la opción Hibernar.

La acción seleccionada se iniciará cuando finalicen todos los análisis que se están ejecutando. Cuando se seleccione **Apagar** o **Reiniciar**, se mostrará un cuadro de diálogo de confirmación de apagado con una cuenta atrás de 30 segundos (haga clic en **Cancelar** para desactivar la acción solicitada).

Le recomendamos que ejecute un análisis del ordenador una vez al mes como mínimo. El análisis se puede configurar como una tarea programada en **Herramientas** > **Tareas programadas**. ¿Cómo programar un análisis del ordenador semanal?

Iniciador del análisis personalizado

Puede utilizar el Análisis personalizado para analizar la memoria operativa, la red o determinadas partes de un disco, en lugar del disco al completo. Para ello, haga clic en **Análisis avanzados** > **Análisis personalizado** y seleccione objetos específicos en la estructura de carpetas (árbol).

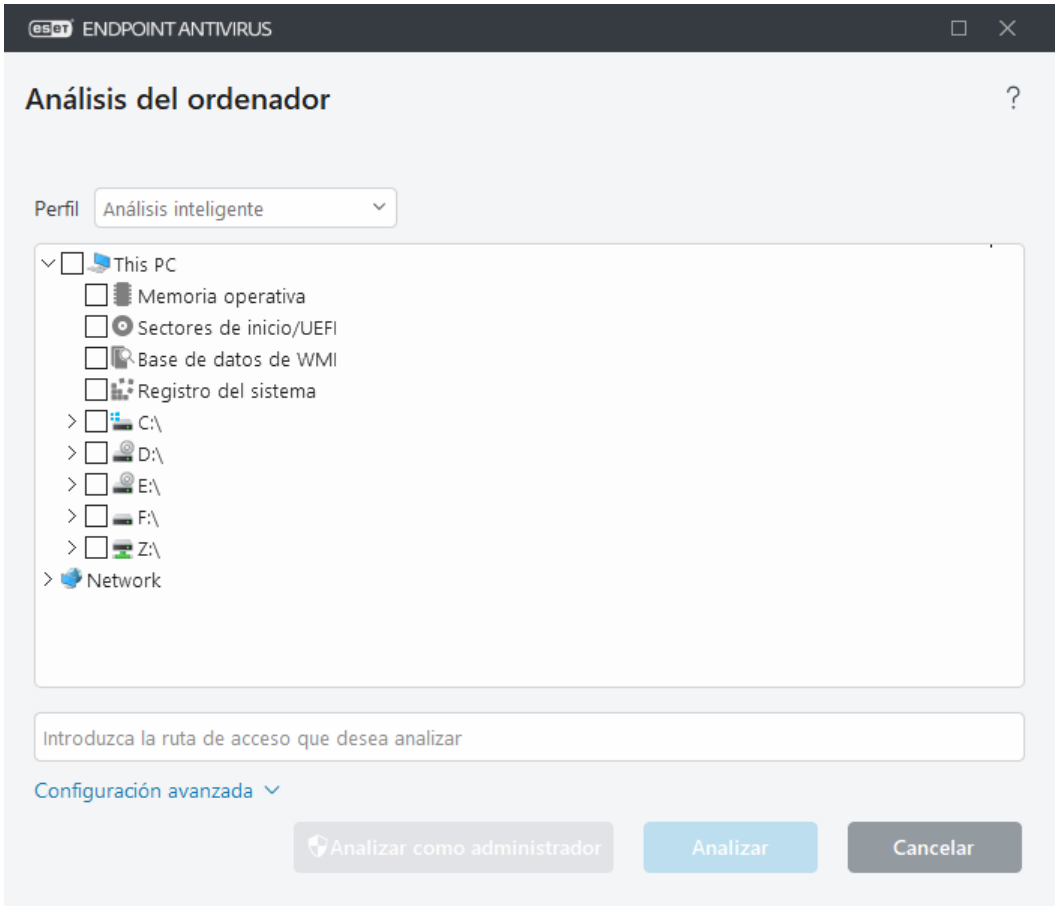
Puede elegir un perfil en el menú desplegable **Perfil** que se utilizará al analizar objetos concretos. El perfil predeterminado es **Análisis inteligente**. Hay otros tres perfiles de análisis predefinidos llamados **Análisis en profundidad**, **Análisis del menú contextual** y **Análisis del ordenador**. Estos perfiles de análisis estándar utilizan distintos parámetros de ThreatSense. Las opciones disponibles se describen en Configuración avanzada > **Motor de detección** > **Análisis de malware** > **Análisis a petición** > ThreatSense.

La estructura (de árbol) de carpetas también contiene objetos de análisis específicos.

- **Memoria operativa**: analiza todos los procesos y datos que actualmente utiliza la memoria operativa.
- **Sectores de inicio/UEFI**: analiza los sectores de inicio y la UEFI en busca de malware. Puede obtener más información sobre el análisis UEFI en el glosario.
- **Base de datos de WMI**: analiza toda la base de datos de Windows Management Instrumentation (WMI), todos los espacios de nombres, todas las instancias de clase y todas las propiedades. Busca referencias a archivos infectados o malware incrustados como datos.
- **Registro del sistema**: analiza todo el registro del sistema, todas las claves y todas las subclaves. Busca referencias a archivos infectados o malware incrustados como datos. Durante la desinfección de las detecciones, la referencia permanece en el registro para garantizar que no se pierda ningún dato importante.

Para ir rápidamente a un objeto de análisis (archivo o carpeta), escriba su ruta en el campo de texto que aparece debajo de la estructura de árbol. La ruta distingue entre mayúsculas y minúsculas. Para incluir el objeto en el análisis, marque su casilla de verificación en la estructura de árbol.

Cómo programar un análisis del ordenador semanal
Para programar una tarea periódica, lea el capítulo Cómo programar un análisis del ordenador semanal.



Puede configurar los parámetros de desinfección del análisis en Configuración avanzada > **Motor de detección** > **Análisis de malware** > **Análisis a petición** > **ThreatSense** > **Desinfección**. Para ejecutar un análisis sin desinfección, haga clic en **Configuración avanzada** y seleccione **Analizar sin desinfectar**. El historial de análisis se guarda en el registro del análisis.

Cuando se selecciona **Ignorar exclusiones**, se analizan sin excepciones los archivos con extensiones excluidas anteriormente del análisis.

Haga clic en **Analizar** para ejecutar el análisis con los parámetros personalizados que ha definido.

Analizar como administrador le permite ejecutar el análisis con la cuenta de administrador. Utilice esta opción si el usuario actual no tiene privilegios para acceder a los archivos que desea analizar. Este botón no está disponible si el usuario actual no puede realizar operaciones de control de cuentas de usuario como administrador.

Si hace clic en Mostrar registro, se mostrará el registro de análisis del ordenador cuando dicho análisis concluya.

Progreso del análisis

En la ventana de progreso del análisis se muestra el estado actual del análisis e información sobre el número de archivos en los que se ha detectado código malicioso.

Es normal que algunos archivos, como los archivos protegidos con contraseña o que son utilizados exclusivamente por el sistema (por lo general, archivos *pagefile.sys* y determinados archivos de registro), no se puedan analizar. Puede obtener más información en nuestro artículo de la base de conocimiento.

> **Cómo programar un análisis del ordenador semanal**
> Para programar una tarea periódica, lea el capítulo Cómo programar un análisis del ordenador semanal.

Progreso del análisis: la barra de progreso muestra el estado del análisis en ejecución.

Objeto: el nombre y la ubicación del objeto que se está analizando.

Detecciones realizadas: muestra el número total de objetos analizados, las amenazas encontradas y las desinfectadas durante un análisis.

Haga clic en Más información para mostrar la siguiente información:

- **Usuario**: nombre de la cuenta de usuario que inició el análisis.
- **Objetos analizados**: número de objetos ya analizados.
- **Duración**: tiempo transcurrido.

Icono de pausa: pausa un análisis.

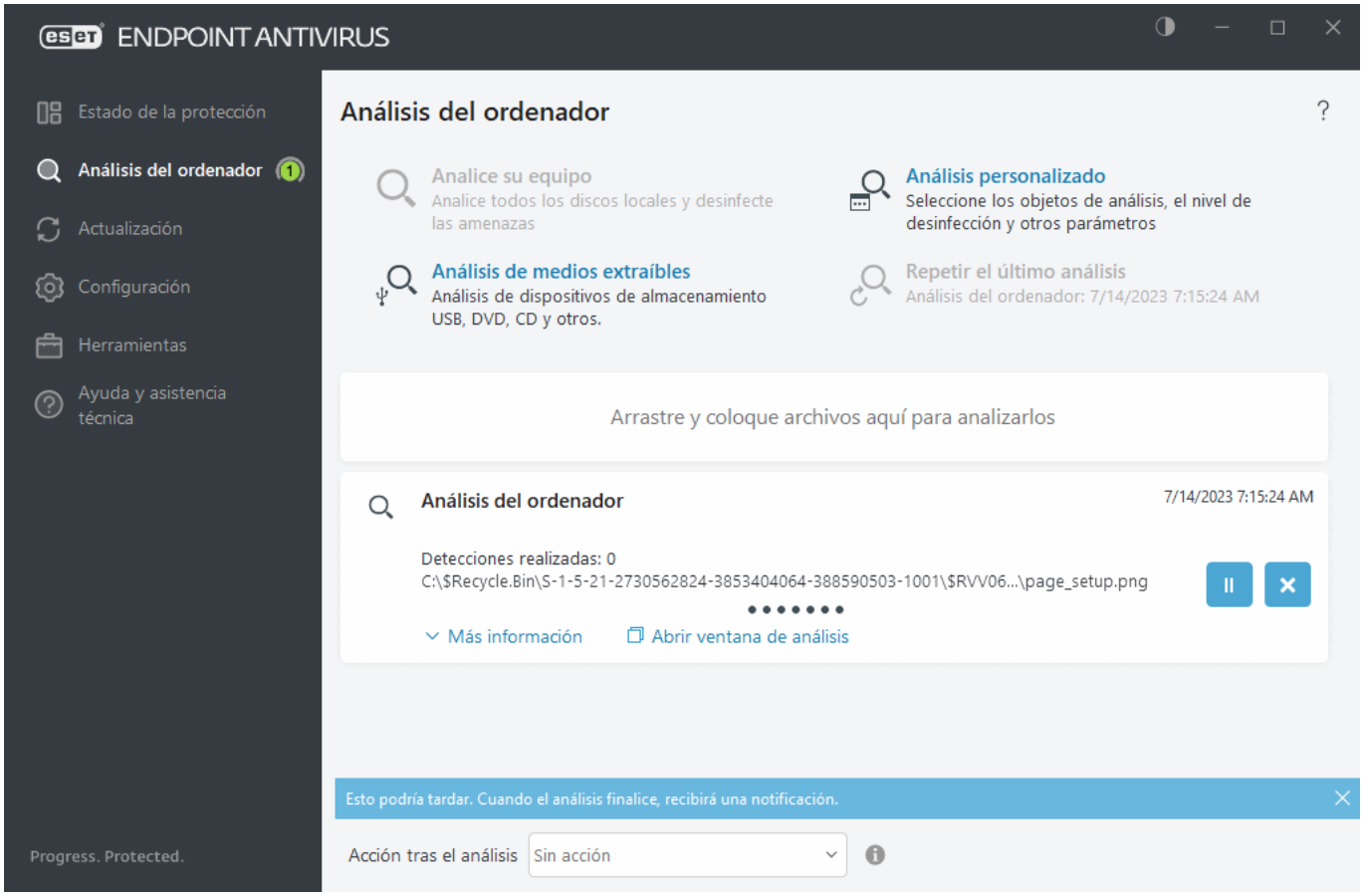
Icono de reanudación: esta opción está visible cuando el progreso del análisis está en pausa. Haga clic en el icono para seguir analizando.

Icono de detención: finaliza el análisis.

Haga clic en **Abrir ventana de análisis** para abrir el Registro de análisis del ordenador, donde puede consultar más detalles sobre el análisis.

Desplazarse por el registro de exploración: si esta opción está activada, el registro de análisis se desplaza automáticamente a medida que se añaden entradas nuevas, de modo que se visualizan las entradas más recientes.

> Haga clic en la lupa o en la flecha para ver los detalles acerca del análisis que se está ejecutando en ese momento. Puede ejecutar otro análisis paralelo haciendo clic en **Análisis del ordenador** o **Análisis avanzados** > **Análisis personalizado**.



En el menú desplegable **Acción tras el análisis** puede establecer la acción que desea efectuar automáticamente cuando concluya el análisis:

- **Sin acciones**: cuando el análisis concluya no se realizará ninguna acción.
- **Apagar**: el ordenador se apaga cuando finaliza el análisis.
- **Reiniciar si es necesario**: el ordenador se reinicia solo si es necesario para completar la desinfección de las amenazas detectadas.
- **Reiniciar**: cierra todos los programas abiertos y reinicia el ordenador cuando concluye el análisis.
- **Forzar reinicio si es necesario**: el ordenador fuerza el reinicio solo si es necesario para completar la desinfección de las amenazas detectadas.
- **Forzar reinicio**: fuerza el cierre de todos los programas abiertos sin esperar la intervención del usuario y reinicia el ordenador cuando concluye el análisis.
- **Suspender**: guarda la sesión y establece el ordenador en un estado de bajo consumo para que pueda retomar su trabajo rápidamente.
- **Hibernar**: recopila todos los programas y archivos que se encuentran en ejecución en la RAM y los guarda en un archivo especial de su disco duro. El ordenador se apaga, pero la próxima vez que lo encienda presentará el estado anterior al apagado.

Las acciones **Suspender** o **Hibernar** estarán disponibles según la configuración de las opciones de encendido y suspensión del sistema operativo de su ordenador o las prestaciones correspondientes. Debe tener en cuenta que cuando el ordenador está en suspensión sigue en funcionamiento. Sigue ejecutando funciones básicas y utilizando electricidad si funciona con la alimentación de la batería. Si desea ahorrar carga de la batería, por ejemplo al salir de la oficina, le recomendamos utilizar la opción Hibernar.

La acción seleccionada se iniciará cuando finalicen todos los análisis que se están ejecutando. Cuando se seleccione **Apagar** o **Reiniciar**, se mostrará un cuadro de diálogo de confirmación de apagado con una cuenta atrás de 30 segundos (haga clic en **Cancelar** para desactivar la acción solicitada).

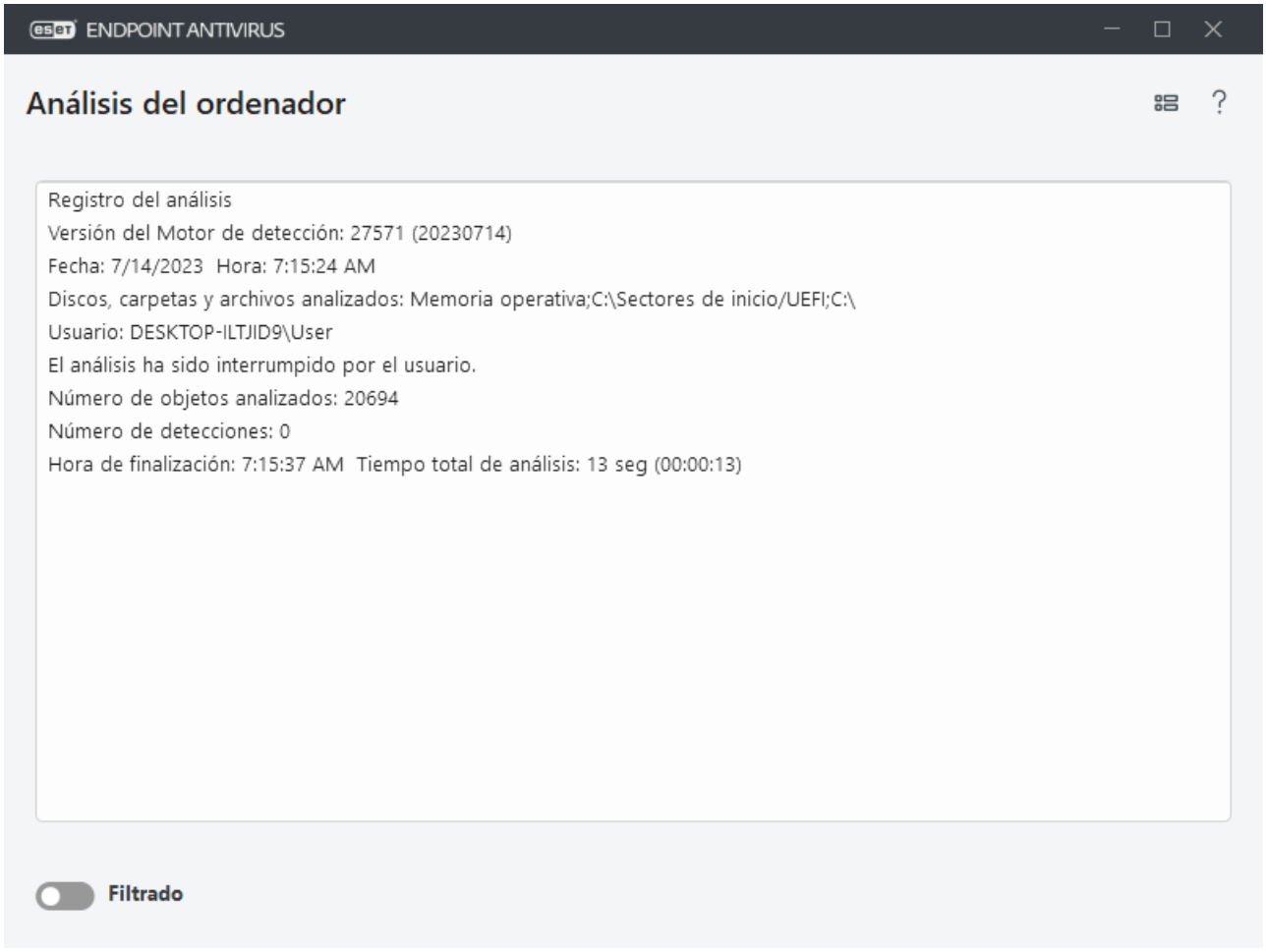
Registro de análisis del ordenador

Puede ver información detallada relacionada con un análisis específico en Archivos de registro. El registro de análisis contiene la siguiente información:

- Versión del motor de detección
- Fecha y hora de inicio
- Lista de discos, carpetas y archivos analizados
- Nombre del análisis programado (solo análisis programado)
- Usuario que inició el análisis.
- Estado del análisis
- Número de objetos analizados
- Número de detecciones encontradas
- Hora de finalización
- Tiempo total de análisis

> Se omite el nuevo inicio de una tarea programada de análisis del ordenador si sigue en ejecución la misma tarea programada que se ejecutó anteriormente. La tarea de análisis programado omitida creará un registro del análisis del ordenador con 0 objetos analizados y el estado **El análisis no se inició porque el análisis anterior aún se estaba ejecutando**.

Para encontrar registros de análisis anteriores en la ventana principal del programa, seleccione **Herramientas** > **Archivos de registro**. En el menú desplegable, seleccione **Análisis del ordenador** y haga doble clic en el registro deseado.



Para obtener más información sobre los registros "no se pudo abrir", "error al abrir" o "archivo comprimido dañado", consulte el artículo de la base de conocimiento de ESET.

Haga clic en el icono del interruptor **Filtrado** para abrir la ventana Filtrado de registros, donde puede acotar la búsqueda por criterios personalizados. Para ver el menú contextual, haga clic con el botón derecho del ratón en una entrada de registro específica:

Acción	Uso
Filtrar los mismos registros	Activa el filtrado de registros. El registro solo mostrará los registros del mismo tipo que el seleccionado.
Filtro	Esta opción abre la ventana Filtrado de registros y le permite definir criterios para entradas de registro específicas. Acceso directo: `Ctrl+Shift+F`
Activar filtro	Activa los ajustes de filtro. Si activa el filtro por primera vez, debe definir ajustes y se abre la ventana Filtrado de registros.
Desactivar filtro	Desactiva el filtro (misma acción que hacer clic en el conmutador de la parte inferior).
Copiar	Copia los registros seleccionados en el portapapeles. Acceso directo: `Ctrl+C`
Copiar todo	Copia todos los registros en la ventana.
Exportar	Exporta los registros seleccionados al portapapeles en un archivo XML.
Exportar todo	Esta opción exporta todos los registros en la ventana a un archivo XML.
Descripción de la detección	Abre la Enciclopedia de amenazas de ESET, que contiene información detallada sobre los peligros y los síntomas de la infiltración resaltada.

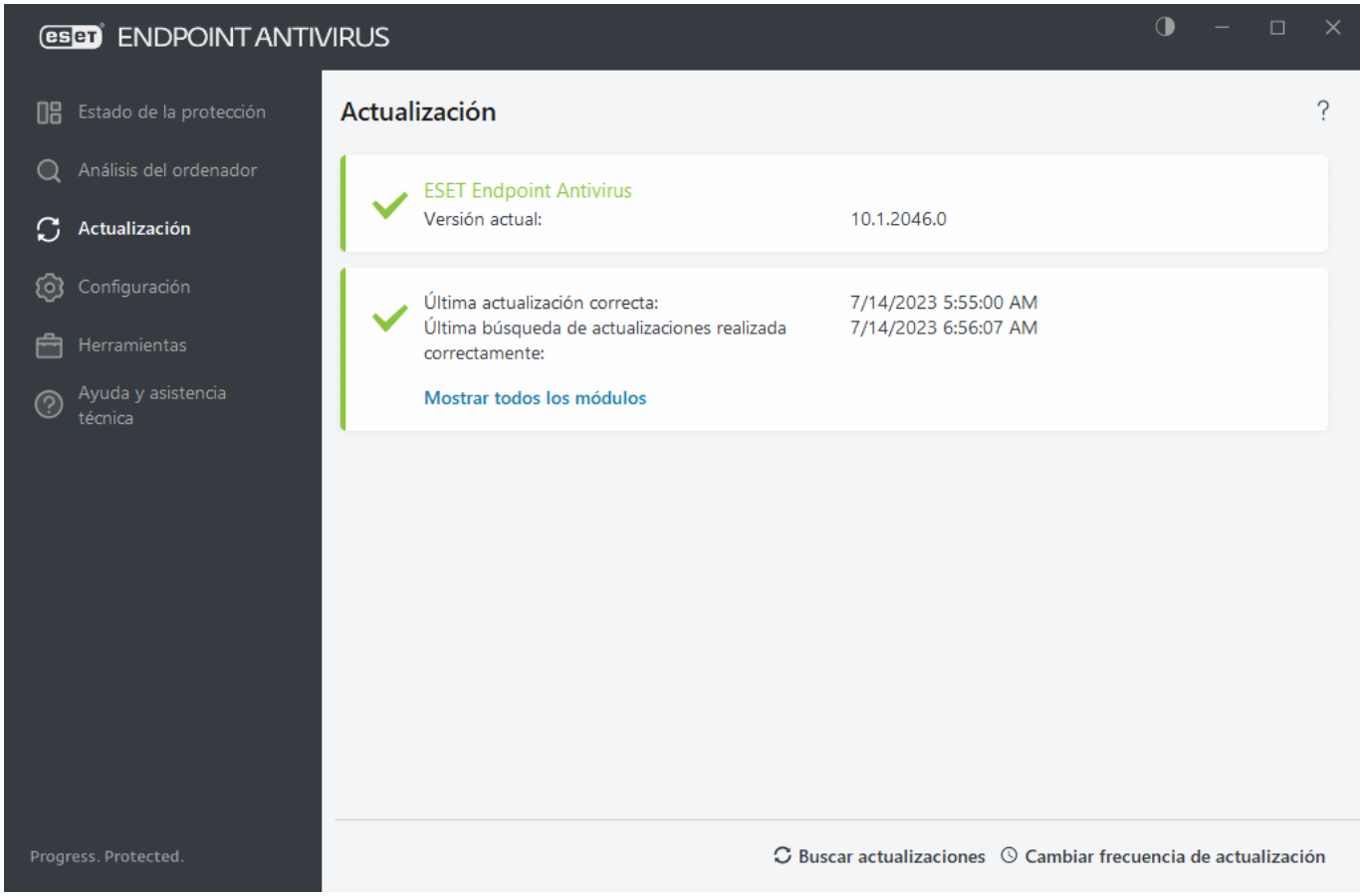
Actualización

La mejor manera de disfrutar del máximo nivel de seguridad en el ordenador es actualizar ESET Endpoint Antivirus de forma periódica. El módulo de actualización garantiza que los módulos del programa y los componentes del sistema están siempre actualizados.

Haga clic en **Actualizar** en la ventana principal del programa para consultar el estado de la actualización, la fecha y la hora de la última actualización, y si es necesario actualizar el programa.

Además de las actualizaciones automáticas, puede hacer clic en **Buscar actualizaciones** para activar una actualización manual. La actualización periódica de los módulos y los componentes del programa es un aspecto importante para mantener una protección completa contra el código malicioso. Preste atención a la configuración y el funcionamiento de los módulos del producto. Debe activar su producto con su clave de licencia para recibir actualizaciones. Si no lo hizo durante la instalación, deberá activar ESET Endpoint Antivirus para acceder a los servidores de actualización de ESET. ESET le envía la clave de licencia en un mensaje de correo electrónico tras la compra de ESET Endpoint Antivirus.

Si activa ESET Endpoint Antivirus con el archivo de licencia sin conexión sin nombre de usuario o contraseña e intenta actualizar, la información en rojo **Error de actualización de los módulos** le indica que solo puede descargar actualizaciones desde el mirror.



Versión actual: el número de compilación de ESET Endpoint Antivirus.

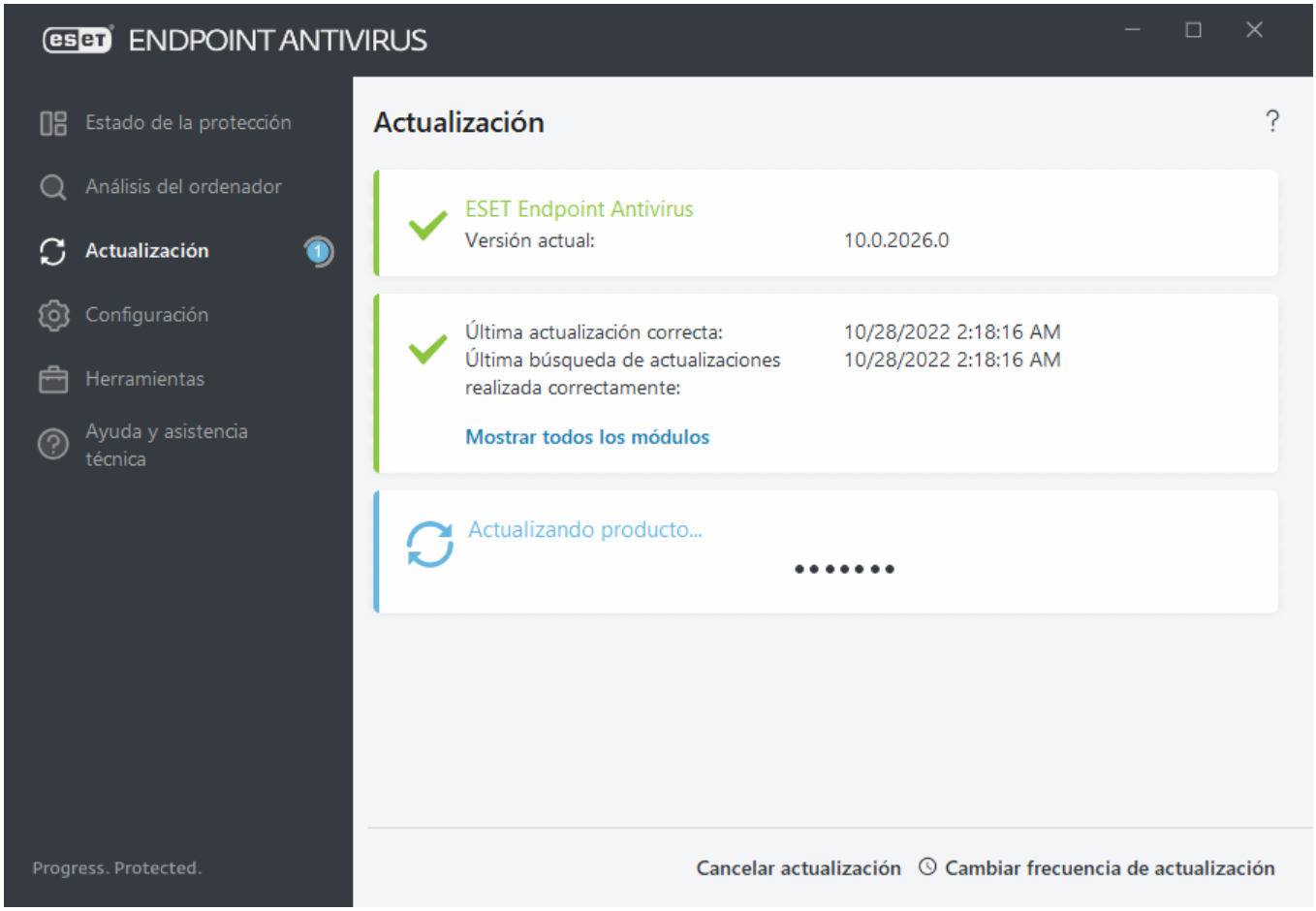
Última actualización correcta: fecha y hora de la última actualización correcta. Asegúrese de que hace referencia a una fecha reciente, lo que significa que el motor de detección está actualizado.

Última búsqueda correcta de actualizaciones: fecha y hora del último intento correcto de actualizar módulos.

Mostrar todos los módulos: haga clic en este enlace para abrir la lista de módulos instalados y comprobar tanto la versión como la última actualización de un módulo.

Proceso de actualización

El proceso comienza tras hacer clic en **Buscar actualizaciones**. Se muestran una barra de progreso de la descarga y el tiempo que falta para que finalice la descarga. Para interrumpir la actualización, haga clic en **Cancelar actualización**.



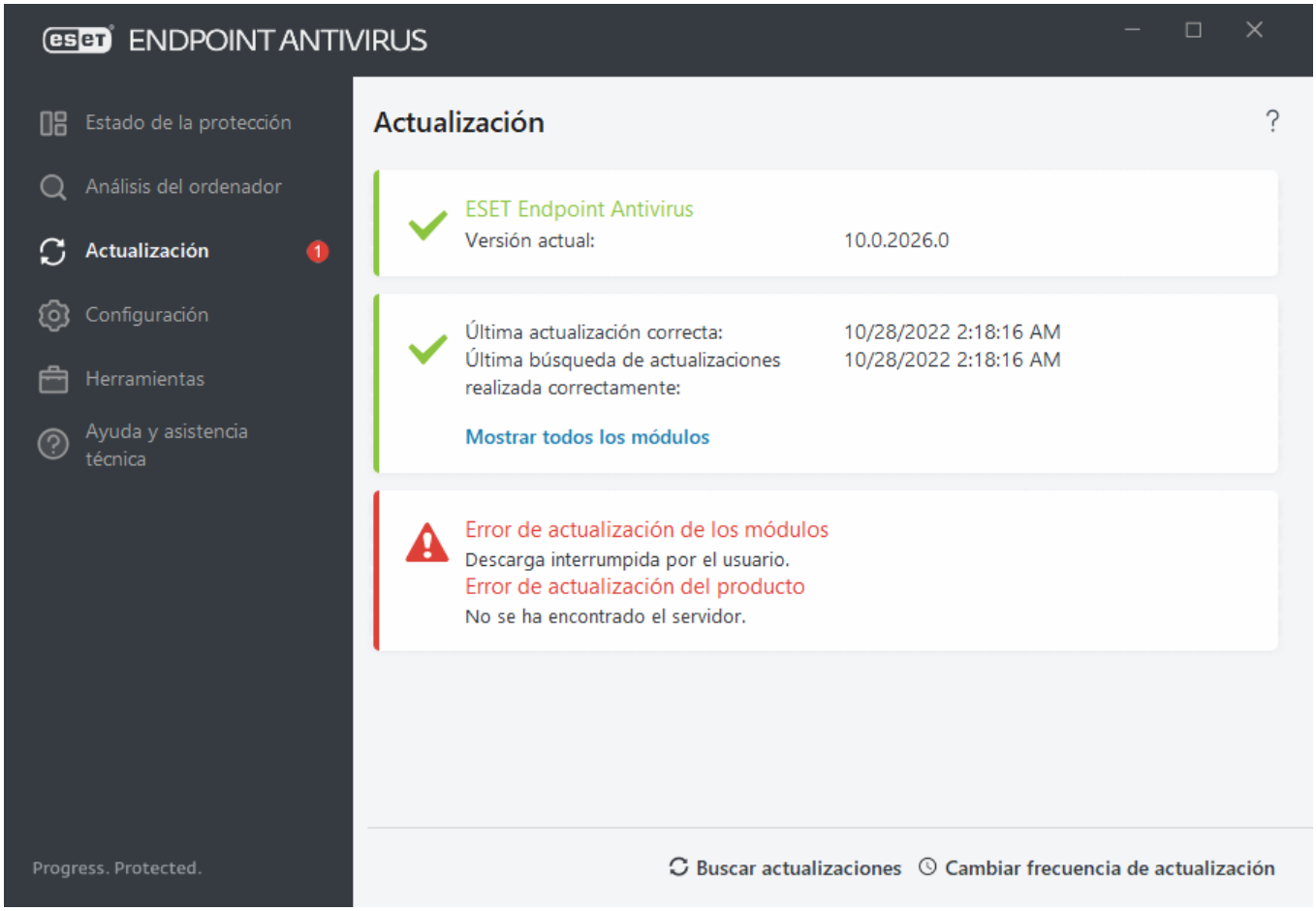
En circunstancias normales, verá la marca de verificación verde en la ventana **Actualización**, que indica que el programa está actualizado. Si no ve la marca de verificación verde, el programa no está actualizado y es más vulnerable a la infección. Actualice los módulos del programa lo antes posible.

Actualización incorrecta

El Motor de detección está obsoleto: este error aparecerá tras varios intentos sin éxito de actualizar los módulos. Le recomendamos que compruebe la configuración de actualización. La causa más frecuente de este error es la introducción incorrecta de los datos de autenticación o una mala configuración de la conexión.

La notificación anterior está relacionada con los dos mensajes **La actualización de módulos ha fallado** siguientes sobre actualizaciones incorrectas:

1. **Licencia no válida**: su licencia no está activa. Recomendamos que compruebe sus datos de autenticación. Haga clic en **Ayuda y soporte** > **Cambiar licencia** en el menú principal para introducir una nueva clave de licencia.
2. **Ha ocurrido un error mientras se descargaban los archivos de actualización**: el error puede deberse a una configuración de la conexión a Internet. Es recomendable que compruebe la conectividad a Internet (por ejemplo, abriendo un sitio web en el navegador web). Si el sitio web no se abre, es probable que no se haya establecido ninguna conexión a Internet o que haya problemas de conectividad con el ordenador. Asegúrese de que tiene una conexión a Internet activa de su Proveedor de servicios de Internet (ISP).



Para obtener más información detallada, consulte el artículo de la base de conocimiento de ESET.

Cómo crear tareas de actualización

Las actualizaciones se pueden activar manualmente al hacer clic en **Buscar actualizaciones** de la ventana principal que se muestra al hacer clic en **Actualización** en el menú principal.

Las actualizaciones también se pueden ejecutar como tareas programadas. Para configurar una tarea programada, haga clic en **Herramientas** > **Tareas programadas**. Las siguientes tareas de actualización están activadas de forma predeterminada en ESET Endpoint Antivirus:

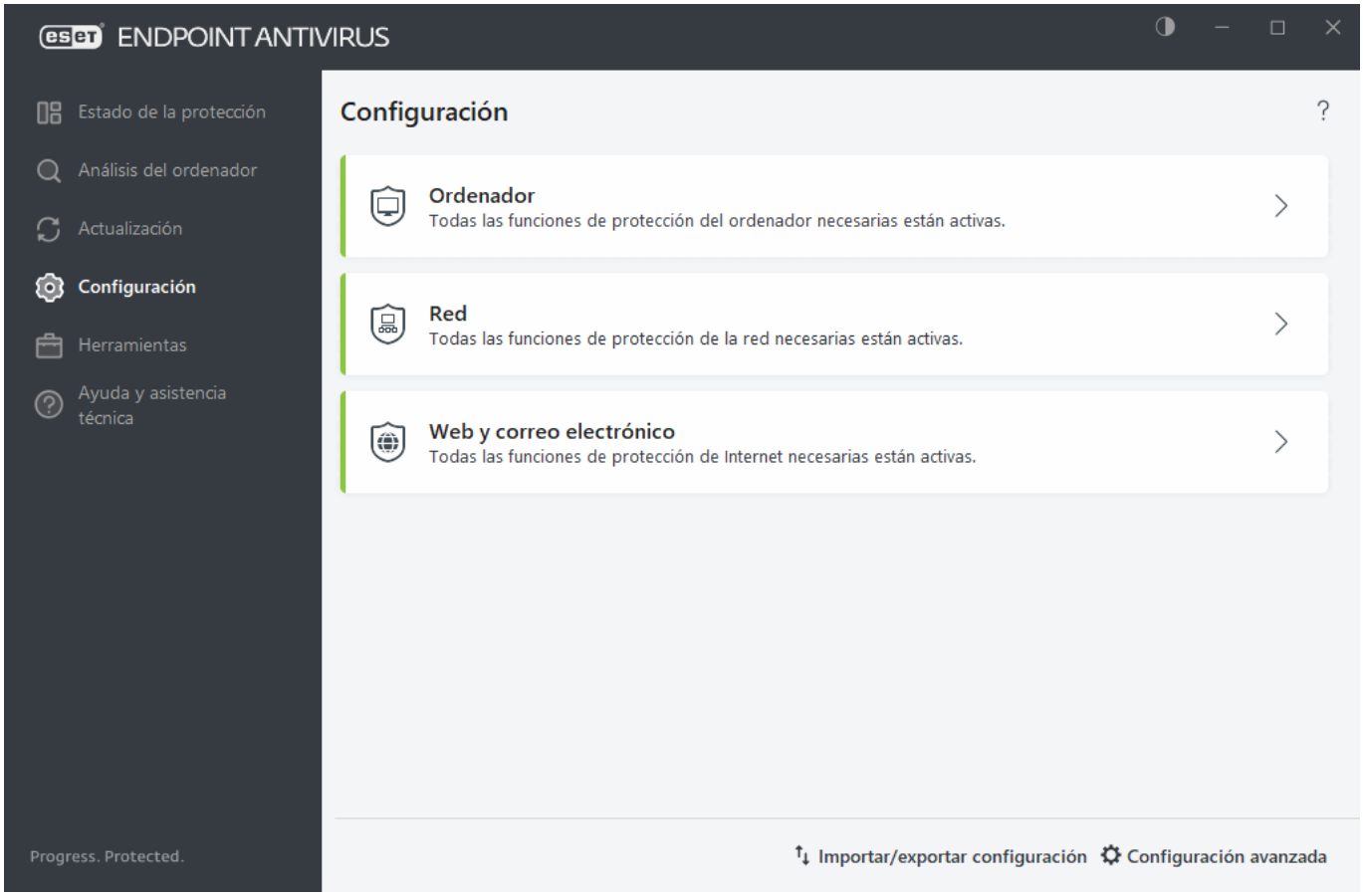
- **Actualización automática de rutina**
- **Actualización automática después del registro del usuario**

Todas las tareas de actualización se pueden modificar en función de sus necesidades. Además de las tareas de actualización predeterminadas, se pueden crear nuevas tareas de actualización con una configuración definida por el usuario. Para obtener más información acerca de la creación y la configuración de tareas de actualización, consulte la sección Planificador de tareas.

Configuración

Puede ver grupos de funciones de protección disponibles en la ventana principal del programa > **Configuración**.

Al crear una política desde ESET PROTECT Consola Web, puede seleccionar el indicador de cada ajuste. Los ajustes que tengan el indicador Forzar tendrán prioridad y no podrán sobrescribirse con una política posterior (aunque también tenga este indicador establecido). Esta práctica garantiza que el ajuste no se verá modificado (por ejemplo, por el usuario o por políticas posteriores a la hora de ejecutar la fusión). Para obtener más información, consulte la ayuda en línea de Indicadores de ESET PROTECT.



El menú **Configuración** incluye las siguientes secciones:

Ordenador

Red

Web y correo electrónico

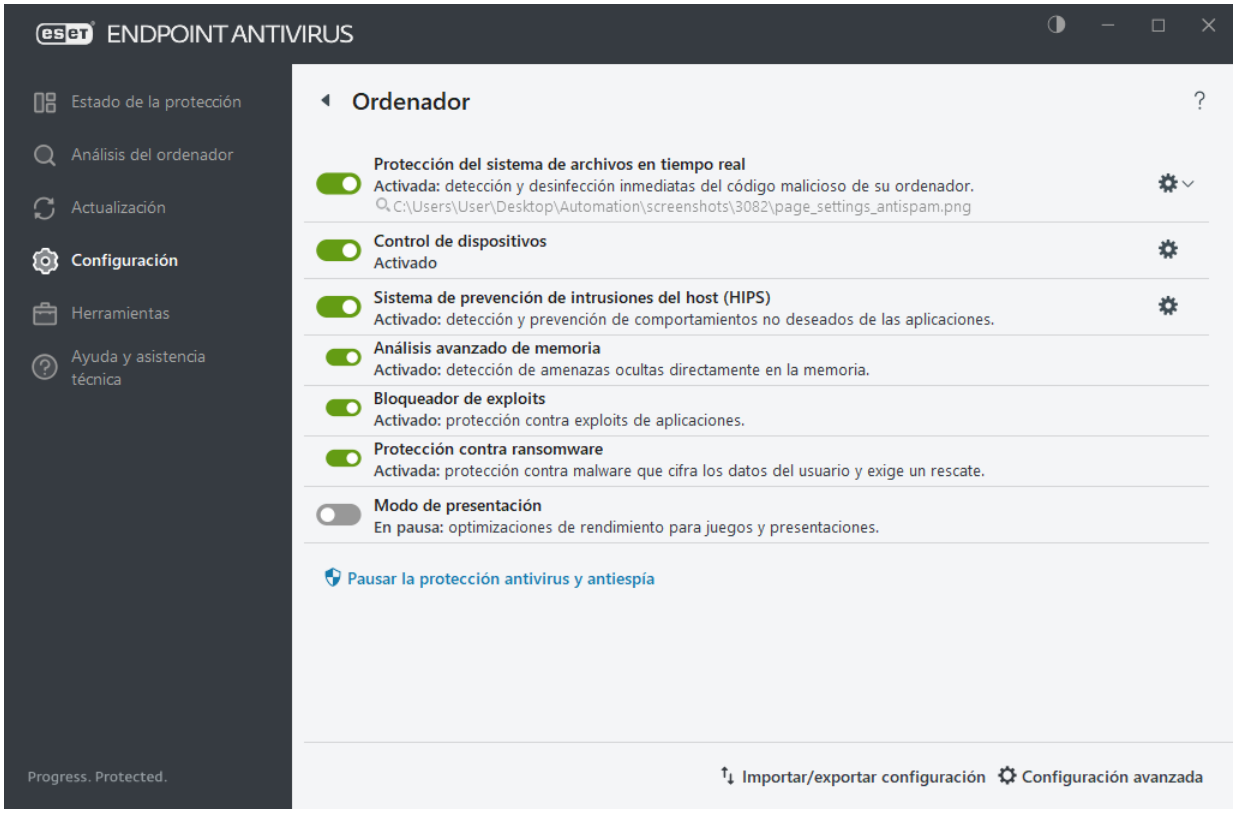
Cuando se aplique la política de ESET PROTECT, verá el icono del candado junto a un componente específico. La política aplicada por ESET PROTECT podrá sobrescribirse de forma local tras la autenticación por parte del usuario conectado (por ejemplo, el administrador). Para obtener más información, consulte la ayuda en línea de ESET PROTECT.

Todas las medidas de protección que se desactiven de esta manera se volverán activar al reiniciar el ordenador.

En la parte inferior de la ventana de configuración encontrará opciones adicionales disponibles. Haga clic en Configuración avanzada para configurar más parámetros detallados de cada módulo. Para cargar los parámetros de configuración con un archivo de configuración .xml, o para guardar los parámetros de configuración actuales en un archivo de configuración, utilice la opción Importar/exportar configuración.

Equipo

Haga clic en **Ordenador** en la ventana principal del programa > **Configuración** para ver una descripción general de todos los módulos de protección:



En la sección **Ordenador** puede activar o desactivar los siguientes componentes:

- Protección del sistema de archivos en tiempo real: todos los archivos se analizan en busca de código malicioso en el momento de abrirlos, crearlos o ejecutarlos en el ordenador. Haga clic en la icono dentada situada junto a Protección del sistema de archivos en tiempo real y haga clic en Editar exclusiones para abrir la ventana de configuración de exclusiones, donde podrá excluir del análisis archivos y carpetas. Para abrir la configuración avanzada de Protección del sistema de archivos en tiempo real, haga clic en Configurar
- Control del dispositivo: permite controlar los dispositivos (CD, DVD, USB, etc.) automáticamente. Este módulo le permite bloquear o ajustar los filtros y permisos ampliados, así como establecer los permisos de un usuario para acceder a un dispositivo dado y trabajar en él.
- Host Intrusion Prevention System (HIPS): el sistema HIPS controla los sucesos del sistema operativo y reacciona según un conjunto de reglas personalizado.
- **Análisis avanzado de memoria**: trabaja conjuntamente con el Bloqueador de exploits para aumentar la protección frente a código malicioso que utiliza los métodos de ofuscación y cifrado para evitar su detección mediante productos de protección frente a este tipo de código. El análisis avanzado de memoria está activado de forma predeterminada. Puede obtener más información sobre este tipo de protección en el glosario.
- **Bloqueo de exploits**: se ha diseñado para fortalecer los tipos de aplicaciones que sufren más ataques, como navegadores, lectores de PDF, clientes de correo electrónico y componentes de MS Office. El bloqueador de exploits está activado de forma predeterminada. Puede obtener más información sobre este tipo de protección en el glosario.
- **Protección contra ransomware** es otra capa de protección que funciona como parte de la función HIPS. Para que la protección contra ransomware funcione, debe tener activado el sistema de reputación ESET

LiveGrid®. Más información sobre este tipo de protección.

- Modo de presentación: es una función pensada para aquellos usuarios que exigen un uso del software sin interrupciones y sin notificaciones, así como un menor uso de la CPU. Cuando se active el modo de presentación, recibirá un mensaje de alerta (posible riesgo de seguridad) y la ventana principal del programa se volverá naranja.

Pausar la protección antivirus y antiespía: cuando desactive la protección antivirus y antiespía de forma temporal, utilice el menú desplegable para seleccionar el período de tiempo durante el que desea que el componente seleccionado esté desactivado y, a continuación, haga clic en **Aplicar** para desactivar el componente de seguridad. Para volver a activar la protección, haga clic en **Activar la protección antivirus y antiespía**.

Para pausar o desactivar módulos de protección específicos, haga clic en el icono .

⚠ Desactivar los módulos de protección puede disminuir el nivel de protección del ordenador.

Se detecta una amenaza

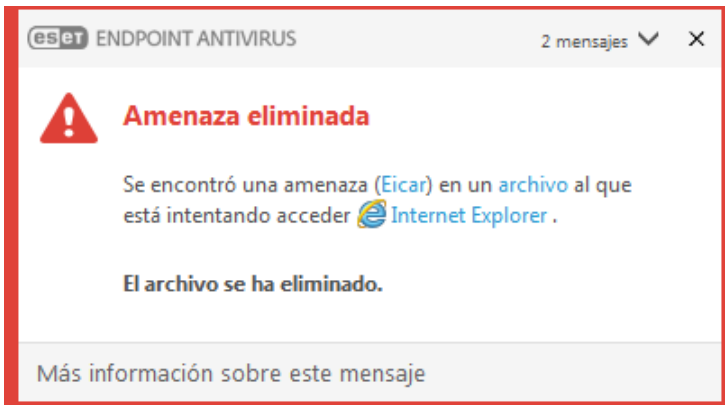
Las amenazas pueden acceder al sistema desde varios puntos de entrada, como páginas web, carpetas compartidas, correo electrónico o dispositivos extraíbles (USB, discos externos, CD, DVD, etc.).

Comportamiento estándar

Como ejemplo general de cómo ESET Endpoint Antivirus gestiona las amenazas, estas se pueden detectar mediante:

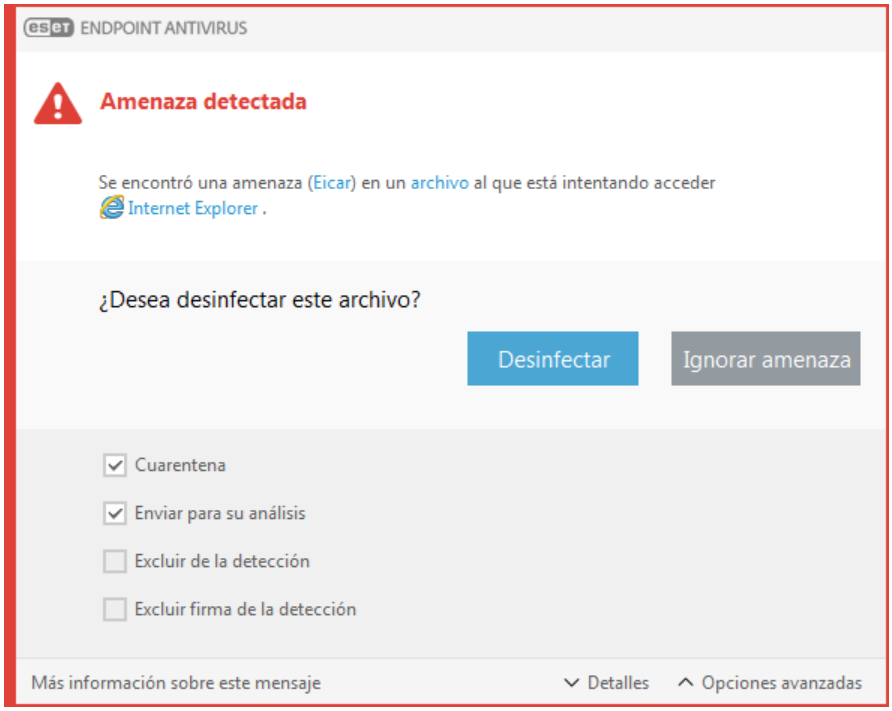
- Protección del sistema de archivos en tiempo real
- Protección del acceso a la Web
- Protección de clientes de correo electrónico
- Análisis del ordenador a petición

Cada uno de estos componentes utiliza el nivel de desinfección estándar e intentará desinfectar el archivo y moverlo a Cuarentena o finalizar la conexión. Se muestra una ventana de notificación en el área de notificación, situada en la esquina inferior derecha de la pantalla. Para obtener más información sobre los objetos detectados/desinfectados, consulte Archivos de registro. Para obtener más información sobre el comportamiento y los niveles de desinfección, consulte Desinfección.



Desinfección y eliminación

Si no hay que realizar ninguna acción predefinida para la protección en tiempo real, se le pedirá que seleccione una opción en la ventana de alerta. Normalmente, están disponibles las opciones **Desinfectar**, **Eliminar** y **Sin acciones**. No se recomienda seleccionar **Sin acciones**, ya que los archivos infectados quedarían intactos. La única excepción es cuando está seguro de que el archivo es inofensivo y se ha detectado por error.



Aplique esta opción si un archivo ha sido infectado por un virus que le ha añadido código malicioso. Si este es el caso, primero intente desinfectar el archivo infectado para restaurarlo a su estado original. Si el archivo consta exclusivamente de código malicioso, se eliminará.

Si un proceso del sistema "bloquea" o está utilizando un archivo infectado, por lo general solo se eliminará cuando se haya publicado (normalmente, tras reiniciar el sistema).

Restauración de archivos de cuarentena

La cuarentena está disponible en la ventana principal de ESET Endpoint Antivirus; para acceder, haga clic en **Herramientas** > **Cuarentena**.

Los archivos en cuarentena también pueden restaurarse en su ubicación original:

- Utilice la función **Restaurar** para tal fin, disponible desde el menú contextual si hace clic con el botón derecho en un archivo determinado en cuarentena.
- Si un archivo se marca como aplicación potencialmente indeseable, la opción **Restaurar y excluir del análisis** se activa. Consulte también Exclusiones.
- El menú contextual también ofrece la opción **Restaurar a**, que le permite restaurar archivos en una ubicación distinta de la cual se eliminaron.
- La función de restauración no está disponible en algunos casos, por ejemplo, para los archivos que se encuentran en un recurso compartido de red de solo lectura.

Múltiples amenazas

Si durante un análisis del ordenador no se desinfectaron algunos archivos infectados (o el Nivel de desinfección se estableció en **Sin desinfección**), aparecerá una ventana de alerta solicitándole que seleccione la acción que desea llevar a cabo en esos archivos.

Eliminación de amenazas en archivos comprimidos

En el modo de desinfección predeterminado, solo se eliminará todo el archivo comprimido si todos los archivos que contiene están infectados. En otras palabras, los archivos comprimidos no se eliminan si también contienen archivos no infectados e inofensivos. Tenga cuidado cuando realice un análisis con desinfección exhaustiva activada, ya que un archivo comprimido se eliminará si contiene al menos un archivo infectado, sin tener en cuenta el estado de los otros archivos.

Si el ordenador muestra señales de infección por código malicioso — por ejemplo, se ralentiza, se bloquea con frecuencia, etc., le recomendamos que haga lo siguiente:

- Abra ESET Endpoint Antivirus y haga clic en Análisis del ordenador.
- Haga clic en **Análisis estándar** (para obtener más información, consulte Análisis del ordenador).
- Una vez que haya finalizado el análisis, revise el registro para consultar el número de archivos analizados, infectados y desinfectados.

Si solo desea analizar una parte específica del disco, haga clic en **Análisis personalizado** y seleccione los objetos que desea incluir en el análisis de virus.

Red

Abra la ventana principal del programa **Configuración** > **Red** > para configurar las opciones básicas de protección de red o solucionar problemas de comunicación de red.

Para pausar o desactivar módulos de protección específicos, haga clic en el icono  .

Desactivar los módulos de protección puede disminuir el nivel de protección del ordenador.

Haga clic en el icono del engranaje ubicado junto a un módulo de protección para acceder a la configuración avanzada.

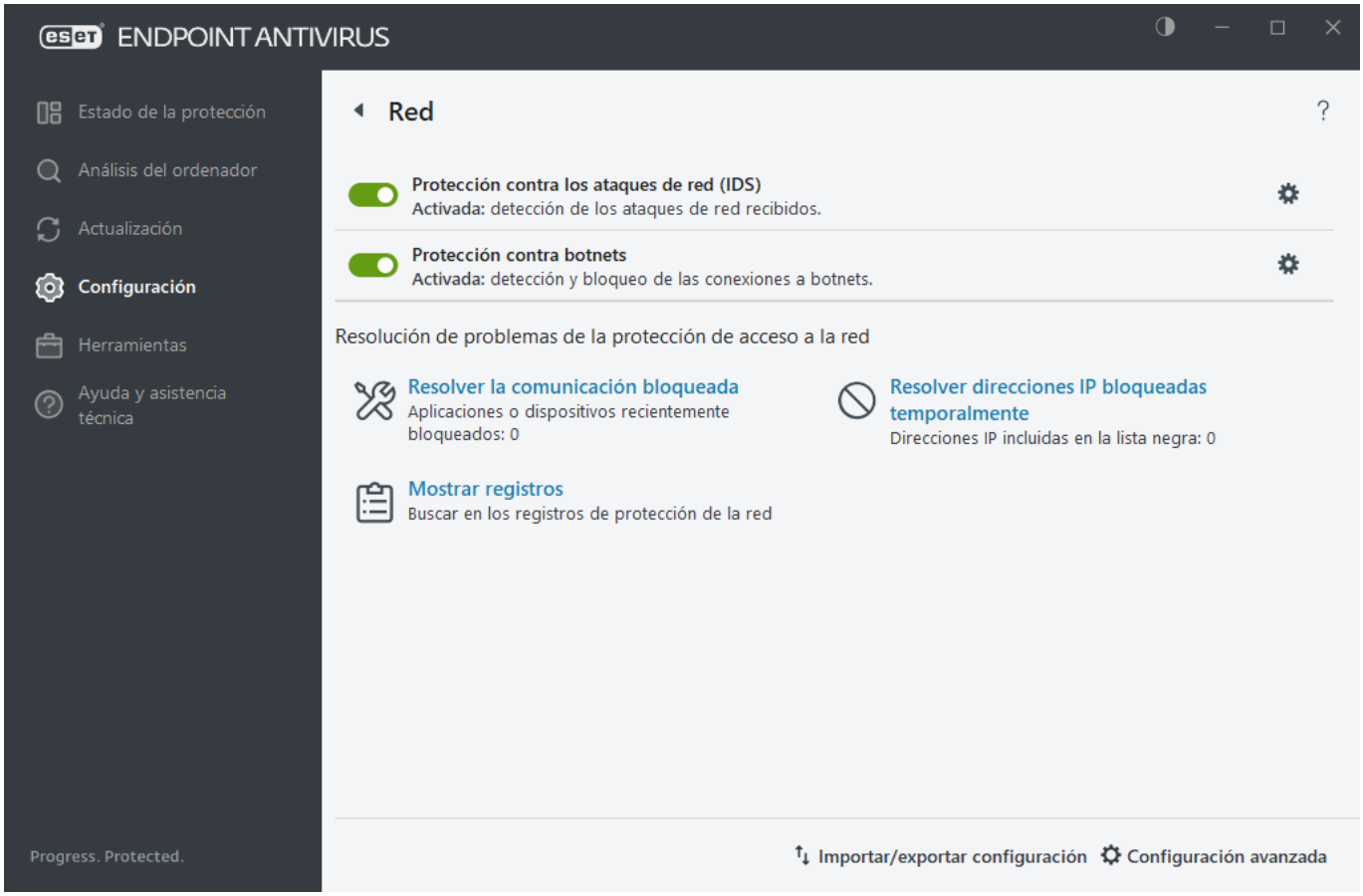
Protección contra los ataques de red (IDS): analiza el contenido del tráfico de red y protege frente a ataques de red. Se bloquea todo aquel tráfico que se considera perjudicial. ESET Endpoint Antivirus le avisa cuando se conecta a una red inalámbrica no protegida o a una red con un nivel de protección débil.

Protección contra botnets: identifica malware en el sistema de forma rápida y precisa.

Resolver la comunicación bloqueada: le ayuda a solucionar los problemas de conectividad provocados por el cortafuegos de ESET. Para obtener información más detallada, consulte el Asistente de solución de problemas.

Resolver direcciones IP bloqueadas temporalmente: ver una lista de direcciones IP que se han detectado como fuente de los ataques y se han agregado a la lista negra para bloquear la conexión durante un período de tiempo concreto.

Mostrar registros: abre el archivo de registro de protección de red.



Resolución de problemas de acceso a la red

El asistente de solución de problemas le ayuda a solucionar los problemas de conectividad provocados por el cortafuegos. **Resolución de problemas de acceso a la red** está disponible en la ventana principal del programa > **Configuración** > **Red** > **Resolver la comunicación bloqueada**.

Seleccione si desea mostrar la comunicación bloqueada para **Aplicaciones locales** o la comunicación bloqueada desde **Dispositivos remotos**.

En el menú desplegable, seleccione un período de tiempo durante el que se haya bloqueado la comunicación. Una lista de comunicaciones bloqueadas recientemente ofrece una descripción general sobre el tipo de aplicación o dispositivo, la reputación y el número total de aplicaciones y dispositivos bloqueados durante ese período de tiempo. Para obtener más información sobre la comunicación bloqueada, haga clic en **Detalles**. El siguiente paso es desbloquear la aplicación o dispositivo en el que experimente problemas de conectividad.

Tras hacer clic en **Desbloquear**, se permitirá la comunicación bloqueada anteriormente. Si sigue experimentando problemas con una aplicación o el dispositivo no funciona según lo esperado, haga clic en **crear otra regla** para permitir todas las comunicaciones bloqueadas anteriormente para ese dispositivo. Reinicie el ordenador si el problema persiste.

Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:
- Agregar una excepción con el asistente de solución de problemas

Si no se puede crear la regla, recibirá un mensaje de error. Haga clic en **Volver a intentarlo** y repita el proceso para desbloquear la comunicación o cree otra regla desde la lista de comunicaciones bloqueadas.

Lista negra de direcciones IP temporales

Para ver las direcciones IP detectadas como fuentes de ataques y agregadas a la lista negra para bloquear la conexión durante un periodo de tiempo concreto, abra la ventana principal del programa > **Configuración** > **Protección de la red** > **Lista negra temporal de direcciones IP**. Las direcciones IP bloqueadas temporalmente se bloquean durante 1 hora.

Columnas

Dirección IP: muestra una dirección IP que se ha bloqueado.

Motivo del bloqueo: muestra el tipo de ataque que se ha evitado desde la dirección (por ejemplo, ataque de exploración de puerto TCP).

Tiempo de espera: muestra la fecha y la hora a la que la dirección se eliminará de la lista negra.

Elementos de control

Quitar: haga clic en esta opción para eliminar una dirección de la lista negra antes de que expire.

Quitar todo: haga clic en esta opción para eliminar todas las direcciones de la lista negra de inmediato.

Agregar excepción: haga clic en esta opción para agregar una excepción del cortafuegos en el filtrado de IDS.

Registros de protección de la red

La protección de la red de ESET Endpoint Antivirus guarda todos los sucesos importantes en un archivo de registro. Para ver el archivo de registro, abra la ventana principal del programa > **Configuración** > **Red** > **Mostrar registros**.

Los archivos de registro sirven para la detección de errores e intrusiones en el sistema. Los registros de protección de la red contienen los datos siguientes:

- Fecha y hora del suceso.
- Nombre del suceso
- Fuente
- Dirección de la red de destino
- Protocolo de comunicación de red
- Regla aplicada o nombre del gusano (si se identifica)
- Ruta de acceso y nombre de la aplicación
- Hash
- Usuario
- Firmante de la aplicación (editor)
- Nombre del paquete
- Nombre del servicio

Un análisis exhaustivo de estos datos puede ayudarle a detectar los intentos de poner en peligro la seguridad del

sistema. Existen otros muchos factores que indican posibles riesgos de seguridad y le permiten minimizar el impacto: conexiones frecuentes desde ubicaciones desconocidas, intentos repetidos de establecer conexiones, comunicación de aplicaciones desconocidas o utilización de números de puertos poco comunes.

> **Explotación de vulnerabilidades de seguridad**
> El mensaje de explotación de vulnerabilidades de seguridad se registra incluso si la vulnerabilidad concreta se ha revisado desde que se ha detectado y bloqueado el intento de explotación en el nivel de red antes de que se produzca la explotación propiamente dicha.

Solución de problemas con la protección de la red de ESET

Si tiene problemas de conectividad cuando ESET Endpoint Antivirus está instalado, tiene a su disposición varias maneras de comprobar si el Protección de la red de ESET es la causa del problema. Además, el Protección de la red de ESET puede ayudarle a crear reglas o excepciones nuevas para solucionar los problemas de conectividad.

Consulte los temas siguientes para obtener ayuda a la hora de solucionar problemas con el Protección de la red de ESET:

- Resolución de problemas de acceso a la red
- Registro y creación de reglas o excepciones del registro
- Registro avanzado de la protección de la red
- Resolución de problemas con el análisis de tráfico de red

Registro y creación de reglas o excepciones del registro

De forma predeterminada, el cortafuegos de ESET no registra todas las conexiones bloqueadas. Si desea ver qué estaba bloqueado por la protección de la red, abra Configuración avanzada > **Herramientas** > **Diagnóstico** > **Registro avanzado** y active **Activar registro avanzado de la protección de red**. Si ve en el registro algo que no desea que el cortafuegos bloquee, puede crear una regla o una regla de IDS haciendo clic con el botón derecho del ratón en dicho elemento y seleccionando **No bloquear sucesos similares en el futuro**. Tenga en cuenta que el registro de todas las conexiones bloqueadas puede contener miles de elementos, por lo que puede resultar complicado encontrar una conexión específica en este registro. Una vez que haya resuelto el problema, puede desactivar el registro.

Para obtener más información sobre el registro, consulte Archivos de registro.

> Utilice el registro para ver el orden en que el Protección de la red bloqueó las conexiones. Además, la creación de reglas a partir del registro le permite crear reglas que hagan exactamente lo que usted desee.

Crear una regla desde un registro

La nueva versión de ESET Endpoint Antivirus le permite crear una regla desde el registro. En el menú principal, haga clic en **Herramientas** > **Archivos de registro**. Seleccione **Protección de la red** en el menú desplegable, haga clic con el botón derecho en la entrada del registro que desee y seleccione **No bloquear sucesos similares en el futuro** en el menú contextual. Se abrirá una ventana de notificación con la nueva regla.

Si desea permitir la creación de reglas nuevas a partir del registro, configure ESET Endpoint Antivirus con los ajustes siguientes:

1. Defina el nivel mínimo de detalle al registrar en **Diagnóstico**, en Configuración avanzada > **Herramientas** > **Archivos de registro**.
2. Active **Notificar ataques entrantes contra vulnerabilidades de seguridad** en Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Protección contra los ataques de red (IDS)** > **Opciones avanzadas** > **Detección de intrusiones**.

Registro avanzado de la protección de la red

El objetivo de esta característica es proporcionar archivos de registro más complejos para el servicio de soporte técnico de ESET. Solo se debe utilizar cuando lo solicite el servicio de soporte técnico de ESET, ya que puede generar un archivo de registro muy grande y ralentizar su ordenador.

1. Abrir Configuración avanzada > **Herramientas** > **Diagnóstico** y active **Activar registro avanzado de la protección de red**.
2. Intente repetir los pasos que provocaron el problema.
3. Desactive el registro avanzado de la protección de la red.
4. El archivo de registro PCAP creado por el registro avanzado de protección de la red está en el mismo directorio en el que se generan los volcados de memoria de diagnóstico: *C:\ProgramData\ESET\ESET Security\Diagnostics*

Resolución de problemas con el análisis de tráfico de red

Si tiene problemas con el navegador o cliente de correo electrónico, lo primero que debe hacer es comprobar si la causa es el análisis del tráfico de red. Para ello, desactive de forma temporal el análisis de tráfico de red en Configuración avanzada > **Motor de detección** > **Análisis del tráfico de red** (no olvide volver a activarlo cuando haya terminado, de lo contrario el navegador y el cliente de correo electrónico no estarán protegidos). Si el problema desaparece al desactivar el filtrado, consulte esta lista de problemas habituales y soluciones:

Problemas de comunicación segura o actualización

Si su aplicación se queja porque no se puede actualizar o el canal de comunicación no es seguro:

- Si tiene activado SSL/TLS, desactívelo temporalmente. Si esto soluciona el problema, siga utilizando SSL/TLS y realice el trabajo de actualización excluyendo la comunicación problemática:
  Desactivar SSL/TLS. Vuelva a ejecutar la actualización. Debería aparecer un cuadro de diálogo para informarle sobre el tráfico de red cifrado. Asegúrese de que la aplicación coincide con la que tiene el problema y que el certificado procede del servidor desde el que se está actualizando. A continuación, seleccione la opción Recordar acción para este certificado y haga clic en Omitir. Si no se muestra ningún otro cuadro de diálogo, puede volver a poner el modo de filtrado en automático. El problema debería estar resuelto.

- Si la aplicación en cuestión no es un navegador o un cliente de correo electrónico, puede excluirla totalmente de la Protección de acceso a la web (si hace esto con un navegador o cliente de correo electrónico, quedaría muy expuesto). Todas las aplicaciones cuya comunicación se haya filtrado

previamente deberían aparecer en la lista que se le proporcionó al agregar una excepción, por lo que no tendría que añadirlas de forma manual.

Problemas de acceso a un dispositivo de la red

Si no puede utilizar alguna funcionalidad del dispositivo en la red (como abrir un página web de la cámara web o reproducir vídeo en un reproductor multimedia), agregue sus direcciones IPv4 y IPv6 a la lista de direcciones excluidas.

Problemas con un sitio web determinado

Puede excluir sitios web específicos de la Protección de acceso a la web mediante la gestión de direcciones URL. Por ejemplo, si no puede acceder a https://www.gmail.com/intl/en/mail/help/about.html, inténtelo agregando *gmail.com* a la lista de direcciones excluidas.

Error "Algunas de las aplicaciones capaces de importar el certificado raíz aun están en funcionamiento"

Cuando se activa SSL/TLS, ESET Endpoint Antivirus se asegura de que las aplicaciones instaladas confíen en su método de filtrado del protocolo SSL importando un certificado a su almacén de certificados. Algunas aplicaciones pueden requerir un reinicio para importar un certificado. Asegúrese de que no se está ejecutando ninguna de ellas (la mejor manera de hacerlo es abrir el Administrador de tareas y comprobar que no haya ninguna entrada firefox.exe ni opera.exe en la ficha Procesos). Verifique que ninguno de ellos se esté ejecutando (la mejor manera de hacerlo es abrir el Administrador de tareas y asegurarse de que no estén firefox.exe ni opera.exe en la pestaña Procesos), luego pulse Reintentar.

Error de emisor no fiable o firma no válida

Lo más probable es que este error haga referencia al fallo de importación descrito anteriormente. Primero, asegúrese de que no se está ejecutando ninguna de las aplicaciones mencionadas. A continuación, desactive SSL/TLS y vuelva a activarlo. El proceso de importación se volverá a ejecutar.

Amenaza de red bloqueada

Esta situación puede darse cuando alguna de las aplicaciones del ordenador está intentando transmitir tráfico malicioso a otro dispositivo de la red, aprovechando una vulnerabilidad de seguridad, o incluso si se detecta un intento de análisis de puertos en su sistema.

En la notificación puede ver el tipo de amenaza y la dirección IP del dispositivo relacionado. Haga clic en **Cambiar la gestión de esta amenaza** para mostrar las siguientes opciones:

Seguir bloqueando: bloquea la amenaza detectada. Si desea dejar de recibir notificaciones de este tipo de amenaza desde la dirección remota concreta, marque el botón de opción situado junto a **No notificar** antes de hacer clic en **Seguir bloqueando**. De esta forma se creará una regla del Servicio de detección de intrusiones (IDS) con la siguiente configuración: **Bloquear**: predeterminado; **Notificar**: no; **Registrar**: no.

Permitir: crea una regla del Servicio de detección de intrusiones (IDS) para permitir la amenaza detectada. Seleccione una de las siguientes opciones antes de hacer clic en **Permitir** para especificar la configuración de la regla:

- **Avisar solo cuando se bloquee esta amenaza**—Configuración de la regla: **Bloquear**: no; **Notificar**: no; **Registrar**: no.
- **Avisar siempre que se produzca esta amenaza**—Configuración de la regla: **Bloquear**: no; **Notificar**: predeterminado; **Registrar**: predeterminado.
- **No avisar**—Configuración de la regla: **Bloquear**: no; **Notificar**: no; **Registrar**: no.

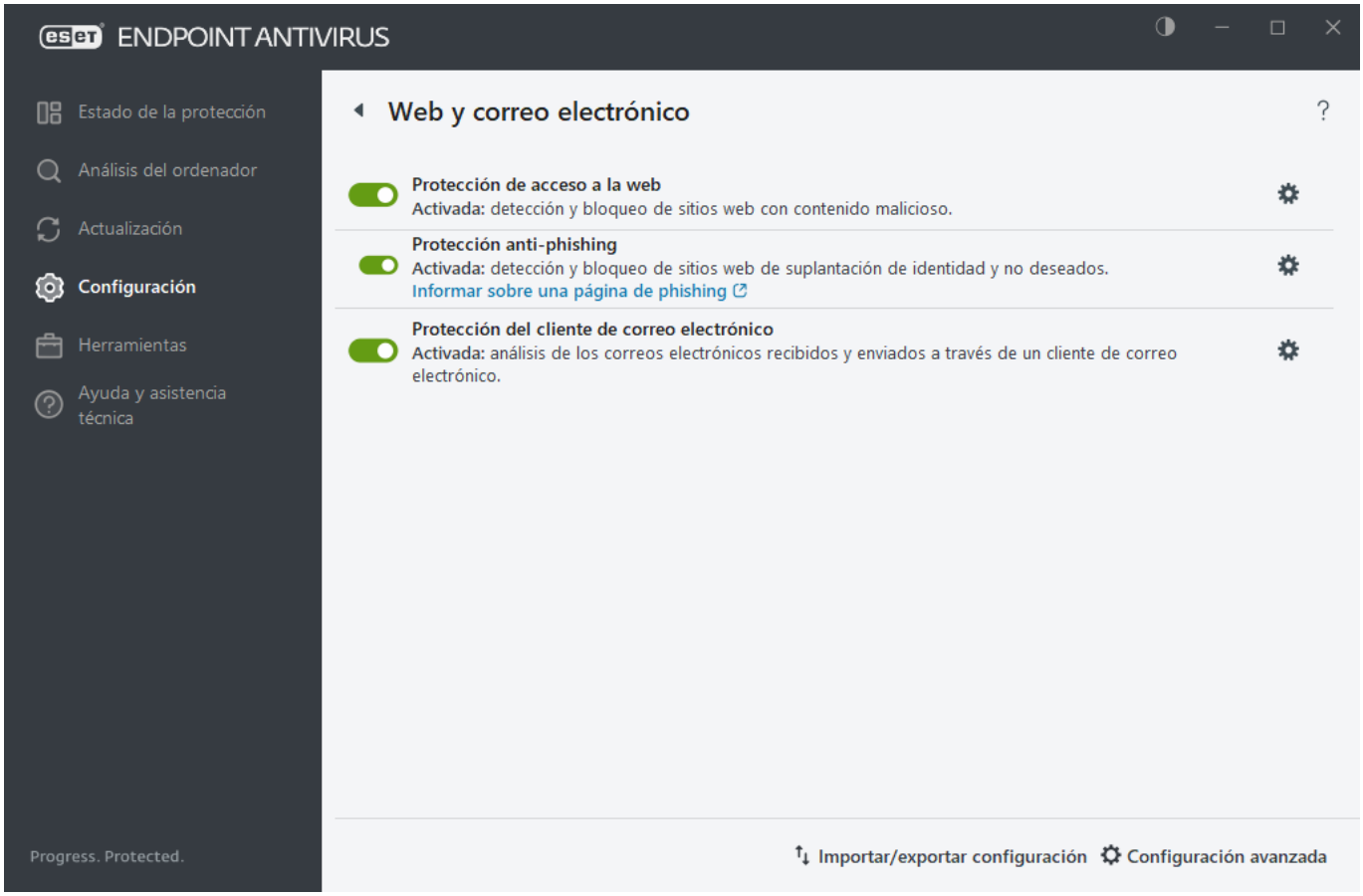
La información que se muestra en esta ventana de notificación puede variar en función del tipo de amenaza detectado.
Si desea obtener más información sobre amenazas y otros términos relacionados, consulte Tipos de ataques remotos o Tipos de amenazas detectadas.
Para resolver los sucesos de **redes con direcciones IP duplicadas**, consulte el artículo de la base de conocimiento de ESET.

Web y correo electrónico

La conectividad a Internet es una función esencial en un ordenador personal, pero también el medio principal para transferir código malicioso. Abra la ventana principal del programa > **Configuración** > **Web y correo electrónico** para configurar las funciones de ESET Endpoint Antivirus que aumentan la protección de Internet.

Para pausar o desactivar módulos de protección específicos, haga clic en el icono .

Desactivar los módulos de protección puede disminuir el nivel de protección del ordenador.



Haga clic en el icono del engranaje ubicado junto a un módulo de protección para acceder a la configuración avanzada de ese módulo.

La protección de acceso a la web analiza la comunicación HTTP/HTTPS en busca de malware y phishing. Protección de acceso a la web solo debe desactivarse para solucionar problemas.

Protección antiphishing le permite bloquear páginas web conocidas por distribuir contenido de phishing. Le recomendamos encarecidamente que deje Anti-Phishing activado.

Informar sobre una página de phishing: envía un informe sobre un sitio web malicioso o de phishing a ESET para su análisis.

> Antes de enviar un sitio web a ESET, asegúrese de que cumple uno o más de los siguientes criterios:
> • El sitio web no se detecta en absoluto.
> • El sitio web se detecta como una amenaza, pero no lo es. En este caso, puede Informar de página bloqueada incorrectamente.

La opción Protección del cliente de correo electrónico proporciona control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3(S) e IMAP(S). Con el programa de complemento para su cliente de correo electrónico, ESET Endpoint Antivirus ofrece control de todas las comunicaciones realizadas desde el cliente de correo electrónico.

Protección Anti-Phishing

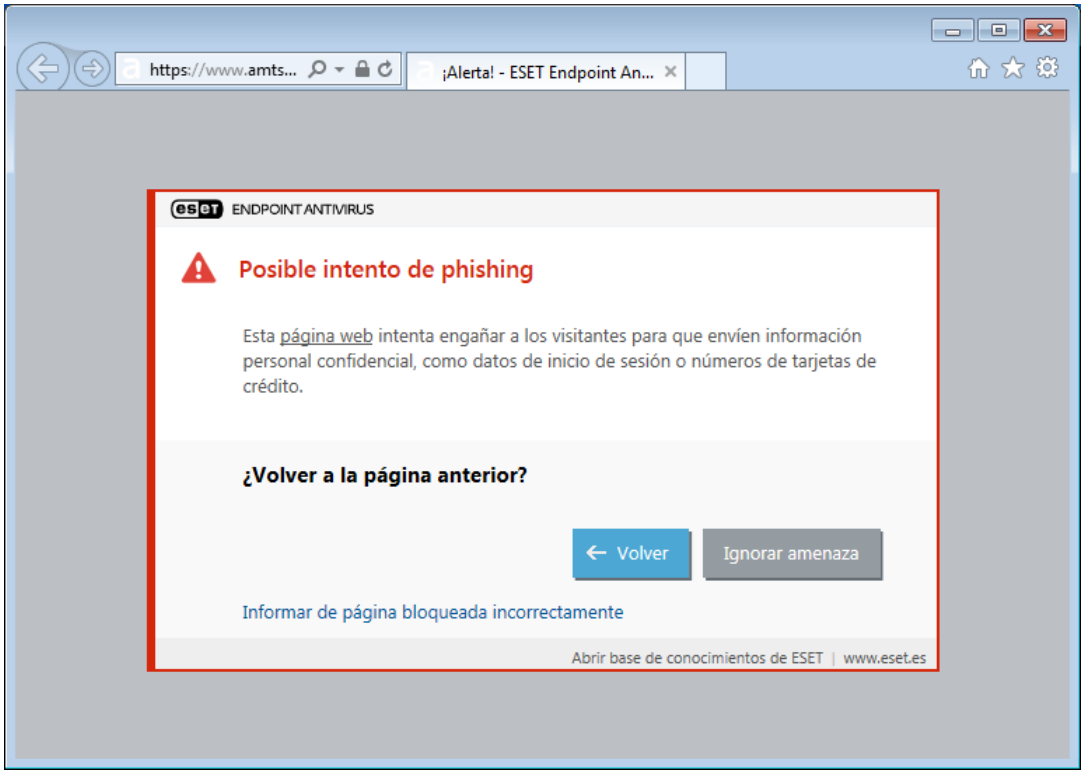
El phishing es una actividad delictiva en la que se aplica ingeniería social, es decir, se manipula al usuario para obtener información confidencial. El phishing se utiliza para acceder a datos confidenciales, como números de cuentas bancarias, PIN, etc. Para obtener más información, consulte el glosario. ESET Endpoint Antivirus incluye protección anti-phishing, que bloquea las páginas web conocidas por distribuir este tipo de contenido.

La protección antiphishing está activada de forma predeterminada. Esta opción se puede configurar en Configuración avanzada > **Protecciones** > **Protección de acceso web**.

Visite nuestro artículo de la base de conocimiento para obtener más información sobre la protección Anti-Phishing de ESET Endpoint Antivirus.

Acceso a un sitio web de phishing

Al acceder a un sitio web de phishing reconocido, su navegador web mostrará el siguiente cuadro de diálogo. Si aun así quiere acceder al sitio web, haga clic en **Ignorar amenaza** (no recomendado).



Los posibles sitios de phishing que se han incluido en la lista blanca expirarán de forma predeterminada después de unas horas. Para permitir un sitio web permanentemente, use la herramienta Gestión de direcciones URL. En Configuración avanzada > **Protecciones** > **Protección de acceso a la web** > **Gestión de direcciones URL** > **Lista de direcciones** > **Modificar** agregue a la lista el sitio web que desee modificar.

Informar sobre una página de phishing

El vínculo **Informar de una página bloqueada incorrectamente** le permite informar de un sitio web que se detecta incorrectamente como una amenaza.

También puede enviar el sitio web por correo electrónico. Envíe su correo electrónico a samples@eset.com. Utilice un asunto descriptivo y adjunte toda la información posible sobre el sitio web (por ejemplo, el sitio web que le refirió a este, cómo tuvo constancia de su existencia, etc.).

Importar y exportar configuración

Puede importar o exportar el archivo de configuración .xml de ESET Endpoint Antivirus del menú **Configuración**.

Instrucciones con ilustraciones

Consulte Importar o exportar los ajustes de configuración de ESET con un archivo .xml para obtener instrucciones con ilustraciones disponibles en inglés y en otros idiomas.

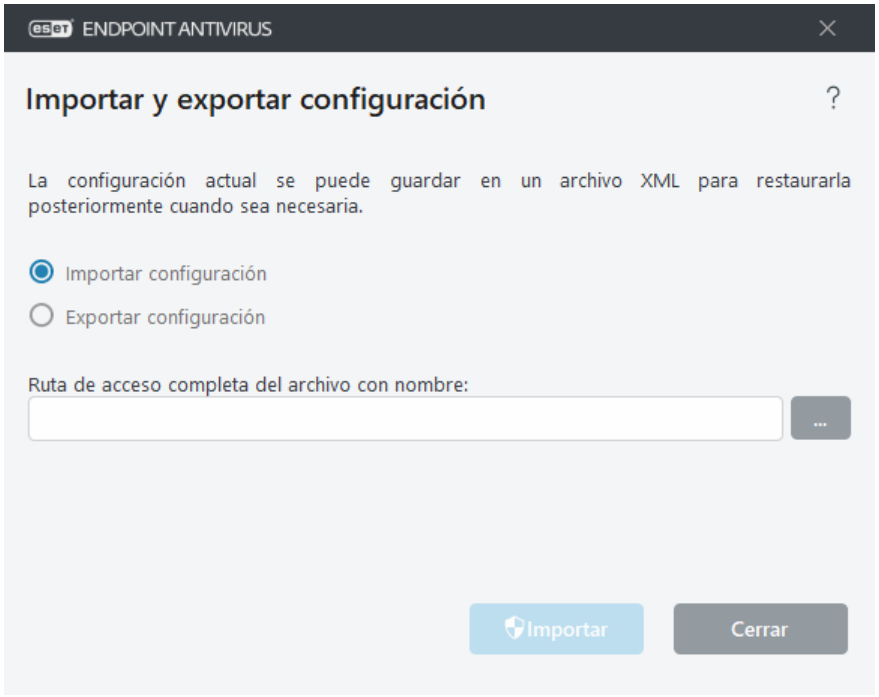
La importación y la exportación de archivos de configuración son útiles cuando necesita realizar una copia de seguridad de la configuración actual de ESET Endpoint Antivirus para utilizarla en otro momento. La opción de configuración de exportación también es conveniente cuando desea utilizar su configuración preferida en varios sistemas. Ya que le permite importar un archivo .xml para transferir estos ajustes.

Para importar la configuración, en la ventana principal del programa, haga clic en **Configuración** > **Importar/exportar configuración** y seleccione **Importar configuración**. Escriba el nombre del archivo de

configuración o haga clic en el botón **...** para buscar el archivo de configuración que desea importar.

Para exportar la configuración, en la ventana principal del programa, haga clic en **Configuración** > **Importar/exportar configuración**. Seleccione **Exportar configuración** y escriba la ruta de acceso completa del archivo con el nombre. Haga clic en **...** para desplazarse a un lugar del ordenador en el que guardar el archivo de configuración.

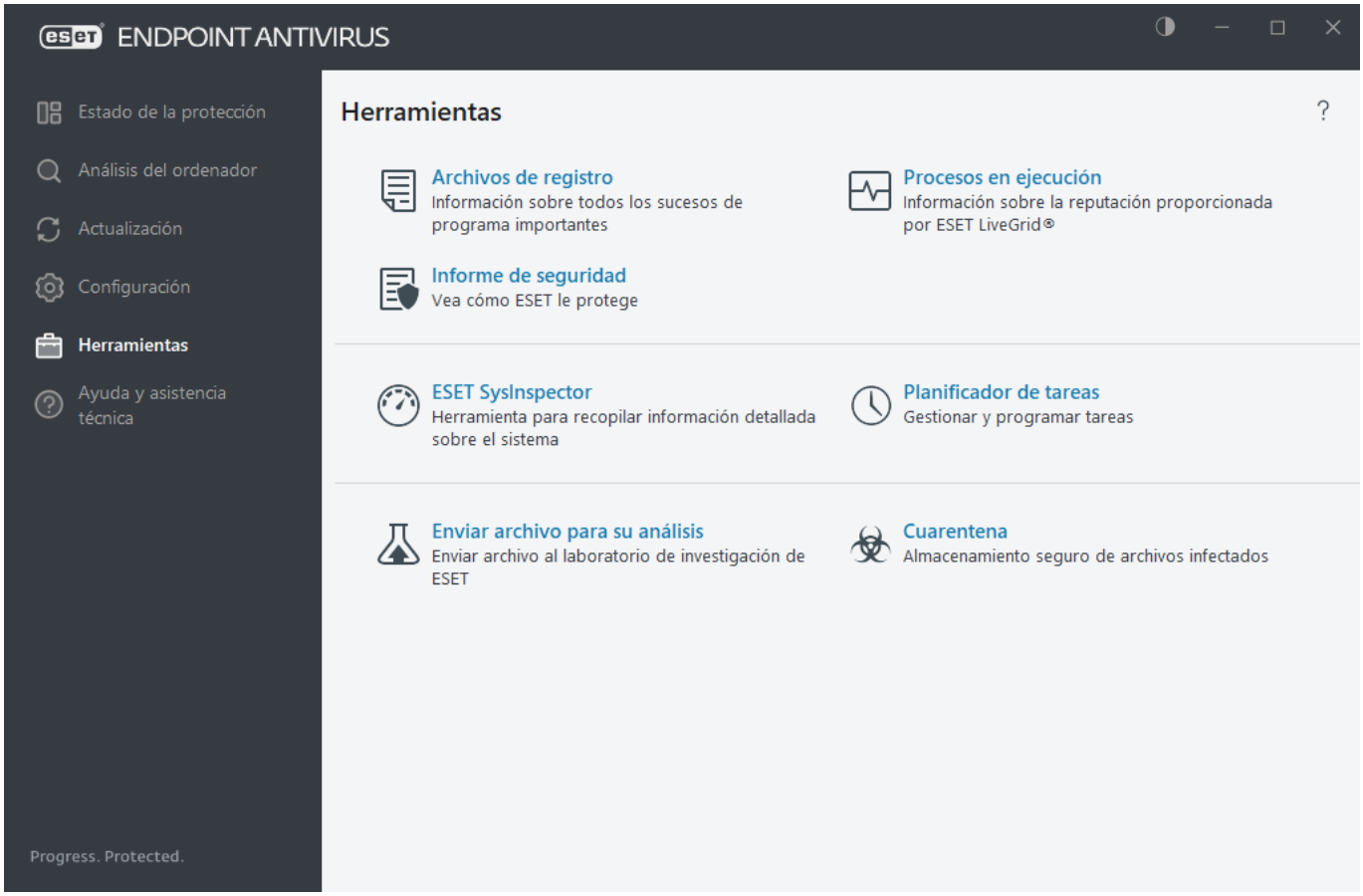
> Puede encontrarse con un error al exportar la configuración si no dispone de derechos suficientes para escribir el archivo exportado en el directorio especificado.



Herramientas

El menú **Herramientas** incluye módulos que ayudan a simplificar la administración del programa y ofrece opciones adicionales para usuarios avanzados.

- Archivos de registro
- Procesos en ejecución (si ESET LiveGrid® se ha activado en ESET Endpoint Antivirus)
- Informe de seguridad (para equipos no administrados)
- ESET SysInspector
- Tareas programadas
- Enviar muestra para su análisis: le permite enviar un archivo sospechoso para que lo analicen en el laboratorio de investigación de ESET (puede que no esté disponible en función de su configuración de ESET LiveGrid®).
- Cuarentena



Archivos de registro

Los archivos de registro contienen información relacionada con todos los sucesos importantes del programa y proporcionan información general acerca de las amenazas detectadas. Los registros constituyen una herramienta esencial en el análisis del sistema, la detección de amenazas y la resolución de problemas. Se lleva a cabo de forma activa en segundo plano, sin necesidad de que intervenga el usuario. La información se registra según el nivel de detalle de los registros. Los mensajes de texto y los registros se pueden ver directamente desde el entorno de ESET Endpoint Antivirus. También es posible comprimir los archivos de registro.

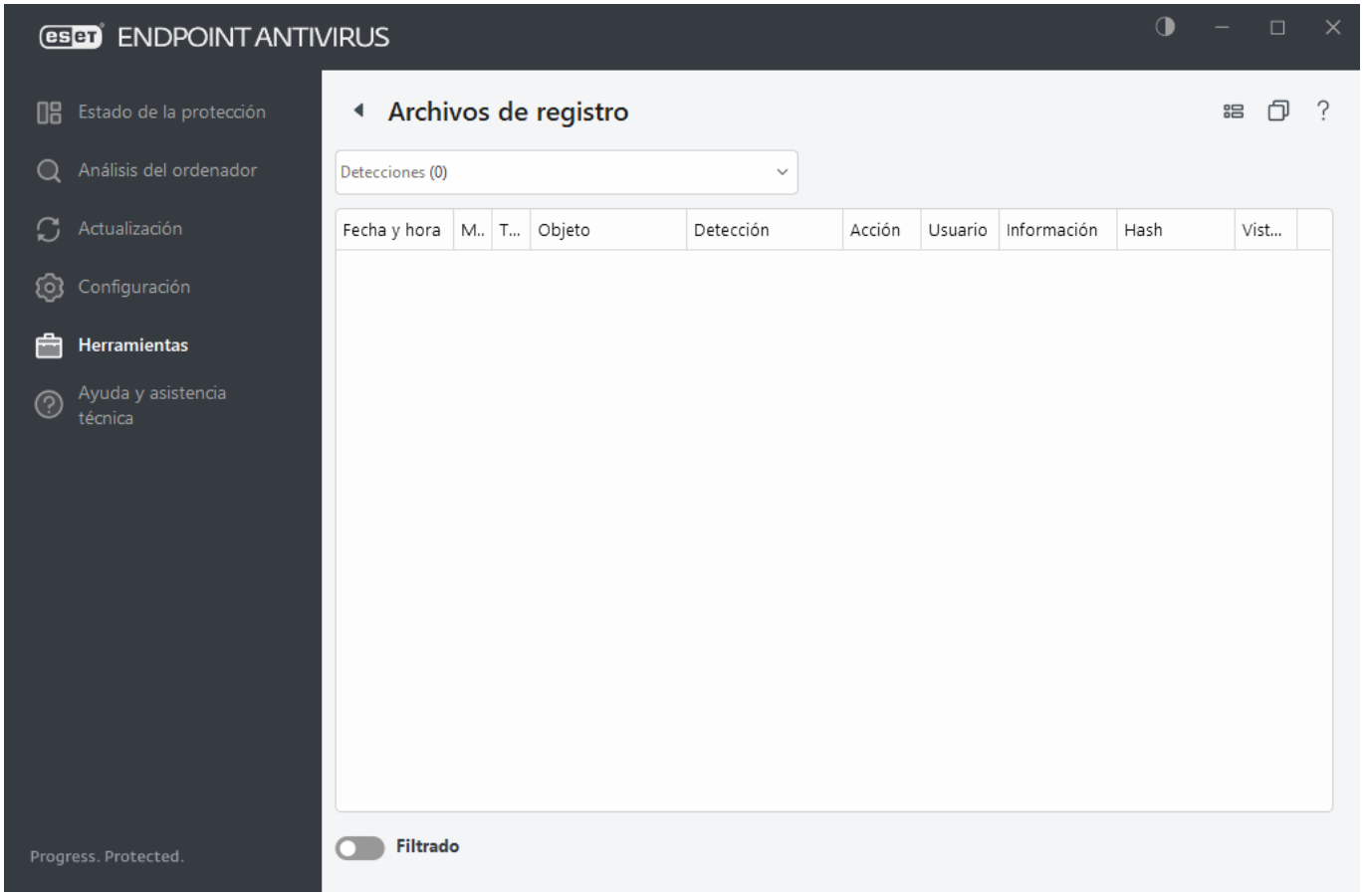
Se puede acceder a los archivos de registro desde ventana principal del programa de haciendo clic en **Herramientas** > **Archivos de registro**. Seleccione el tipo de registro que desee en el menú desplegable **Registrar**. Están disponibles los siguientes registros:

- **Amenazas detectadas**: este registro ofrece información detallada acerca de las amenazas y las infiltraciones detectadas por los módulos de ESET Endpoint Antivirus. La información incluye la hora de la detección, el nombre de la amenaza detectada, la ubicación, la acción realizada y el nombre del usuario con sesión iniciada en el momento en el que se detectó la infiltración. Haga doble clic en cualquier entrada del registro para ver sus detalles en una ventana independiente. Las infiltraciones no eliminadas siempre se marcan con texto rojo sobre fondo rojo claro; las infiltraciones eliminadas se marcan con texto amarillo sobre fondo blanco. Las PUA o las aplicaciones potencialmente peligrosas no eliminadas se marcan con texto amarillo sobre fondo blanco.
- **Sucesos**: todas las acciones importantes realizadas por ESET Endpoint Antivirus se registran en el registro de sucesos. El registro de sucesos contiene información sobre sucesos y errores que se produjeron en el programa. Esta opción se ha diseñado para ayudar a los administradores del sistema y los usuarios con la solución de problemas. Con frecuencia, la información aquí disponible puede ayudarle a encontrar una solución para un problema del programa.

- **Análisis del ordenador**: en esta ventana se muestran todos los resultados del análisis. Cada línea se corresponde con un control informático individual. Haga doble clic en cualquier entrada para ver los detalles del análisis correspondiente.
- **Archivos bloqueados**: contiene registros de los archivos bloqueados a los que no fue posible acceder al conectarse a ESET Enterprise Inspector. El protocolo muestra el motivo y el módulo de origen que bloqueó el archivo, así como la aplicación y el usuario que ejecutaron el archivo. Para obtener más información, consulte la guía del usuario de ESET Enterprise Inspector en línea.
- **Archivos enviados**: contiene registros de archivos enviados a ESET LiveGrid® o ESET LiveGuard para su análisis.
- **Registros de auditoría**: cada registro contiene información sobre la fecha y la hora en las que se realizó el cambio, el tipo de cambio, la descripción, la fuente y el usuario. Para obtener más información, consulte Registros de auditoría.
- **HIPS**: contiene registros de reglas específicas que se marcaron para su registro. El protocolo muestra la aplicación que invocó la operación, el resultado (si la regla se admitió o no) y el nombre de la regla creada.
- **Protección de la red**: el registro del cortafuegos muestra todos los ataques remotos detectados por la protección contra los ataques de red. Aquí encontrará información sobre todos los ataques a su ordenador. En la columna Suceso se incluyen los ataques detectados. En la columna Origen se proporciona más información sobre el atacante. En la columna Protocolo se indica el protocolo de comunicación que se utilizó para el ataque. El análisis del registro de protección de la red puede ayudarle a detectar a tiempo amenazas del sistema, para así poder evitar el acceso no autorizado al sistema. Para obtener más información sobre los ataques de red, consulte la sección Sistema de detección de intrusos y opciones avanzadas.

- **Sitios web filtrados**: esta lista es útil si desea ver una lista de sitios web bloqueados por la Protección de acceso a la web. En estos registros puede ver la hora, la URL, el usuario y la aplicación que estableció una conexión con el sitio web determinado.

- **Control de dispositivos**: contiene registros de los dispositivos o los soportes extraíbles conectados al ordenador. Solo los dispositivos con una regla de control de dispositivos se registran en el archivo de registro. Si la regla no coincide con un dispositivo conectado, no se creará una entrada de registro para un dispositivo conectado. Aquí puede ver también detalles como el tipo de dispositivo, número de serie, nombre del fabricante y tamaño del medio (si está disponible).



Seleccione el contenido de cualquier registro y pulse `Ctrl + C` **para copiarlo en el portapapeles**. Mantenga pulsadas las teclas `Ctrl + Shift` para seleccionar varias entradas.

Haga clic en **Filtrado** para abrir la ventana Filtrado de registros, donde puede definir los criterios de filtrado.

Haga clic con el botón derecho en un registro concreto para abrir el menú contextual. En este menú contextual, están disponibles las opciones siguientes:

- **Mostrar**: muestra información detallada sobre el registro seleccionado en una ventana nueva.
- **Filtrar los mismos registros**: tras activar este filtro, solo verá registros del mismo tipo (diagnósticos, advertencias, etc.).
- **Filtro**: después de hacer clic en esta opción, puede definir los criterios de filtrado para entradas de registro específicas en la ventana de filtrado de registros.
- **Activar filtro**: activa la configuración del filtro.
- **Desactivar filtro**: borra todos los ajustes del filtro (tal como se describe arriba).
- **Copiar/Copiar todo**: copia información sobre todos los registros de la ventana.
- **Copiar celda**: copia el contenido de la celda en la que se hace clic con el botón derecho.
- **Eliminar/Eliminar todos**: elimina los registros seleccionados, o todos los registros mostrados. Se necesitan privilegios de administrador para poder realizar esta acción.
- **Exportar**: exporta información acerca de los registros en formato XML.
- **Exportar todo**: exportar información acerca de todos los registros en formato XML.
- **Buscar/Buscar siguiente/Buscar anterior**: después de hacer clic en esta opción, puede definir los criterios de filtrado para resaltar la entrada específica desde la ventana Filtrado de registros.
- **Crear exclusión**: cree una nueva Exclusión de detección con un asistente (no disponible para detecciones de malware).

Filtrado de registros

Haga clic en **Filtrado** en **Herramientas** > **Archivos de registro** para definir los criterios de filtrado.

La característica de filtrado de registros le ayudará a encontrar la información que busca, especialmente cuando haya muchos registros. Le permite limitar las entradas de registro, por ejemplo, si busca un tipo específico de suceso, estado o periodo de tiempo. Para filtrar las entradas de registro, especifique determinadas opciones de búsqueda, y solo los registros relevantes (según esas opciones de búsqueda) se mostrarán en la ventana Archivos de registro.

Escriba en el campo **Buscar texto** la palabra clave que busca. Utilice el menú desplegable **Buscar en columnas** para restringir su búsqueda. Elija uno o más registros en el menú desplegable **Tipos de registro**. Defina el **Periodo de tiempo** al que desee que pertenezcan los resultados que se muestren. También puede utilizar otras opciones de búsqueda, como **Solo palabras completas** o **Distinguir mayúsculas y minúsculas**.

Buscar texto

Escriba una cadena (palabra o parte de una palabra). Solo se mostrarán los registros que contengan esta cadena. Los demás registros se omitirán.

Buscar en columnas

Seleccione las columnas que se tendrán en cuenta al buscar. Puede marcar una o más columnas que se utilizarán en la búsqueda.

Tipos de registro

Elija uno o más tipos de registro en el menú desplegable:

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Advertencias**: registra errores graves y mensajes de alerta.
- **Errores**: se registran los errores graves y errores del tipo "Error al descargar el archivo".
- **Críticos**: registra únicamente los errores graves (errores al iniciar la protección antivirus

Periodo de tiempo

Define el período de tiempo para el que desea visualizar los resultados.

- **No especificado** (predeterminado): no busca en el periodo de tiempo, sino en todo el registro.
- **Último día**
- **Última semana**
- **Último mes**
- **Periodo de tiempo**: puede especificar el periodo de tiempo exacto (Desde: y Hasta:) para filtrar solo los registros del periodo de tiempo especificado.

Solo palabras completas

Utilice la casilla de verificación si desea buscar palabras completas para obtener resultados más precisos.

Distinguir mayúsculas y minúsculas

Active esta opción si es importante utilizar letras mayúsculas o minúsculas al filtrar. Cuando haya configurado sus opciones de filtrado/búsqueda, haga clic en **Aceptar** para mostrar los registros filtrados o en Buscar para empezar a buscar. Los archivos de registro se buscan de arriba abajo, desde su posición (el registro resaltado). La búsqueda se detiene cuando se encuentra el primer registro que coincide con los criterios de dicha búsqueda. Pulse **F3** para buscar el siguiente registro o haga clic con el botón derecho y seleccione **Buscar** para restringir sus opciones de búsqueda.

Registros de auditoría

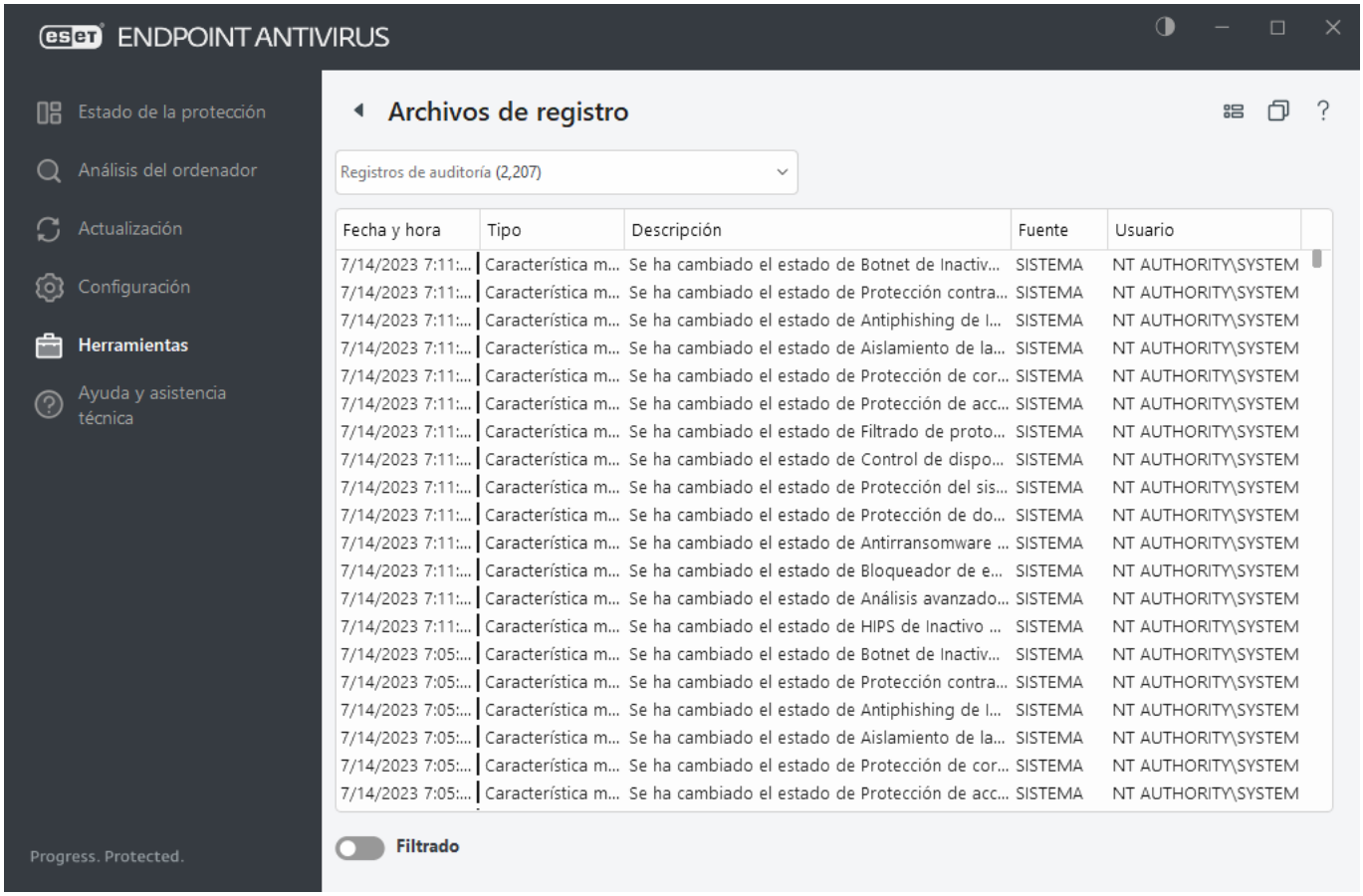
En un entorno empresarial, suelen haber varios usuarios con derechos de acceso definidos para la configuración de equipos. Como la modificación de la configuración del producto puede afectar radicalmente al funcionamiento del producto, es esencial que los administradores quieran controlar los cambios realizados por los usuarios para ayudar a los administradores a identificar y resolver rápidamente estos problemas o problemas similares, así como evitar que se repitan en el futuro.

El registro de auditoría es un nuevo tipo de registro que permite identificar el origen del problema. El registro de auditoría controla los cambios de configuración o el estado de la protección, y registra instantáneas que pueden consultarse en un futuro.

Para ver **Registro de auditoría**, haga clic en **Herramientas** en el menú principal y, a continuación, haga clic en **Archivos de registro** y seleccione **Registros de auditoría** en el menú desplegable.

El registro de auditoría contiene información sobre:

- Hora: cuándo se efectuó el cambio.
- Tipo: qué tipo de ajuste o función se modificó.
- Descripción: qué se modificó concretamente y qué parte del ajuste se ha cambiado, junto con el número de ajustes modificados.
- Origen: cuál es el origen del cambio.
- Usuario: quién efectuó el cambio.



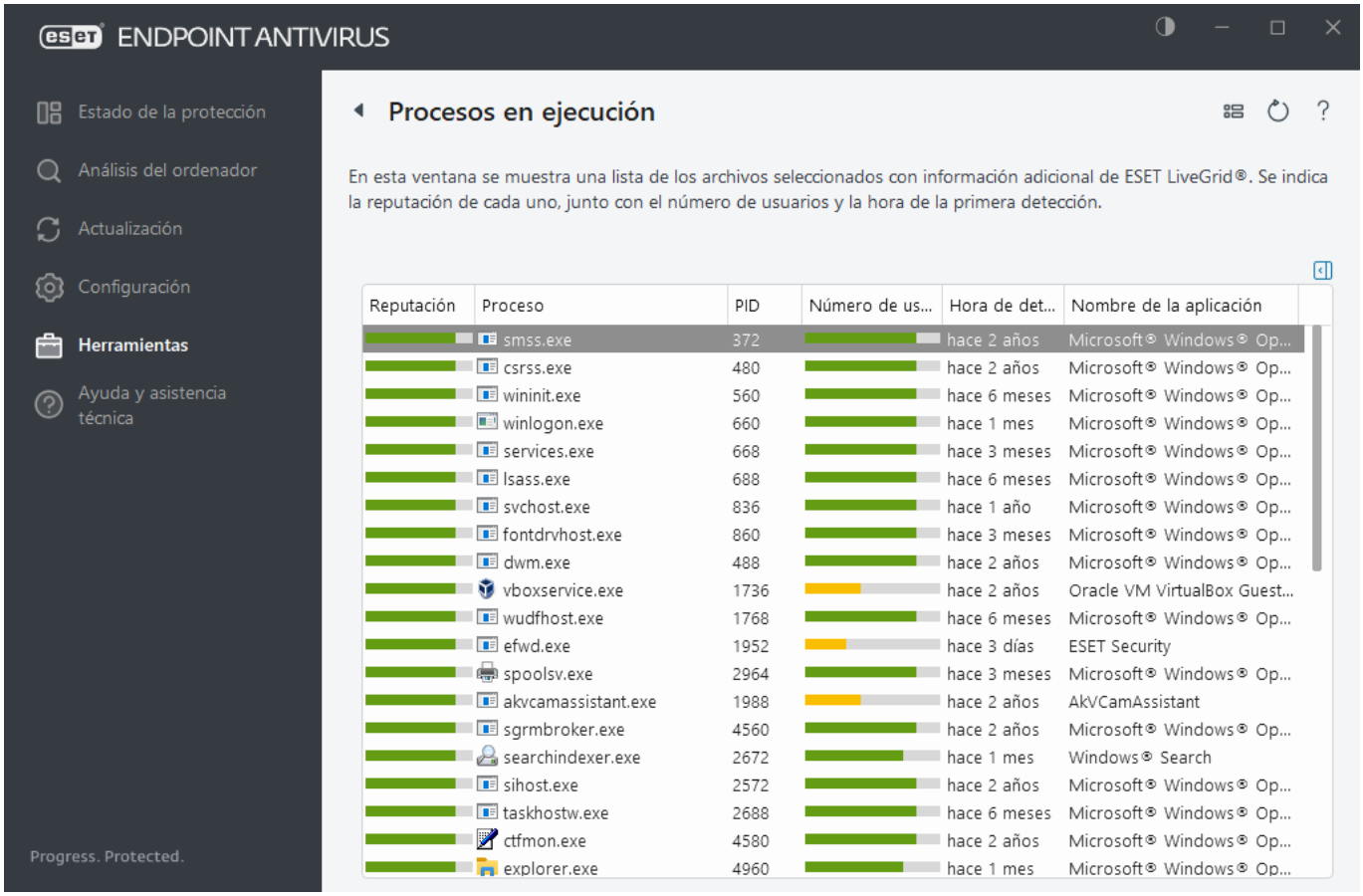
Haga clic con el botón derecho del ratón sobre cualquier tipo de registro de auditoría **Configuración modificada** en la ventana de archivos de registro, y seleccione **Mostrar cambios** en el menú contextual para mostrar información detallada sobre el cambio realizado. Además, puede restaurar el cambio del ajuste si hace clic en **Restaurar** desde el menú contextual (no disponible para un producto administrado mediante ESET PROTECT). Si selecciona **Eliminar todo** en el menú contextual, se creará un registro con información sobre esta acción.

Si la opción **Optimizar archivos de registro automáticamente** está activada en Configuración avanzada > **Herramientas** > **Archivos de registro**, los registros de auditoría se desfragmentarán automáticamente como otros registros.

Si la opción **Eliminar automáticamente los registros con una antigüedad de más de (días)** está activada en Configuración avanzada > **Herramientas** > **Archivos de registro**, las entradas del registro que tengan una antigüedad superior al número de días especificado se eliminarán automáticamente.

Procesos en ejecución

En Procesos en ejecución se indican los programas o procesos que se están ejecutando en el ordenador y se informa a ESET de forma inmediata y continua de las nuevas amenazas. ESET Endpoint Antivirus proporciona información detallada sobre los procesos en ejecución para proteger a los usuarios con la tecnología ESET LiveGrid® activada.



Reputación: en la mayoría de los casos, ESET Endpoint Antivirus y la tecnología ESET LiveGrid® asignan niveles de riesgo a los objetos (archivos, procesos, claves de registro, etc.) con una serie de reglas heurísticas que examinan las características de cada objeto y, a continuación, evalúan su potencial para la actividad maliciosa. Según estas heurísticas, a los objetos se les asignará un nivel de reputación desde el valor "9: mejor reputación" (en color verde) hasta "0: peor reputación" (en color rojo).

Proceso: nombre de la imagen del programa o proceso que se está ejecutando en el ordenador. También puede utilizar el Administrador de tareas de Windows para ver todos los procesos que están en ejecución en el ordenador. Para abrir el Administrador de tareas, haga clic con el botón derecho del ratón sobre un área vacía de la barra de tareas y, a continuación, haga clic en Administrador de tareas o pulse la combinación **Ctrl** + **Mayús** + **Esc** en el teclado.

PID: se trata de un identificador de los procesos que se ejecutan en sistemas operativos Windows.

> Las aplicaciones conocidas marcadas en verde son totalmente seguras (incluidas en lista blanca) y no se analizan; esto aumenta la velocidad del análisis del ordenador a petición o de la protección del sistema de archivos en tiempo real de este.

Número de usuarios: el número de usuarios que utilizan una aplicación determinada. La tecnología ESET LiveGrid® se encarga de recopilar esta información.

Hora de la detección: tiempo transcurrido desde que la tecnología ESET LiveGrid® detectó la aplicación.

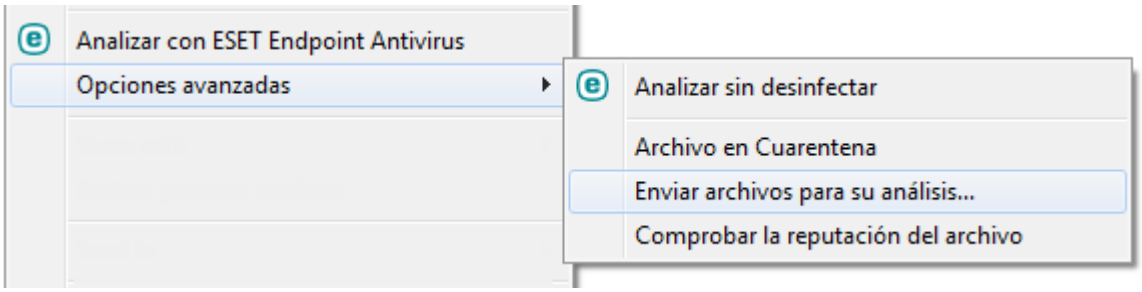
> Cuando una aplicación se marca con el nivel de seguridad Desconocido (naranja), no siempre se trata de software malicioso. Normalmente, se trata de una aplicación reciente. Si el archivo le plantea dudas, utilice la característica enviarlo para su análisis para enviarlo al laboratorio de virus de ESET. Si resulta que el archivo es una aplicación maliciosa, su detección se agregará a una de las siguientes actualizaciones del motor de detección.

Nombre de aplicación: nombre de un programa o un proceso.

Al hacer clic en una aplicación en la parte inferior, se mostrará la siguiente información en la parte inferior de la ventana:

- **Ruta**: ubicación de una aplicación en el ordenador.
- **Descripción**: características del archivo de acuerdo con la descripción del sistema operativo.
- **Versión**: información sobre el editor de la aplicación.
- **Empresa**: nombre del proveedor o el proceso de la aplicación.
- **Producto**: nombre de la aplicación o nombre comercial.
- **Tamaño**: tamaño del archivo en KB (kilobytes) o MB (megabytes).
- **Fecha de creación**: fecha y hora en que se creó una aplicación.
- **Fecha de modificación**: última fecha y hora en que se modificó una aplicación.

La reputación también se puede comprobar en los archivos que no actúan como programas o procesos en ejecución. Para ejecutarla, seleccione los archivos que desea comprobar, haga clic con el botón derecho del ratón en ellos y, en el menú contextual, seleccione **Opciones avanzadas** > **Comprobar la reputación del archivo con ESET LiveGrid®**.



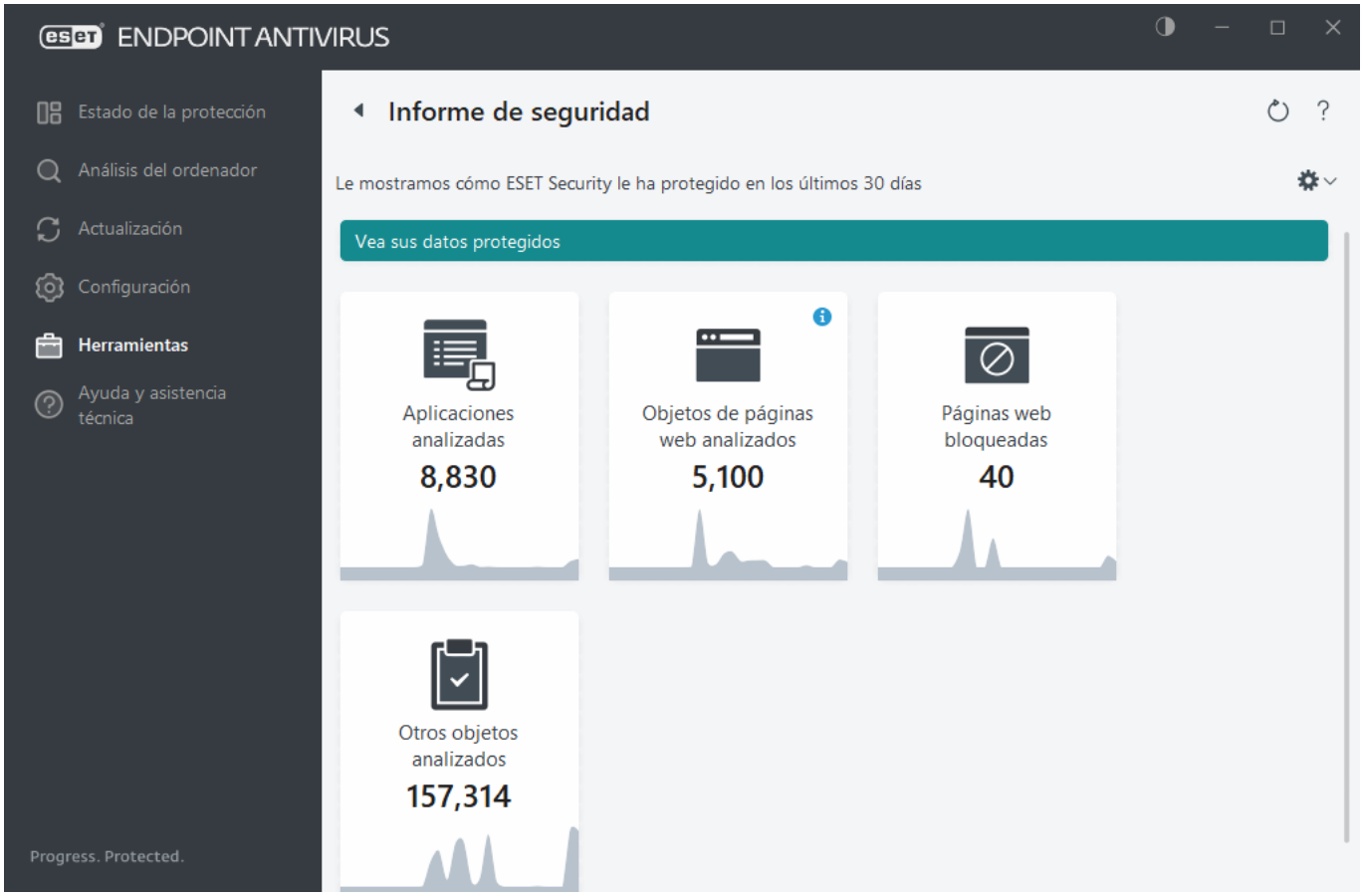
Informe de seguridad

Esta función ofrece una descripción general de las estadísticas para las siguientes categorías.

- **Páginas web bloqueadas**: muestra el número de páginas web bloqueadas (URL de PUA, phishing y router, IP o certificado hackeados en una lista negra).
- **Objetos de correo electrónico infectados detectados**: muestra el número de objetos de correo electrónico infectados detectados.
- **Aplicación potencialmente indeseable detectada**: muestra el número de aplicaciones potencialmente indeseables (PUA).
- **Documentos analizados**: muestra el número de objetos de documento analizados.
- **Aplicaciones analizadas**: muestra el número de objetos ejecutables analizados.
- **Otros objetos analizados**: muestra el número de otros objetos analizados.
- **Objetos de página web analizados**: muestra el número de objetos de página web analizados.
- **Objetos de correo electrónico analizados**: muestra el número de objetos de correo electrónico analizados.

El orden de estas categorías se basa en el valor numérico, de más alto a más bajo. Las categorías que tienen un valor cero no se muestran. Haga clic en **Mostrar más** para desplegar y mostrar las categorías ocultas.

Haga clic en la rueda del engranaje de la esquina superior derecha para **Activar/Desactivar notificaciones del informe de seguridad** o seleccione si se mostrarán datos de los últimos 30 días o desde que se activó el producto. Si ESET Endpoint Antivirus se instaló hace menos de 30 días, solo se podrá seleccionar el número de días que han transcurrido desde que se instaló. De forma predeterminada está establecido un periodo de 30 días.



Restablecer datos borrará todas las estadísticas y quitará los datos existentes en el informe de seguridad. Esta acción se debe confirmar, salvo si desea anular la selección de la opción **Preguntar antes de restablecer las estadísticas** en Configuración avanzada > **Notificaciones** > **Alertas interactivas** > **Mensajes de confirmación**.

ESET SysInspector

ESET SysInspector es una aplicación que inspecciona a fondo el ordenador, recopila información detallada sobre los componentes del sistema (como los controladores y aplicaciones instalados, las conexiones de red o las entradas importantes del registro) y evalúa el nivel de riesgo de cada componente. Esta información puede ayudar a determinar la causa de un comportamiento sospechoso del sistema, que puede deberse a una incompatibilidad de software o hardware o a una infección de código malicioso. Para aprender a usar ESET SysInspector, consulte la Ayuda en línea de ESET SysInspector.

En la ventana de ESET SysInspector se muestra la siguiente información sobre los registros:

- **Fecha y hora**: fecha y hora de creación del registro.
- **Comentario**: breve comentario.
- **Usuario**: nombre del usuario que creó el registro.
- **Estado**: estado de la creación del registro.

Están disponibles las siguientes acciones:

- **Mostrar**: abre el registro seleccionado en ESET SysInspector. También puede hacer clic con el botón derecho del ratón sobre un archivo de registro determinado y seleccionar **Mostrar** en el menú contextual.
- **Crear**: crea un registro nuevo. Espere a que se genere ESET SysInspector (estado **Creado**) antes de intentar acceder al registro. El registro se guarda en C:\ProgramData\ESET\ESET Security\SysInspector.

- **Eliminar**: elimina de la lista los archivos de registro seleccionados.

El menú contextual ofrece las siguientes opciones al seleccionar uno o más archivos de registro:

- **Mostrar**: abre el registro seleccionado en ESET SysInspector (igual que al hacer doble clic en un registro).
- **Crear**: crea un registro nuevo. Espere a que se genere ESET SysInspector (estado **Creado**) antes de intentar acceder al registro.
- **Eliminar**: elimina de la lista los archivos de registro seleccionados.
- **Eliminar todos**: elimina todos los registros.
- **Exportar**: exporta el registro a un archivo .xml o .xml comprimido.

Tareas programadas

el planificador de tareas administra e inicia las tareas programadas con la configuración y las propiedades predefinidas.

Tareas programadas está disponible en la ventana principal de ESET Endpoint Antivirus; para acceder, haga clic en **Herramientas** > **Tareas programadas**. El **Planificador de tareas** contiene una lista de todas las tareas programadas y sus propiedades de configuración, como la fecha, la hora y el perfil de análisis predefinidos utilizados.

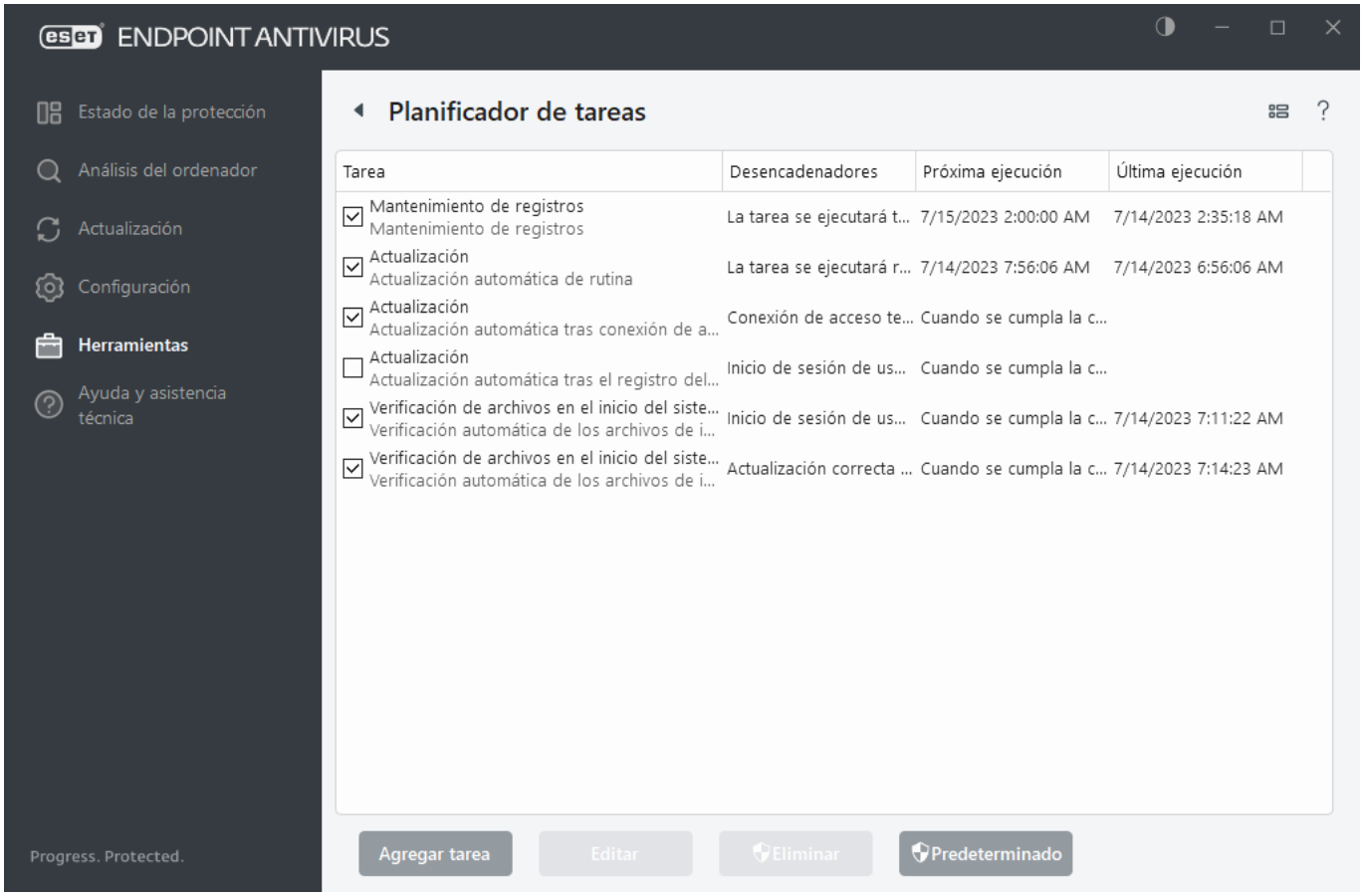
El Planificador de tareas sirve para programar las siguientes tareas: actualización del motor de detección, tarea de análisis, verificación de archivos en el inicio del sistema y mantenimiento de registros. Puede agregar o eliminar tareas directamente desde la ventana Planificador de tareas (haga clic en **Agregar tarea** o **Eliminar** en la parte inferior). Haga clic con el botón derecho en cualquier parte de la ventana Planificador de tareas para realizar las siguientes acciones: mostrar detalles de la tarea, ejecutar la tarea inmediatamente, agregar una tarea nueva y eliminar una tarea existente. Utilice las casillas de verificación disponibles al comienzo de cada entrada para activar o desactivar las tareas.

De forma predeterminada, en el **Planificador de tareas** se muestran las siguientes tareas programadas:

- **Mantenimiento de registros**
- **Actualización automática de rutina**
- **Actualización automática al detectar la conexión por módem**
- **Actualización automática después del registro del usuario**
- **Verificación automática de archivos en el inicio** (tras inicio de sesión del usuario)
- **Comprobación de la ejecución de archivos en el inicio** (tras una actualización correcta del módulo)

> En ESET PROTECT, se puede utilizar el retraso aleatorio de ejecución de la tarea para reducir la carga del servidor al ejecutar tareas, especialmente en redes grandes. Esta opción le permite definir un ámbito temporal durante el que se debe ejecutar una tarea en toda la red, en lugar de ejecutar una tarea en todas las estaciones de trabajo de toda la red al mismo tiempo. Cuando se ejecuta una tarea, el valor de tiempo definido se segmenta de forma aleatoria para asignar un tiempo de ejecución de tarea único a cada estación de trabajo de la red. Esto ayuda a evitar sobrecargas del servidor y problemas relacionados (por ejemplo, algunos servidores pueden informar de un ataque DoS al realizar una actualización masiva simultánea en estaciones de trabajo en toda la red).

Para modificar la configuración de una tarea programada existente (tanto predeterminada como definida por el usuario), haga clic con el botón derecho del ratón en la tarea y, a continuación, haga clic en **Modificar**, o seleccione la tarea que desea modificar y haga clic en el botón **Modificar**.



Agregar una nueva tarea

1. Haga clic en **Agregar tarea**, en la parte inferior de la ventana.
2. Escriba el nombre de la tarea.
3. Seleccione la tarea deseada en el menú desplegable:

- **Ejecutar aplicación externa**: programa la ejecución de una aplicación externa.
- **Mantenimiento de registros**: los archivos de registro también contienen restos de los registros eliminados. Esta tarea optimiza periódicamente los registros incluidos en los archivos para aumentar su eficacia.
- **Verificación de archivos en el inicio del sistema**: comprueba los archivos que se pueden ejecutar al encender o iniciar el sistema.
- **Crear un informe del estado del sistema**: crea una instantánea del ordenador de ESET SysInspector recopila información detallada sobre los componentes del sistema (por ejemplo controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.
- **Análisis del ordenador a petición**: analiza los archivos y las carpetas del ordenador.
- **Actualización**: programa una tarea de actualización mediante la actualización del motor de detección y los módulos del programa.

4. Active la opción **Activado** si desea activar la tarea (puede hacerlo más adelante mediante la casilla de verificación situada en la lista de tareas programas), haga clic en **Siguiente** y seleccione una de las opciones de programación:

- **Una vez**: la tarea se ejecutará en la fecha y a la hora predefinidas.
- **Reiteradamente**: la tarea se realizará con el intervalo de tiempo especificado.
- **Diariamente**: la tarea se ejecutará todos los días a la hora especificada.
- **Semanalmente**: la tarea se ejecutará el día y a la hora seleccionados.
- **Cuando se cumpla la condición**: la tarea se ejecutará tras un suceso especificado.

5. **Seleccione No ejecutar la tarea si está funcionando con batería** para minimizar los recursos del sistema mientras un ordenador portátil esté funcionando con batería. La tarea se ejecutará en la fecha y hora especificadas en el campo **Ejecución de la tarea**. Si la tarea no se pudo ejecutar en el tiempo predefinido, puede especificar cuándo se ejecutará de nuevo:

- **En la siguiente hora programada**
- **Lo antes posible**
- **Inmediatamente, si la hora desde la última ejecución excede un valor especificado** (el intervalo se puede definir con el cuadro **Tiempo desde la última ejecución**)

Para revisar una tarea programada, haga clic con el botón derecho en la tarea y, a continuación, haga clic en **Mostrar detalles de la tarea**.

Opciones de análisis programado

En esta ventana puede especificar opciones avanzadas para una tarea de análisis programado del ordenador.

Para ejecutar un análisis sin desinfección, haga clic en **Configuración avanzada** y seleccione **Analizar sin desinfectar**. El historial del análisis se guarda en el registro del análisis.

Cuando se selecciona **Ignorar exclusiones**, se analizan sin excepciones los archivos con extensiones excluidas anteriormente del análisis.

En el menú desplegable puede establecer la acción que desea efectuar automáticamente cuando concluya el análisis:

- **Sin acciones**: cuando el análisis concluya no se realizará ninguna acción.
- **Apagar**: el ordenador se apaga cuando finaliza el análisis.
- **Reiniciar**: cierra todos los programas abiertos y reinicia el ordenador cuando concluye el análisis.
- **Reiniciar si es necesario**: el ordenador se reinicia si solo es necesario para completar la limpieza de las amenazas detectadas.
- **Forzar reinicio**: fuerza el cierre de todos los programas abiertos sin esperar la intervención del usuario y reinicia el ordenador cuando concluye el análisis.
- **Forzar reinicio si es necesario**: el ordenador se reinicia si solo es necesario para completar la limpieza de las amenazas detectadas.
- **Suspender**: guarda la sesión y establece el ordenador en un estado de bajo consumo para que pueda retomar su trabajo rápidamente.
- **Hibernar**: recopila todos los programas y archivos que se encuentran en ejecución en la RAM y los guarda en un archivo especial de su disco duro. El ordenador se apaga, pero la próxima vez que lo encienda presentará el estado anterior al apagado.

> Las acciones **Suspender** o **Hibernar** estarán disponibles según la configuración de las opciones de encendido y suspensión del sistema operativo de su ordenador o las prestaciones correspondientes. Debe tener en cuenta que cuando el ordenador está en suspensión sigue en funcionamiento. Sigue ejecutando funciones básicas y utilizando electricidad si funciona con la alimentación de la batería. Si desea ahorrar carga de la batería, por ejemplo al salir de la oficina, le recomendamos utilizar la opción Hibernar.

Seleccione **El análisis no se puede cancelar** para impedir a los usuarios sin privilegios que detengan las acciones realizadas tras el análisis.

Seleccione la opción **El usuario puede poner en pausa el análisis durante (min)** si desea permitir que un usuario

limitado pause el análisis del ordenador durante un periodo de tiempo especificado.

Consulte también Progreso del análisis.

Resumen general de tareas programadas

En este cuadro de diálogo se muestra información detallada sobre la tarea programada seleccionada al hacer doble clic en una tarea personalizada o al hacer clic con el botón derecho del ratón en una tarea personalizada del planificador de tareas y, a continuación, hacer clic en **Mostrar detalles de la tarea**.

Detalles de la tarea

Escriba el **nombre de la tarea**, seleccione un **tipo de tarea** y, a continuación, haga clic en **Siguiente**:

- **Ejecutar aplicación externa**: programa la ejecución de una aplicación externa.
- **Mantenimiento de registros**: los archivos de registro también contienen restos de los registros eliminados. Esta tarea optimiza periódicamente los registros incluidos en los archivos para aumentar su eficacia.
- **Verificación de archivos en el inicio del sistema**: comprueba los archivos que se pueden ejecutar al encender o iniciar el sistema.
- **Crear un informe del estado del sistema**: crea una instantánea del ordenador de ESET SysInspector recopila información detallada sobre los componentes del sistema (por ejemplo controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.
- **Análisis del ordenador a petición**: analiza los archivos y las carpetas del ordenador.
- **Actualización**: programa una tarea de actualización mediante la actualización de los módulos.

Tiempo de las tareas

La tarea se repetirá con el intervalo de tiempo especificado. Seleccione una de las opciones de programación:

- **Una vez**: la tarea se ejecutará solo una vez en la fecha y a la hora predefinidas.
- **Reiteradamente**: la tarea se ejecutará en el intervalo especificado (en horas).
- **Diariamente**: la tarea se ejecutará todos los días a la hora especificada.
- **Semanalmente**: la tarea se ejecutará una o varias veces por semana, en los días y a la hora seleccionados.
- **Cuando se cumpla la condición**: la tarea se ejecutará tras un suceso especificado.

No ejecutar la tarea si está funcionando con batería: la tarea no se iniciará si el ordenador está funcionando con batería en el momento en que está programado el inicio de la tarea. Esto también se aplica a los ordenadores que funcionan con SAI (sistema de alimentación ininterrumpida).

Sincronización de la tarea: una vez

Ejecución de la tarea: la tarea especificada solo se ejecutará una vez a la fecha y hora especificadas.

Sincronización de la tarea: diariamente

La tarea se ejecutará todos los días a la hora especificada.

Sincronización de la tarea: semanalmente

La tarea se ejecutará todas las semanas en los días y horas seleccionados.

Sincronización de la tarea: cuando se cumpla la condición

La tarea se desencadenará cuando se produzca uno de los siguientes sucesos:

- **Cada vez que se inicie el ordenador.**
- **La primera vez que se inicie el ordenador en el día**
- **Conexión a Internet/VPN por módem**
- **Actualización de módulo correcta**
- **Actualización de producto correcta**
- **Registro del usuario**
- **Detección de amenazas**

Cuando se programa una tarea desencadenada por un suceso, se puede especificar el intervalo mínimo entre dos finalizaciones de la tarea. Por ejemplo, si inicia sesión en su ordenador varias veces al día, seleccione 24 horas para realizar la tarea solo en el primer inicio de sesión del día y, después, al día siguiente.

Tarea omitida

Una tarea se puede omitir si el ordenador está apagado o funciona con batería. Seleccione cuándo desea que se ejecute la tarea omitida y haga clic en **Siguiente**:

- **En la siguiente hora programada**: la tarea se ejecutará si el ordenador está encendido en la siguiente hora programada.
- **Lo antes posible**: la tarea se ejecutará cuando el ordenador esté encendido.
- **Inmediatamente, si el tiempo desde la última ejecución programada supera (horas)**: representa el tiempo transcurrido desde la primera ejecución omitida de la tarea. Si se supera este tiempo, la tarea se ejecutará inmediatamente.

Inmediatamente, si el tiempo desde la última ejecución programada supera (horas) –ejemplos

Hay una tarea de ejemplo configurada para que se ejecute de forma reiterada en cada hora. La opción **Inmediatamente, si el tiempo desde la última ejecución programada supera (horas)** está seleccionada y el tiempo superado está establecido en dos horas. La tarea se ejecuta a las 13:00 y, cuando finaliza, el ordenador se queda en suspensión:

• El ordenador se activa a las 15:30. La primera ejecución omitida de la tarea fue a las 14:00. Solo han transcurrido 1,5 horas desde las 14:00, por lo que la tarea se ejecutará a las 16:00.

• El ordenador se activa a las 16:30. La primera ejecución omitida de la tarea fue a las 14:00. Han transcurrido dos horas y media desde las 14:00, por lo que la tarea se ejecutará inmediatamente.

Detalles de la tarea: actualización

Si desea actualizar el programa desde dos servidores de actualización, es necesario crear dos perfiles de actualización diferentes. Así, si el primer servidor no descarga los archivos de actualización, el programa cambia al otro automáticamente. Esta función es útil para portátiles, por ejemplo, ya que normalmente se actualizan desde un servidor de actualización LAN local, aunque sus propietarios suelen conectarse a Internet utilizando otras redes. Así pues, en caso de que el primer perfil falle, el segundo descargará automáticamente los archivos de actualización de los servidores de actualización de ESET.

Detalles de la tarea: ejecutar aplicación

Esta tarea programa la ejecución de una aplicación externa.

Archivo ejecutable: seleccione un archivo ejecutable en el árbol de directorios y haga clic en la opción **...**, o introduzca la ruta manualmente.

Carpeta de trabajo: defina el directorio de trabajo de la aplicación externa. Todos los archivos temporales del **archivo ejecutable** seleccionado se crearán en este directorio.

Parámetros: parámetros de la línea de comandos de la aplicación (opcional).

Haga clic en **Finalizar** para aplicar la tarea.

Envío de muestras para el análisis

Si encuentra un archivo sospechoso en su ordenador o un sitio sospechoso en Internet, puede enviarlos al laboratorio de investigación de ESET para que los analicen (puede que no esté disponible en función de su configuración de ESET LiveGrid®).

No envíe muestras que no cumplan al menos uno de los siguientes criterios:

• Su producto de ESET no detecta la muestra.

• La muestra se detecta como una amenaza, pero no lo es.

• No aceptamos archivos personales (que le gustaría que ESET analizara para buscar malware) como muestras (el laboratorio de investigación de ESET no realiza análisis bajo demanda para sus usuarios).

• Utilice un asunto descriptivo y adjunte toda la información posible sobre el archivo (por ejemplo, una captura de pantalla o el sitio web del que lo descargó).

El envío de muestras le permite enviar con uno de estos métodos un archivo o un sitio a ESET para que los

analice:

1. Con el cuadro de diálogo de envío de muestras, que está en **Herramientas** > **Enviar muestra para su análisis**.
2. También puede enviar el archivo por correo electrónico. Si prefiere esta opción, comprima los archivos con WinRAR/ZIP, proteja el archivo comprimido con la contraseña "infected" y envíelo a samples@eset.com.
3. Para informar de spam o falsos positivos de spam, consulte el artículo de la base de conocimiento de ESET.

Con **Seleccionar muestra para el análisis**, seleccione la descripción que mejor se ajuste a su mensaje en el menú desplegable **Motivo de envío de la muestra**:

- Archivo sospechoso
- Sitio sospechoso (sitio web que está infectado por código malicioso)
- Archivo de falso positivo (archivo que se detecta como amenaza pero no está infectado)
- Sitio de falso positivo
- Otros

Archivo/Sitio: la ruta del archivo o sitio web que quiere enviar.

Correo electrónico de contacto: la dirección de correo de contacto se envía a ESET junto con los archivos sospechosos y se puede utilizar para el contacto con usted en caso de que sea necesario enviar más información para poder realizar el análisis. Introducir una dirección de correo electrónico de contacto es opcional. Seleccione **Enviar de forma anónima** para dejar el campo vacío.

> No obtendrá ninguna respuesta de ESET a menos que sea necesario que envíe información adicional. Cada día, nuestros servidores reciben decenas de miles de archivos, lo que hace imposible responder a todos los envíos.
> Si la muestra resulta ser una aplicación o un sitio web maliciosos, su detección se agregará a una actualización futura de ESET.

Seleccionar muestra para el análisis: archivo sospechoso

Signos y síntomas observados de la infección por código malicioso: describa el comportamiento del archivo sospechoso que ha observado en el ordenador.

Origen del archivo (dirección URL o proveedor): escriba el origen (fuente) del archivo y cómo llegó a él.

Notas e información adicional: aquí puede especificar más información o una descripción que le ayude con el proceso de identificación del archivo sospechoso.

> El primer parámetro (**Signos y síntomas observados de la infección por código malicioso**) es necesario; la información adicional que proporcione será de gran utilidad para nuestros laboratorios en el proceso de identificación de muestras.

Seleccionar muestra para el análisis: sitio sospechoso

Seleccione una de las opciones siguientes en el menú desplegable **Problema del sitio**:

- **Infectado**: sitio web que contiene virus u otro código malicioso distribuido por diversos métodos.
- **Phishing**: su objetivo suele ser acceder a datos confidenciales como, por ejemplo, números de cuentas bancarias, códigos PIN, etc. Puede obtener más información sobre este tipo de ataque en el glosario.
- **Fraude**: sitio web fraudulento o de estafas, destinado sobre todo a obtener un beneficio rápido.
- Seleccione **Otros** si las opciones anteriores no hacen referencia al sitio que va a enviar.

Notas e información adicional: aquí puede especificar más información o una descripción que ayude a analizar el sitio web sospechoso.

Seleccionar muestra para el análisis: archivo de falso positivo

Le rogamos que nos envíe los archivos que se detectan como amenazas pero no están infectados, para mejorar nuestro motor de antivirus y antiespía y ayudar a proteger a otras personas. Los falsos positivos (FP) se generan cuando el patrón de un archivo coincide con un mismo patrón disponible en un motor de detección.

Nombre y versión de la aplicación: título y versión del programa (por ejemplo, número, alias o nombre en código).

Origen del archivo (dirección URL o proveedor): escriba el origen (fuente) del archivo y cómo llego a él.

Objetivo de la aplicación: descripción general de la aplicación, tipo de aplicación (por ejemplo, navegador, reproductor multimedia, etc.) y su funcionalidad.

Notas e información adicional: aquí puede especificar más información o una descripción que ayude a procesar el archivo sospechoso.

> Los tres primeros parámetros son necesarios para identificar las aplicaciones legítimas y distinguirlas del código malicioso. La información adicional que proporcione será de gran ayuda para los procesos de identificación y procesamiento de muestras en nuestros laboratorios.

Seleccionar muestra para el análisis: sitio de falso positivo

Le solicitamos que nos envíe los sitios que se detectan como amenazas, fraudes o phishing, pero no lo son. Los falsos positivos (FP) se generan cuando el patrón de un archivo coincide con un mismo patrón disponible en un motor de detección. Proporcione este sitio web para mejorar nuestro motor de antivirus y anti-phishing y ayudar a proteger a otras personas.

Notas e información adicional: aquí puede especificar más información o una descripción que ayude a procesar el sitio web sospechoso.

Seleccionar muestra para el análisis: otros

Utilice este formulario si el archivo no se puede categorizar como un **Archivo sospechoso** o un **Falso positivo**.

Motivo de envío del archivo: introduzca una descripción detallada y el motivo por el que envía el archivo.

Cuarentena

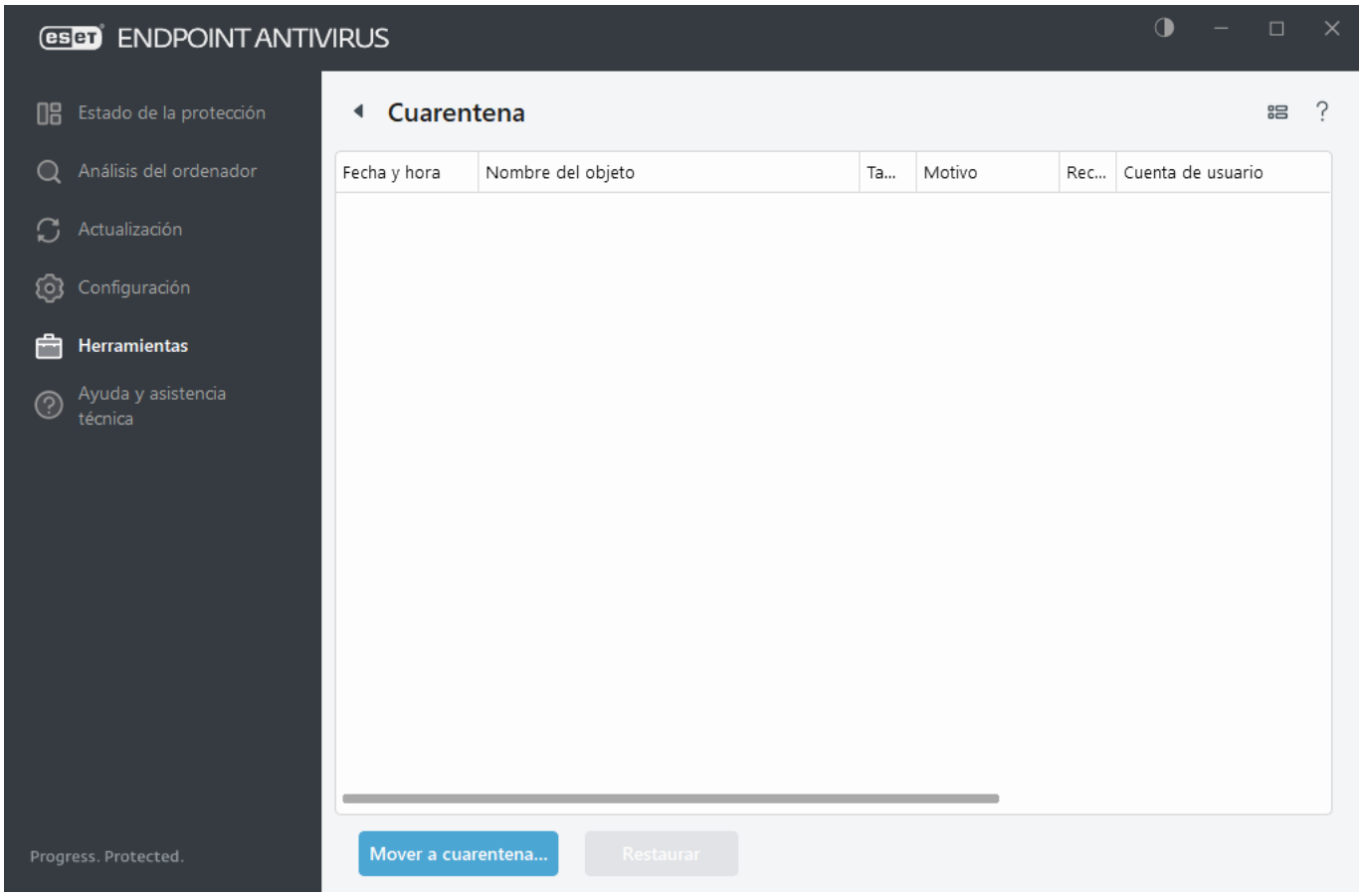
La función principal de la cuarentena es almacenar de forma segura objetos que se clasifican como peligrosos (como malware, archivos infectados o aplicaciones potencialmente indeseables).

La cuarentena está disponible en la ventana principal de ESET Endpoint Antivirus; para acceder, haga clic en **Herramientas** > **Cuarentena**.

Los archivos almacenados en la carpeta de cuarentena se pueden ver en una tabla que muestra:

- La fecha y la hora de la cuarentena.
- La ruta de acceso a la ubicación original del archivo.
- Su tamaño en bytes.
- Motivo (por ejemplo, objeto agregado por el usuario).
- Número de detecciones (por ejemplo, detecciones duplicadas de un mismo archivo o si se trata de un archivo comprimido que contiene varias infiltraciones).

Administro la cuarentena en estaciones de trabajo cliente de forma remota



Poner archivos en cuarentena

ESET Endpoint Antivirus pone en cuarentena automáticamente los archivos eliminados (si no ha cancelado esta opción en la ventana de alertas).

Otros archivos se deben poner en cuarentena si:

- No se pueden desinfectar.
- No es seguro ni aconsejable eliminarlos.
- ESET Endpoint Antivirus los detecta incorrectamente como infectados.
- El comportamiento de un archivo es sospechoso, pero el análisis no lo detecta.

Para poner en cuarentena un archivo, tiene varias opciones:

- Utilice la función de arrastrar y colocar para poner en cuarentena un archivo manualmente al hacer clic en el archivo, desplazar el cursor del ratón hasta la zona marcada mientras se mantiene pulsado el botón del ratón, para después soltarlo. Después, la aplicación pasa al primer plano.
- Haga clic en **Mover a cuarentena** en la ventana principal del programa.
- El menú contextual también se puede utilizar con este fin: haga clic con el botón derecho en la ventana **Cuarentena** y seleccione **Poner en cuarentena**.

Restauración de archivos de cuarentena

Los archivos en cuarentena también pueden restaurarse en su ubicación original:

- Utilice la función **Restaurar** para tal fin, disponible desde el menú contextual si hace clic con el botón derecho en un archivo determinado en cuarentena.
- Si un archivo se marca como aplicación potencialmente indeseable, la opción **Restaurar y excluir del análisis** se activa. Consulte también Exclusiones.
- El menú contextual también ofrece la opción **Restaurar a**, que le permite restaurar archivos en una ubicación distinta de la cual se eliminaron.
- La función de restauración no está disponible en algunos casos, por ejemplo, para los archivos que se encuentran en un recurso compartido de red de solo lectura.

Eliminación de archivos de cuarentena

Haga clic con el botón derecho del ratón en el elemento que desee y seleccione **Eliminar de la cuarentena**, o seleccione el elemento que desee eliminar y pulse **Suprimir** en el teclado. También es posible seleccionar varios elementos y eliminarlos al mismo tiempo. Los elementos eliminados se eliminarán de forma permanente de su dispositivo y de la cuarentena.

Envío de un archivo de cuarentena

Si ha puesto en cuarentena un archivo sospechoso que el programa no ha detectado o si se ha determinado incorrectamente que un archivo está infectado (por ejemplo, por el análisis heurístico del código) y, consecuentemente, se ha puesto en cuarentena, envíe la muestra al laboratorio de investigación de ESET para su análisis. Para enviar un archivo, haga clic con el botón derecho del ratón en el archivo y seleccione **Enviar para su análisis** en el menú contextual.

Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:
- Administrar la cuarentena en ESET PROTECT
- Mi producto de ESET me ha avisado de una detección, ¿qué debo hacer?

Ayuda y asistencia técnica

Haga clic en **Ayuda y asistencia técnica** en la ventana principal del programa para mostrar información de soporte técnico y herramientas de solución de problemas que le ayudarán a resolver los problemas que pueda encontrar.

Producto instalado

- Acerca de ESET Endpoint Antivirus: muestra información sobre su copia de ESET Endpoint Antivirus.
- Resolver problemas con el producto: haga clic en este vínculo para buscar soluciones a los problemas más frecuentes.
- Resolver problemas con la licencia: haga clic en este vínculo para buscar soluciones a problemas relacionados con la activación o el cambio de licencia.
- Cambiar licencia: haga clic para abrir la ventana de activación y activar el producto.

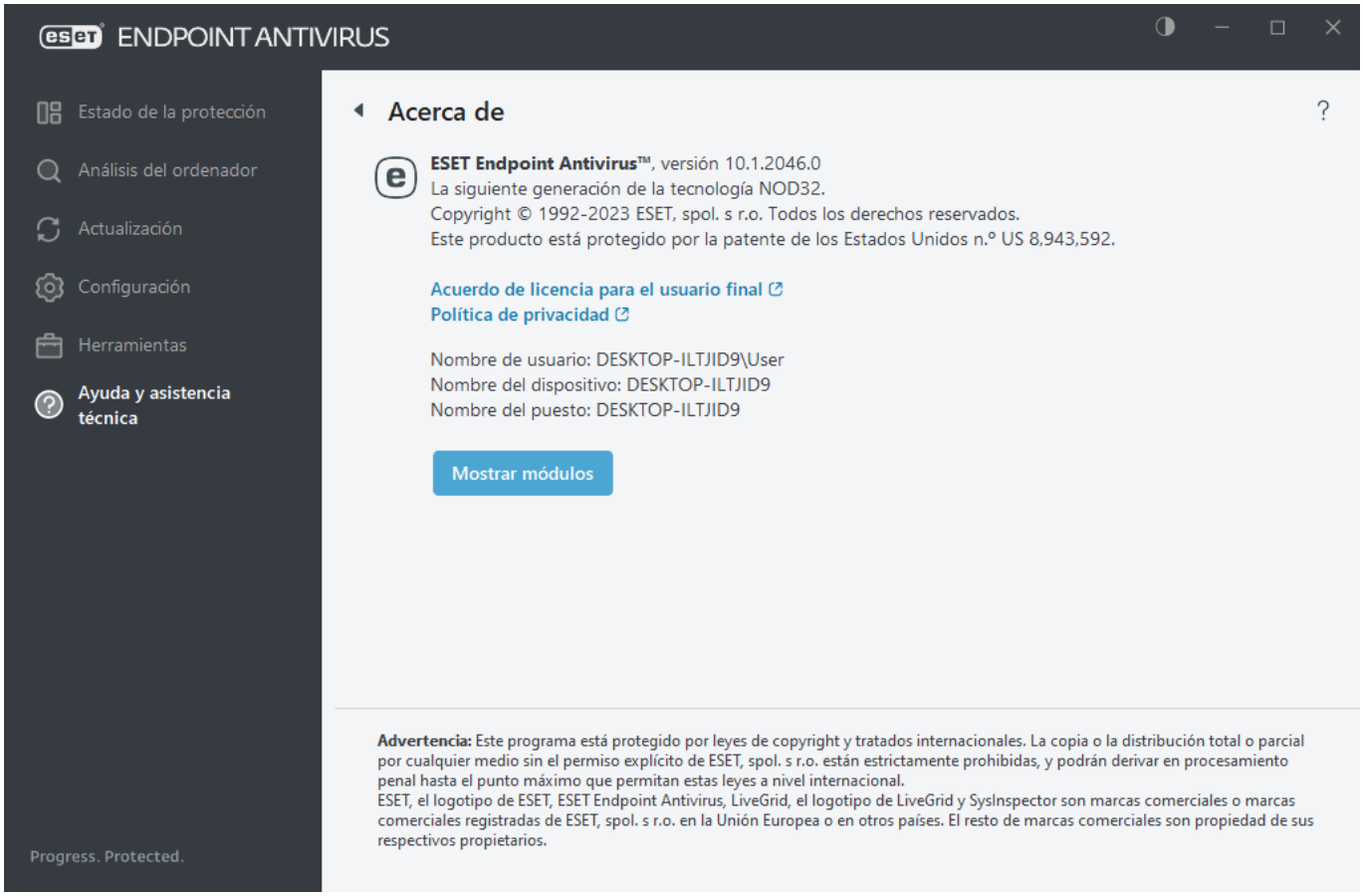
Página de ayuda: haga clic en este enlace para abrir las páginas de ayuda de ESET Endpoint Antivirus.

Soporte técnico

Base de conocimientos: la base de conocimiento de ESET contiene respuestas a las preguntas más frecuentes y posibles soluciones a diferentes problemas. La actualización periódica por parte de los especialistas técnicos de ESET convierte a esta base de conocimientos en la herramienta más potente para resolver diversos problemas.

Acerca de ESET Endpoint Antivirus

En esta ventana se muestran detalles sobre la versión instalada de ESET Endpoint Antivirus y su ordenador.



Haga clic en **Mostrar módulos** para ver información sobre la lista de módulos del programa cargados.

- Para copiar en el portapapeles información sobre los módulos, haga clic en **Copiar**. Esto puede ser útil para resolver problemas o ponerse en contacto con el servicio de soporte técnico.
- Haga clic en **Motor de detección** en la ventana Módulos para abrir el radar de virus de ESET, que contiene información sobre cada versión del Motor de detección de ESET.

Enviar datos de configuración del sistema

Con el fin de prestar asistencia con la máxima rapidez y precisión posibles, ESET requiere información sobre la configuración de ESET Endpoint Antivirus, información detallada y de los procesos en ejecución (Archivo de registro de ESET SysInspector), así como datos del registro. ESET utilizará estos datos solo para prestar asistencia técnica al cliente.

Después de enviar el formulario web, también se enviarán a ESET los datos de configuración de su sistema. Seleccione **Enviar siempre esta información** si desea recordar esta acción para este proceso. Para enviar el formulario web sin enviar ningún dato, haga clic en **No enviar datos** y continúe.

Puede configurar el envío de los datos de configuración del sistema en Configuración avanzada > **Herramientas** > **Diagnóstico** > Soporte técnico.

Si ha decidido enviar los datos de configuración del sistema, es necesario completar y enviar el formulario web. De lo contrario, no se creará el ticket y se perderán los datos de configuración del sistema. Si no se pueden enviar los datos de configuración del sistema, rellene el formulario web y espere las instrucciones del Soporte técnico.

Soporte técnico

En la ventana principal del programa, haga clic en **Ayuda y asistencia técnica** > **Soporte técnico**.

Ponerse en contacto con el servicio de soporte técnico

Solicitar soporte: si no encuentra respuesta a su problema, puede usar este formulario del sitio web de ESET para ponerse rápidamente en contacto con el departamento de soporte técnico de ESET. En función de su configuración, se mostrará la ventana de envío de datos de configuración del sistema antes de rellenar el formulario web.

Obtener información de soporte técnico

Detalles para el servicio de soporte técnico: cuando se le solicite, podrá copiar y enviar información al servicio de soporte técnico de ESET (como, por ejemplo, detalles de la licencia, nombre del producto, versión del producto, sistema operativo e información sobre el ordenador).

ESET Log Collector – vínculo al artículo de la base de conocimiento de ESET, donde puede descargar ESET Log Collector, aplicación que recopila información y registros de un ordenador automáticamente para ayudar a resolver problemas con mayor rapidez. Si desea obtener más información, consulte la guía del usuario de ESET Log Collector en línea.

Active **Registro avanzado** para crear registros avanzados de todas las funciones disponibles con el objetivo de ayudar a los desarrolladores a diagnosticar y resolver problemas. El nivel mínimo de detalle del registro es **Diagnóstico**. El registro avanzado se desactivará automáticamente después de dos horas, a menos que lo detenga antes haciendo clic en **Detener registro avanzado**. Una vez creados todos los registros, aparece la ventana de notificación, que proporciona acceso directo a la carpeta Diagnóstico con los registros creados.

Configuración avanzada

La configuración avanzada le permite configurar ajustes ESET Endpoint Antivirus detallados para satisfacer sus necesidades.

Para abrir Configuración avanzada, abra la ventana principal del programa y presione la tecla **F5** del teclado o haga clic en **Configuración** > **Configuración avanzada**.

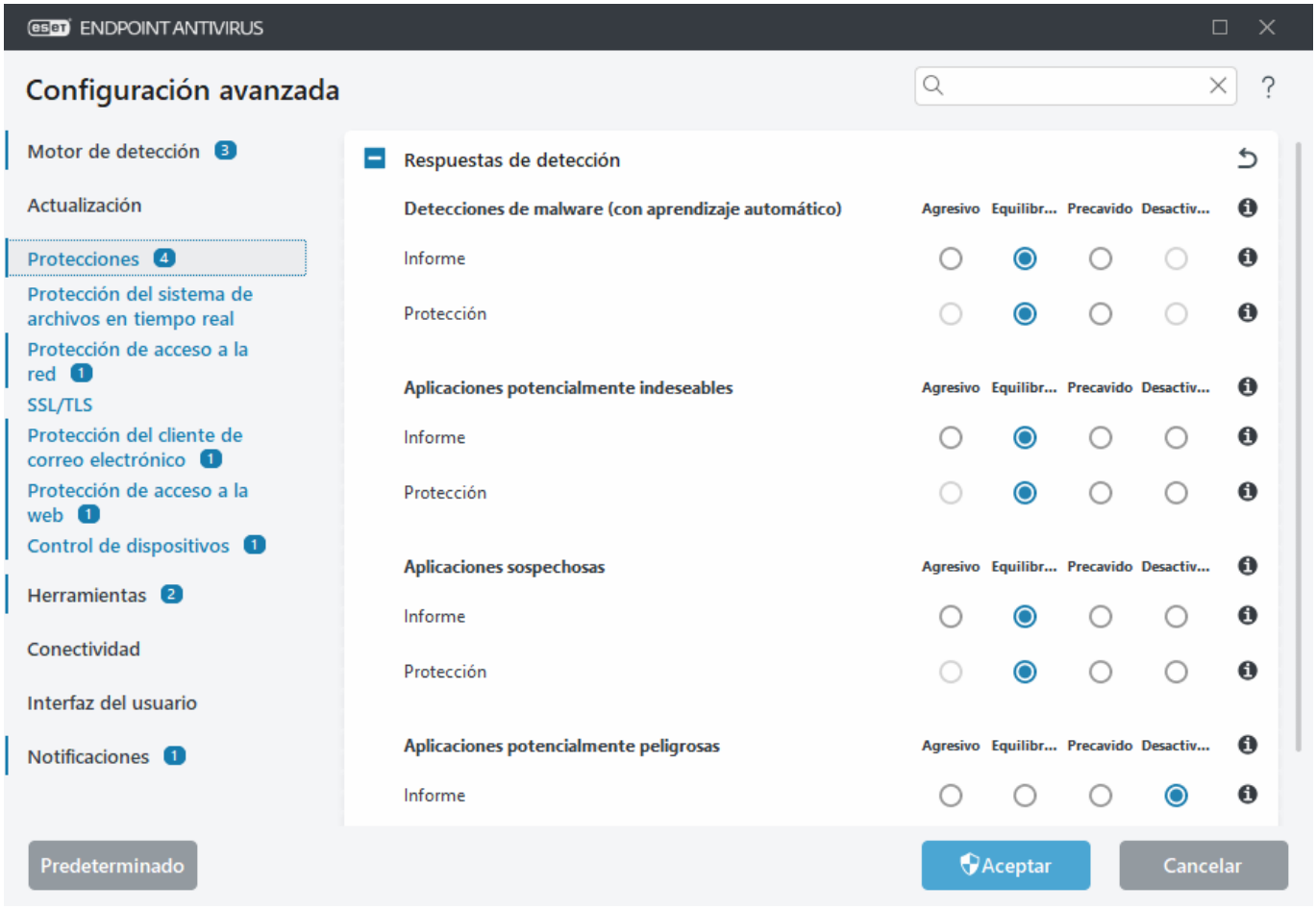
> Al crear una política desde ESET PROTECT Consola Web, puede seleccionar el indicador de cada ajuste. Los ajustes que tengan el indicador Forzar tendrán prioridad y no podrán sobrescribirse con una política posterior (aunque también tenga este indicador establecido). Esta práctica garantiza que el ajuste no se verá modificado (por ejemplo, por el usuario o por políticas posteriores a la hora de ejecutar la fusión). Para obtener más información, consulte la ayuda en línea de Indicadores de ESET PROTECT.

> En función de su configuración de acceso, es posible que se le pida que escriba una contraseña para abrir la configuración avanzada.

En la configuración avanzada, puede configurar los siguientes ajustes:

- Motor de detección
- Actualización

- Protecciones
- Herramientas
- Conectividad
- Interfaz del usuario
- Notificaciones



Motor de detección

Configuración avanzada > **Motor de detección** le permite configurar las siguientes opciones:

- Exclusiones
- Opciones avanzadas
- Análisis de tráfico de red

Exclusiones

Exclusiones le permite excluir objetos del motor de detección. Para garantizar que se analizan todos los objetos, le recomendamos que solo cree exclusiones cuando sea absolutamente necesario. Entre las situaciones en las que quizá deba excluir un objeto se pueden incluir el análisis de entradas de grandes bases de datos, que ralentizaría su ordenador durante un análisis, o de software que entre en conflicto con el análisis.

Exclusiones de rendimiento: excluya archivos y carpetas del análisis. Las exclusiones de rendimiento son útiles para excluir el análisis a nivel de archivo de aplicaciones de juego o cuando cause un comportamiento anómalo del sistema o un aumento del rendimiento.

Las exclusiones de detección le permiten excluir de la desinfección objetos mediante el nombre de detección, la ruta de acceso o su hash. Las exclusiones de detección no excluyen archivos y carpetas del análisis como las exclusiones de rendimiento. Las exclusiones de detección solo excluyen objetos cuando los detecta el motor de detección y existe una regla apropiada en la lista de exclusiones.

No deben confundirse con otros tipos de exclusiones:

- Exclusiones de procesos: todas las operaciones de archivos atribuidas a procesos de aplicaciones excluidos se excluyen del análisis (puede ser necesario para aumentar la velocidad de la copia de seguridad y la disponibilidad del servicio).
- Extensiones de archivo excluidas
- Exclusiones del HIPS
- Filtro de exclusión para protección en la nube

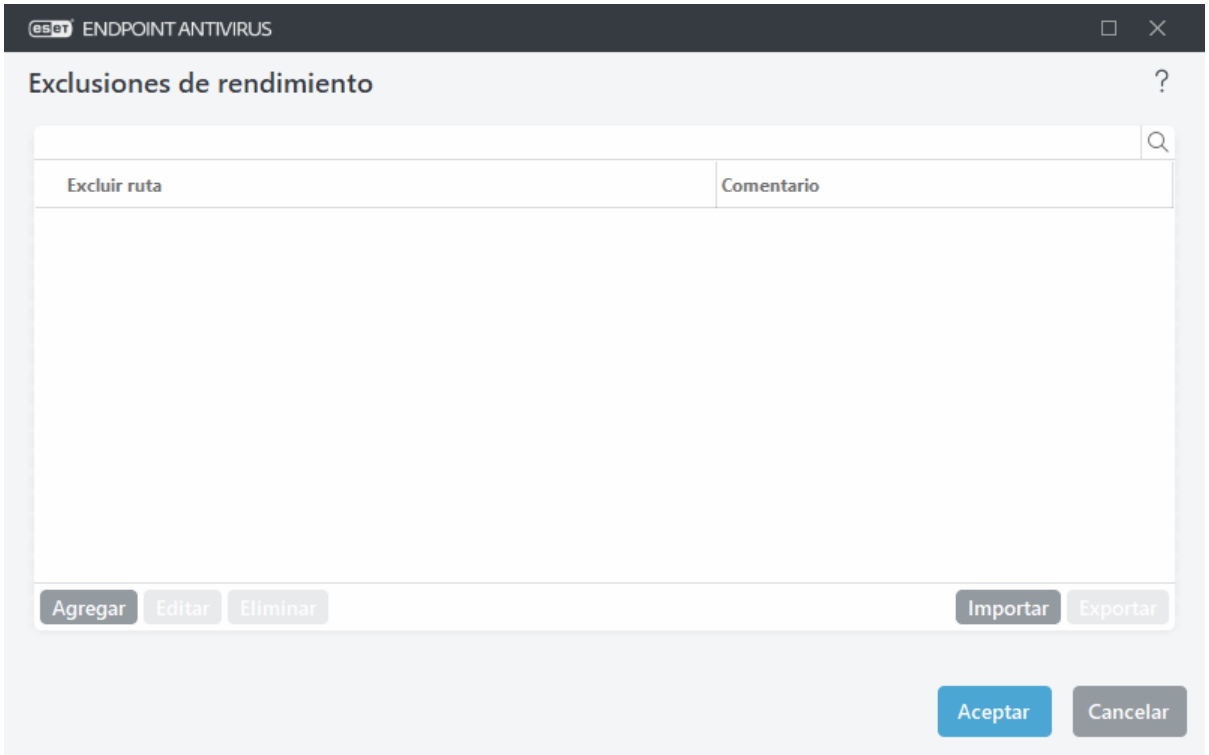
Exclusiones de rendimiento

Las exclusiones de rendimiento le permiten excluir archivos y carpetas del análisis.

Para garantizar que se analizan todos los objetos en busca de amenazas, le recomendamos que solo cree exclusiones cuando sea absolutamente necesario. Sin embargo, hay situaciones en las que puede necesitar excluir un objeto, como en el caso de las entradas de bases de datos grandes que ralentizarían su ordenador durante un análisis o en el del software que entre en conflicto con el análisis.

Puede agregar los archivos y las carpetas que se excluirán del análisis a la lista de exclusiones en Configuración avanzada > **Motor de detección** > **Exclusiones** > **Exclusiones de rendimiento** > **Editar**.

Para excluir un objeto (ruta de acceso: archivo o carpeta) del análisis, haga clic en **Agregar** e introduzca la ruta de acceso aplicable o selecciónelo en la estructura de árbol.



El módulo de **protección del sistema de archivos en tiempo real** o de **análisis del ordenador** no detectará las amenazas que haya contenidas en un archivo si este cumple los criterios de exclusión del análisis.

Elementos de control

- **Agregar**: agregue una nueva entrada para excluir objetos del análisis.
- **Modificar**: le permite modificar las entradas seleccionadas.
- **Eliminar**: quita las entradas seleccionadas (pulse CTRL y haga clic para seleccionar varias entradas).
- **Importar/Exportar**: la importación y la exportación de exclusiones de rendimiento son útiles cuando necesita realizar una copia de seguridad de las exclusiones actuales para utilizarla en otro momento. La opción de exportación de configuración también es de utilidad para los usuarios en entornos no administrados que desean utilizar su configuración preferida en varios sistemas, ya que les permite importar fácilmente un archivo .txt para transferir estos ajustes.

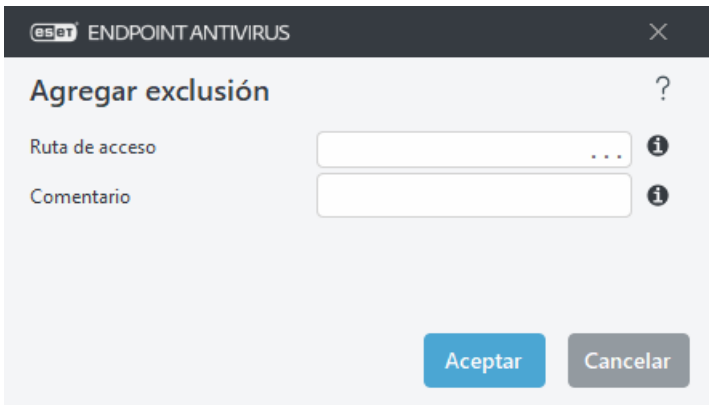
  Ejemplo de visualización del formato de archivo de importación/exportación

```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagement.PerformanceExclusions","columns":["Path","Description"]}

C:\Backup\*,custom comment

C:\pagefile.sys
```

Agregar o modificar la exclusión de rendimiento

Este cuadro de diálogo excluye una ruta de acceso (archivo o directorio) específica de este ordenador.

> Para elegir una ruta de acceso apropiada, haga clic en **...** en el campo **Ruta de acceso**. Cuando la introduzca manualmente, vea más ejemplos de formato de exclusión a continuación.



Puede utilizar comodines para excluir un grupo de archivos. El signo de interrogación (*?*) representa un carácter único, y el asterisco (***) una cadena variable de cero o más caracteres.

• Si desea excluir todos los archivos y subcarpetas de una carpeta, escriba la ruta de acceso a la carpeta y utilice la máscara *.
• Si desea excluir únicamente los archivos .doc, utilice la máscara *.doc.
• Si el nombre de un archivo ejecutable tiene un determinado número de caracteres (con caracteres distintos) y solo conoce el primero (por ejemplo, "D"), utilice el siguiente formato:
D????.exe (los signos de interrogación sustituyen a los caracteres que faltan o son desconocidos)
Ejemplos:
• *C:\Tools**: la ruta de acceso debe terminar con la barra invertida (\) y el asterisco (*) para indicar que es una carpeta y se excluirá todo el contenido de la carpeta (archivos y subcarpetas).
• *C:\Tools*.**: el mismo comportamiento que *C:\Tools**.
• *C:\Tools*: no se excluirá la carpeta *Tools*. Desde la perspectiva del análisis, *Tools* también puede ser un nombre de archivo.
• *C:\Tools*.dat*: esto excluirá los archivos .dat de la carpeta *Tools*.
• *C:\Tools\sg.dat*: esto excluirá este archivo concreto de la ruta de acceso exacta.

Puede utilizar variables del sistema, como *%PROGRAMFILES%*, para definir las exclusiones del análisis.
• Para excluir la carpeta Program Files con esta variable del sistema, utilice la ruta de acceso *%PROGRAMFILES%** (recuerde agregar la barra invertida y el asterisco al final de la ruta de acceso) al agregarla a las exclusiones.
• Para excluir todos los archivos y carpetas de un subdirectorio de *%PROGRAMFILES%*, utilice la ruta de acceso *%PROGRAMFILES%\Directorio_excluido**

Ampliar la lista de variables del sistema compatibles

En el formato de exclusión de ruta de acceso se pueden usar las siguientes variables:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
No son compatibles las variables del sistema específicas de usuario (como *%TEMP%* o *%USERPROFILE%*) ni variables de entorno (como *%PATH%*).

El uso de comodines en el medio de una ruta de acceso (por ejemplo, *C:\Tools*\Data\file.dat*) puede funcionar, pero no es compatible oficialmente con las exclusiones de rendimiento. Consulte el siguiente artículo de la base de conocimiento para obtener más información.
Cuando usa exclusiones de detección, no hay restricciones en lo que respecta al uso de comodines en el medio de una ruta de acceso.

Orden de las exclusiones:
• No hay opciones para ajustar el nivel de prioridad de las exclusiones con los botones arriba/abajo.
• Cuando el motor de análisis encuentre la primera regla aplicable, no se evaluará la segunda regla aplicable.
• Cuantas menos reglas haya, mayor será el rendimiento de análisis.
• Evite crear reglas simultáneas.

Formato de exclusión de ruta de acceso

Puede utilizar comodines para excluir un grupo de archivos. El signo de interrogación (*?*) representa un carácter único, y el asterisco (***) una cadena variable de cero o más caracteres.

• Si desea excluir todos los archivos y subcarpetas de una carpeta, escriba la ruta de acceso a la carpeta y utilice la máscara *.
• Si desea excluir únicamente los archivos .doc, utilice la máscara *.doc.
• Si el nombre de un archivo ejecutable tiene un determinado número de caracteres (con caracteres distintos) y solo conoce el primero (por ejemplo, "D"), utilice el siguiente formato:
D????.exe (los signos de interrogación sustituyen a los caracteres que faltan o son desconocidos)
Ejemplos:
• *C:\Tools**: la ruta de acceso debe terminar con la barra invertida (\) y el asterisco (*) para indicar que es una carpeta y se excluirá todo el contenido de la carpeta (archivos y subcarpetas).
• *C:\Tools*.**: el mismo comportamiento que *C:\Tools**.
• *C:\Tools*: no se excluirá la carpeta *Tools*. Desde la perspectiva del análisis, *Tools* también puede ser un nombre de archivo.
• *C:\Tools*.dat*: esto excluirá los archivos .dat de la carpeta *Tools*.
• *C:\Tools\sg.dat*: esto excluirá este archivo concreto de la ruta de acceso exacta.

Puede utilizar variables del sistema, como *%PROGRAMFILES%*, para definir las exclusiones del análisis.
• Para excluir la carpeta Program Files con esta variable del sistema, utilice la ruta de acceso *%PROGRAMFILES%** (recuerde agregar la barra invertida y el asterisco al final de la ruta de acceso) al agregarla a las exclusiones.
• Para excluir todos los archivos y carpetas de un subdirectorio de *%PROGRAMFILES%*, utilice la ruta de acceso *%PROGRAMFILES%\Directorio_excluido**

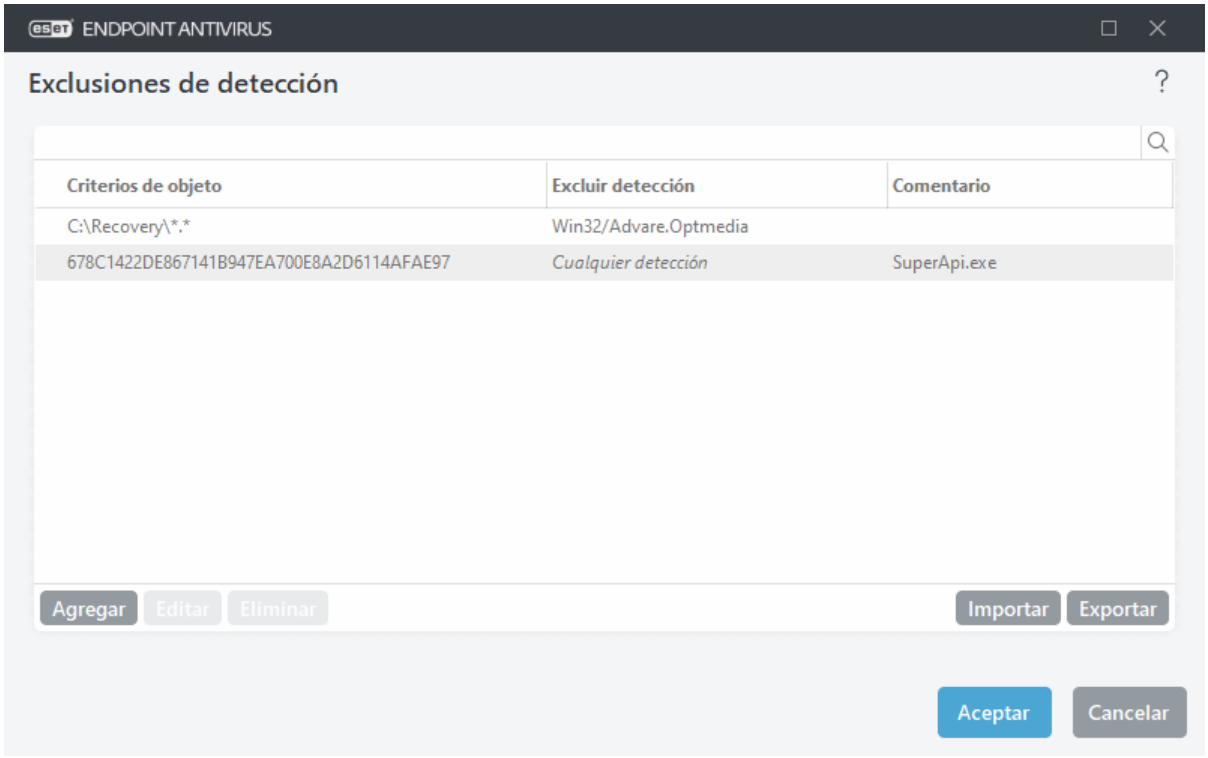
Ampliar la lista de variables del sistema compatibles

En el formato de exclusión de ruta de acceso se pueden usar las siguientes variables:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
No son compatibles las variables del sistema específicas de usuario (como *%TEMP%* o *%USERPROFILE%*) ni variables de entorno (como *%PATH%*).

Exclusiones de detección

Las exclusiones de detección le permiten excluir objetos de la desinfección filtrando el nombre de detección, la ruta de acceso del objeto o su hash.

Las exclusiones de detección no excluyen archivos y carpetas del análisis como las Exclusiones de rendimiento. Las exclusiones de detección solo excluyen objetos cuando los detecta el motor de detección y existe una regla apropiada en la lista de exclusiones.
Por ejemplo (consulte la primera fila de la imagen que aparece a continuación), cuando un objeto se detecta como Win32/Adware.Optmedia y el archivo detectado es *C:\Recovery\file.exe*. En la segunda fila, cada archivo, que tiene el hash SHA-1 apropiado, se excluirá siempre a pesar del nombre de detección.



Para garantizar que se detecten todas las amenazas, recomendamos crear exclusiones de detección solo cuando sea absolutamente necesario.

Para agregar archivos y carpetas a la lista de exclusiones, abra Configuración avanzada > **Motor de detección** > **Exclusiones** > **Exclusiones de detección** > **Editar**.

Para excluir un objeto (por su nombre de detección o hash) de la desinfección, haga clic en **Agregar**.

En el caso de Aplicaciones potencialmente indeseables y Aplicaciones potencialmente peligrosas, también se puede crear la exclusión por su nombre de detección:

- En la ventana de alerta que informa de la detección (haga clic en **Mostrar opciones avanzadas** y, a continuación, seleccione **Excluir de la detección**).
- Desde el menú contextual Archivos de registro con el Asistente de creación de exclusión de detección.
- Haciendo clic en **Herramientas** > **Cuarentena** y, a continuación, haciendo clic con el botón derecho en el archivo en cuarentena y seleccionando **Restaurar y excluir del análisis** en el menú contextual.

Criterios de objetos de exclusiones de detección

- **Ruta de acceso**: limite una exclusión de detección para una ruta de acceso especificada (o para cualquiera).
- **Nombre de la detección**: si se muestra el nombre de una detección junto a un archivo excluido, significa que el archivo se excluye únicamente para dicha detección, pero no por completo. Si más adelante este archivo se infecta con otro malware, se detectará.
- **Hash**: excluye un archivo según el hash especificado SHA-1, sea cual sea el tipo de archivo, la ubicación, el nombre o su extensión.

Elementos de control

- **Agregar**: agregue una nueva entrada para excluir objetos de la desinfección.
- **Modificar**: le permite modificar las entradas seleccionadas.
- **Eliminar**: quita las entradas seleccionadas (pulse CTRL y haga clic para seleccionar varias entradas).
- **Importar/Exportar**: la importación y la exportación de exclusiones de detección son útiles cuando necesita realizar una copia de seguridad de las exclusiones actuales para utilizarla en otro momento. La opción de exportación de configuración también es de utilidad para los usuarios en entornos no administrados que desean utilizar su configuración preferida en varios sistemas, ya que les permite importar fácilmente un archivo .txt para transferir estos ajustes.

  Ejemplo de visualización del formato de archivo de importación/exportación

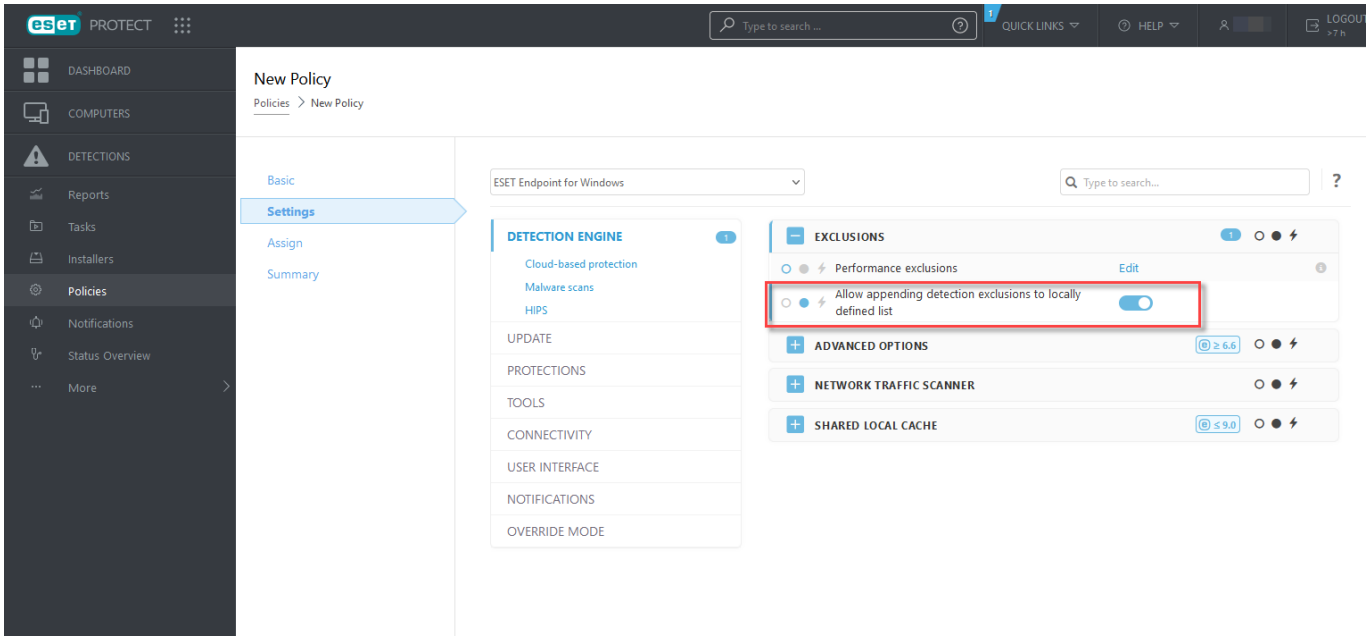
```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","File Hash"]}

4c59cd02-357c-4b20-a0ac-ca8400000001,,,SuperApi.exe,00117F70C86ADB0F979021391A8AEAA497C2C8DF

2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,
```

Configuración de exclusiones de detección en ESET PROTECT

Asistente de gestión de exclusiones de detección de ESET PROTECT: cree una exclusión de detección y aplíquela a más ordenadores o grupos.

Posible anulación de exclusiones de detección desde ESET PROTECT

Cuando hay una lista local de exclusiones de detección, el administrador debe aplicar una política con **Permitir agregar exclusiones de detección a una lista definida localmente**. A continuación, la acción de agregar exclusiones de detección desde ESET PROTECT funcionará como se espera.

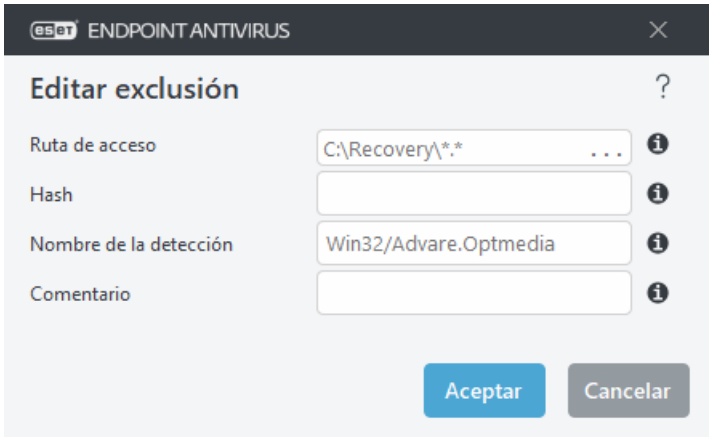


Agregar o editar una exclusión de detección

Excluir detección

Se debe facilitar un nombre de detección de ESET válido. Para obtener un nombre de detección válido, consulte Archivos de registro y, a continuación, seleccione **Detecciones** en el menú desplegable Archivos de registro. Esta opción resulta útil cuando se está detectando un falso positivo en ESET Endpoint Antivirus. Excluir infiltraciones reales es muy peligroso, por lo que le recomendamos que excluya únicamente los archivos o los directorios afectados haciendo clic en **...** en el campo **Ruta de acceso** o solo durante un periodo de tiempo concreto. Las exclusiones también se aplican a las Aplicaciones potencialmente indeseables, las aplicaciones potencialmente peligrosas y las aplicaciones sospechosas.

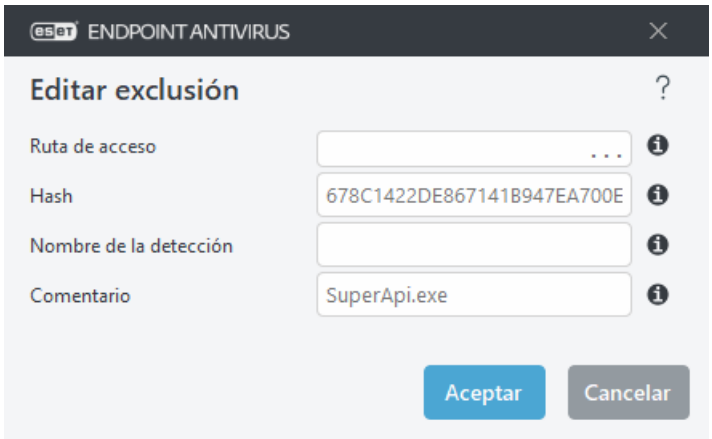
Consulte también Formato de exclusión de ruta de acceso.



Consulte el Ejemplo de exclusiones de detección a continuación.

Excluir hash

Excluye un archivo según el hash especificado SHA-1, sea cual sea el tipo de archivo, la ubicación, el nombre o su extensión.



Para excluir una detección específica por su nombre, escriba el nombre de detección válido:
Win32/Adware.Optmedia
También puede usar el siguiente formato cuando excluye una detección de la ventana de alerta de ESET Endpoint Antivirus:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Elementos de control

- **Agregar**: excluye los objetos de la detección.
- **Modificar**: le permite modificar las entradas seleccionadas.
- **Eliminar**: quita las entradas seleccionadas (pulse CTRL y haga clic para seleccionar varias entradas).

Asistente de creación de exclusión de detección

Las exclusiones de detección también se pueden crear desde el menú contextual Archivos de registro (no disponible para detecciones de malware):

1. En la ventana del programa principal, haga clic en **Herramientas** > **Archivos de registro**.
2. Haga clic con el botón derecho en una detección en el **Registro de detecciones**.
3. Haga clic en **Crear exclusión**.

Para excluir una o más detecciones en función de los **Criterios de exclusión**, haga clic en **Cambiar criterios**:

- **Archivos exactos**: excluya cada archivo por su hash SHA-1.
- **Detección**: excluya cada archivo por su nombre de detección.
- **Ruta de acceso + Detección**: excluya cada archivo por su nombre de detección y ruta de acceso, incluido el nombre del archivo (por ejemplo, *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

La opción recomendada se preselecciona en función del tipo de detección.

También puede agregar un **Comentario** antes de hacer clic en **Crear exclusión**.

Opciones avanzadas del motor de detección

Activar análisis avanzado mediante AMSI es la herramienta Interfaz de análisis contra el código malicioso de Microsoft que permite el análisis de scripts Powershell, scripts ejecutados por Windows Script Host y datos analizados con el SDK de AMSI.

Análisis de tráfico de red

El escáner de tráfico de red proporciona protección contra malware para protocolos de aplicación, que integra múltiples técnicas avanzadas de escaneo de malware. El analizador de tráfico de red analiza los protocolos

HTTP(S), POP3(S) e IMAP(S) automáticamente, independientemente del navegador de Internet o del cliente de correo electrónico. Puede activar/desactivar el analizador de tráfico de red en Configuración avanzada > **Motor de detección** > **Analizador de tráfico de red**.

Activar analizador de tráfico de red: si desactiva esta opción, no se analizarán los protocolos HTTP(S), POP3(S) e IMAP(S). Tenga en cuenta que las siguientes funciones ESET Endpoint Antivirus requieren que el analizador de tráfico de red esté habilitado:

- Protección del acceso a la Web
- SSL/TLS
- Protección Anti-Phishing
- Protección de clientes de correo electrónico

Protección en la nube

ESET LiveGrid® (que se basa en el sistema avanzado de alerta temprana ThreatSense.Net) utiliza los datos enviados por usuarios de ESET de todo el mundo y los envía al laboratorio de investigación de ESET. ESET LiveGrid® Proporciona metadatos y muestras sospechosas, lo cual nos permite reaccionar de forma inmediata a las necesidades de nuestros clientes y hace posible la respuesta de ESET a las amenazas más recientes.

Están disponibles las opciones siguientes:

Opción 1: activar el sistema de reputación ESET LiveGrid®

El sistema de reputación ESET LiveGrid® permite crear listas blancas y listas negras en la nube.

Consultar la reputación de los archivos y Procesos en ejecución directamente en la interfaz del programa o en el menú contextual; además, disponen de información adicional en ESET LiveGrid®.

Opción 2: activar el sistema de respuesta ESET LiveGrid®

Además del sistema de reputación ESET LiveGrid®, el sistema de respuesta ESET LiveGrid® recopilará información anónima del ordenador relacionada con las amenazas detectadas recientemente. Esta información puede incluir una muestra o copia del archivo donde haya aparecido la amenaza, la ruta a ese archivo, el nombre de archivo, la fecha y la hora, el proceso por el que apareció la amenaza en el ordenador e información sobre el sistema operativo del ordenador.

De forma predeterminada, ESET Endpoint Antivirus está configurado para enviar archivos sospechosos para su análisis detallado en el laboratorio de virus de ESET. Los archivos con determinadas extensiones, como *.doc* o *.xls*, se excluyen siempre. También puede agregar otras extensiones para excluir los archivos específicos que usted o su empresa no deseen enviar.

Opción 3: optar por no activar ESET LiveGrid®

El software no perderá funcionalidad, pero puede que ESET Endpoint Antivirus responda más rápido a las nuevas amenazas que la actualización del motor de detección cuando ESET LiveGrid® está activado.

> Puede obtener más información sobre ESET LiveGrid® en el glosario.
> Consulte nuestras instrucciones con ilustraciones en inglés y otros idiomas sobre cómo activar o desactivar ESET LiveGrid® en ESET Endpoint Antivirus.

Configuración de la protección en la nube en Configuración avanzada

Para acceder a la configuración de ESET LiveGrid®, abra Configuración avanzada > **Motor de detección** > **Protección en la nube**.

Activar el sistema de reputación ESET LiveGrid® (recomendado): el sistema de reputación ESET LiveGrid® mejora la eficiencia de las soluciones contra software malicioso de ESET mediante la comparación de los archivos analizados con una base de datos de elementos incluidos en listas blancas y negras disponibles en la nube.

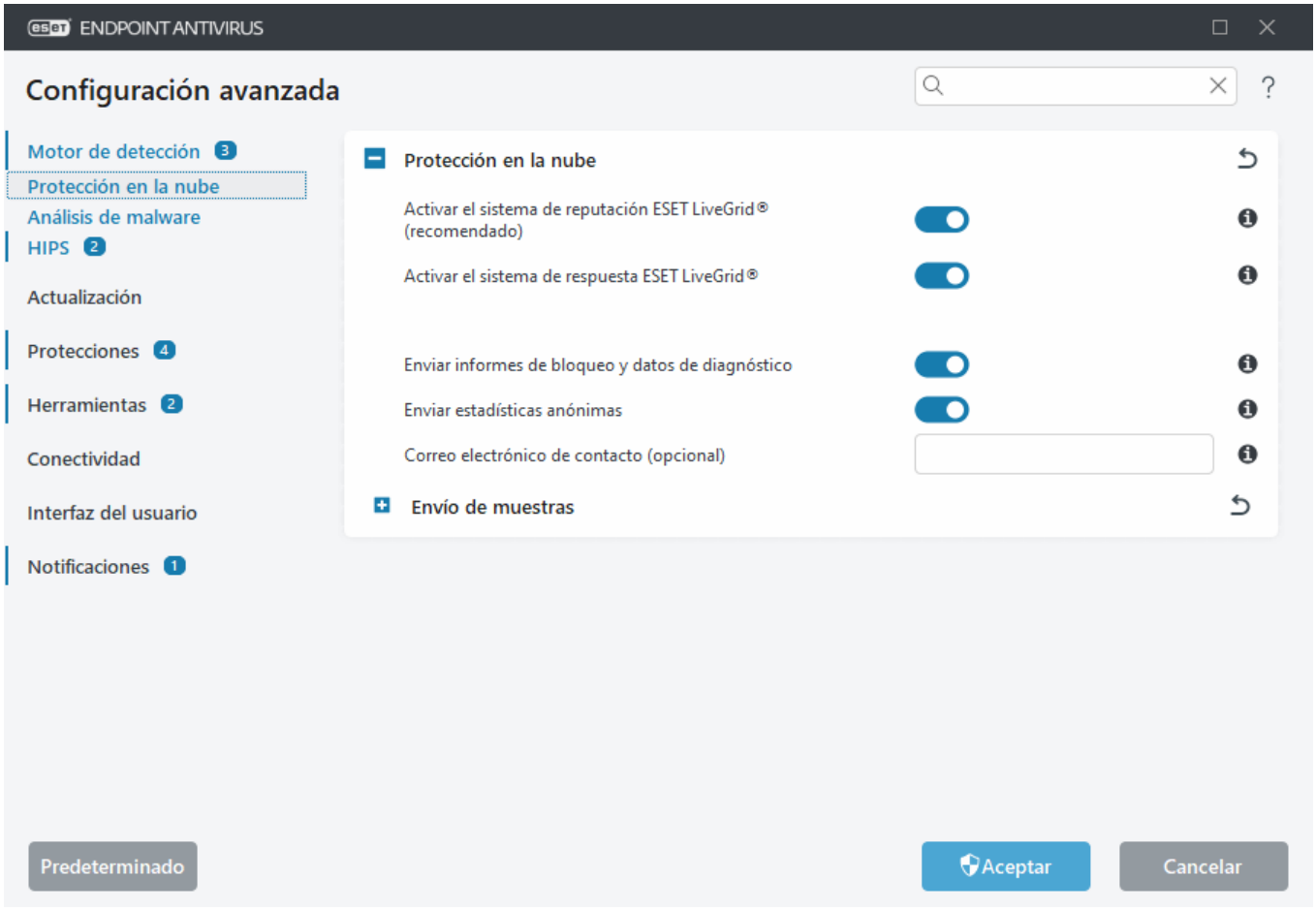
Activar el sistema de respuesta ESET LiveGrid®: envía los datos de envío pertinentes (descritos en la sección **Envío de muestras** a continuación) junto con informes de bloqueo y estadísticas al laboratorio de investigación de ESET para su análisis.

Active ESET LiveGuard (ESET LiveGuard es una funcionalidad adicional comercializada por ESET y no está disponible de forma predeterminada). ESET LiveGuard es un servicio de pago prestado por ESET. Su finalidad es añadir una capa de protección diseñada específicamente para mitigar las amenazas que son nuevas en estado salvaje. Los archivos sospechosos se envían automáticamente a la nube de ESET. En la nube los analizan nuestros motores avanzados de detección de malware. El usuario que proporcionó la muestra recibirá un informe de comportamiento que contiene un resumen del comportamiento de la muestra observada.

Enviar informes de bloqueo y datos de diagnóstico: enviar datos de diagnóstico relacionados con ESET LiveGrid® como informes de bloqueo y volcados de la memoria de los módulos. Se recomienda mantenerlo activado para ayudar a ESET a diagnosticar problemas, mejorar productos y garantizar una mejor protección del usuario final.

Enviar estadísticas anónimas: permita a ESET recopilar información sobre nuevas amenazas detectadas, como el nombre de la amenaza, la fecha y hora en las que se detectó, el método de detección y los metadatos asociados. la versión del producto y la configuración del mismo, incluida información sobre su sistema.

Correo electrónico de contacto (opcional): su correo electrónico de contacto se puede enviar con cualquier archivo sospechoso y puede servir para localizarle si se necesita más información para el análisis. No recibirá una respuesta de ESET, a no ser que sea necesaria más información.



Envío de muestras

Envío manual de muestras: le permite enviar muestras a ESET manualmente desde el menú contextual, la Cuarentena o Herramientas.

Envío automático de muestras detectadas

Seleccione qué tipo de muestras se enviarán a ESET para que las analice y mejore la detección futura. Están disponibles las opciones siguientes:

- **Todas las muestras detectadas**: todos los objetos detectados por el Motor de detección (incluidas aplicaciones potencialmente no deseadas cuando están activadas en los ajustes del análisis).
- **Todas las muestras excepto los documentos**: todos los objetos detectados excepto **Documentos** (consulte más abajo).
- **No enviar**: los objetos detectados no se enviarán a ESET.

Envío automático de muestras sospechosas

Estas muestras también se enviarán a ESET si el motor de detección no las detecta. Por ejemplo, las muestras que casi no se detectaron, o si uno de los ESET Endpoint Antivirus módulos de protección considera que estas muestras son sospechosas o tienen un comportamiento poco claro.

- **Ejecutables**: incluye archivos como .exe, .dll, .sys.
- **Archivos comprimidos**: incluye tipos de archivo como .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Scripts**: incluye tipos de archivo como .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Otros**: incluye tipos de archivo como .jar, .reg, .msi, .sfw, .lnk.

- **Correos electrónicos con posible spam**: esto permitirá el envío de correos electrónicos con posible contenido de spam o correos electrónicos que en su totalidad sean spam con archivos adjuntos a ESET para que los analice. Activar esta opción mejora la detección global de spam, y usted también disfrutará de las futuras mejoras en la detección de spam.
- **Documentos**: incluye documentos de Microsoft Office o PDF con o sin contenido activo.

  Expandir la lista de todos los tipos de archivo de documento incluidos

  ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Exclusiones

Esta opción le permite excluir del envío archivos o carpetas (por ejemplo, puede ser útil para excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo). Los archivos mostrados en la lista nunca se enviarán al laboratorio de ESET para su análisis, aunque contengan código sospechoso. Los tipos de archivos más comunes se excluyen de manera predeterminada (.doc, etc.). Si lo desea, puede añadir elementos a la lista de archivos excluidos.

Para excluir archivos descargados de download.domain.com, vaya a Configuración avanzada > **Protección en la nube** > **Envío de muestras** > **Exclusiones** y agregue la exclusión *download.domain.com*.

Tamaño máximo de las muestras (MB): define el tamaño máximo de las muestras enviadas automáticamente (1-64 MB).

ESET LiveGuard

Para activar el servicio ESET LiveGuard en una máquina cliente con ESET PROTECT Web Console, consulte Configuración de ESET LiveGuard para ESET Endpoint Antivirus.

Si ha utilizado ESET LiveGrid® anteriormente y lo ha desactivado, es posible que aún haya paquetes de datos pendientes de envío. Estos paquetes se enviarán a ESET incluso después de la desactivación. Una vez que se haya enviado toda la información actual, no se crearán más paquetes.

Filtro de exclusión para protección en la nube

El filtro de exclusión le permite excluir del envío de muestras determinados archivos o carpetas. Los archivos mostrados en la lista nunca se enviarán al laboratorio de ESET para su análisis, aunque contengan código sospechoso. Los tipos de archivo más habituales (como .doc, etc.) se excluyen de forma predeterminada.

Esta función resulta útil para, por ejemplo, excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo.

Para excluir archivos descargados de download.domain.com, haga clic en Configuración avanzada > **Motor de detección** > **Protección en la nube** > **Envío de muestras** > **Exclusiones** y agregue la exclusión *download.domain.com*.

Análisis de malware

Se puede acceder a la sección **Análisis de malware** desde Configuración avanzada > **Motor de detección** > **Análisis de malware** y le permite configurar los parámetros de análisis para los perfiles de análisis.

Análisis a petición

Perfil seleccionado: un conjunto específico de parámetros usados por el análisis a petición. Para crear uno nuevo, haga clic en **Modificar** junto a **Lista de perfiles**. Consulte Perfiles de análisis si desea más información.

Después de seleccionar el perfil de escaneo, puede configurar las siguientes opciones:

Objetos de análisis: si solo desea analizar un objeto específico, puede hacer clic en **Editar** junto a **Objetos de análisis** y seleccionar una opción en la estructura de carpetas (árbol). Consulte Objetos de análisis si desea más información.

Respuestas de análisis y detección bajo demanda: puede configurar los niveles de informes y protección para cada perfil de análisis. De forma predeterminada, los perfiles de análisis utilizan la misma configuración definida en la protección del sistema de archivos en tiempo real. Desactive el interruptor junto a **Usar configuración de protección en tiempo real** para configurar niveles de protección e informes personalizados. Consulte Protecciones para obtener una explicación detallada de los niveles de informes y protección.

ThreatSense: opciones de configuración avanzada, como las extensiones de archivo que desea controlar y los métodos de detección utilizados. Consulte ThreatSense para obtener más información.

Perfiles de análisis

Hay 4 perfiles de análisis predefinidos en ESET Endpoint Antivirus:

- **Análisis inteligente** – este es el perfil de análisis avanzado predeterminado. El perfil de análisis inteligente utiliza la tecnología de optimización inteligente, que excluye los archivos que se han comprobado estaban desinfectados en un análisis anterior y no se han modificado desde ese análisis. Esto permite reducir el tiempo de análisis y la repercusión en la seguridad del sistema.
- **Análisis del menú contextual** – puede iniciar un análisis a petición de cualquier archivo desde el menú contextual. El perfil de análisis del menú contextual le permite definir la configuración del análisis que se utilizará cuando active el análisis de esta forma.
- **Análisis exhaustivo** – De forma predeterminada, el perfil de análisis exhaustivo no utiliza la optimización inteligente, por lo que no se excluye ningún archivo del análisis con este perfil.
- **Análisis del ordenador** – este es el perfil predeterminado que se utiliza en el análisis estándar del ordenador.

Puede guardar sus parámetros de análisis preferidos para próximas sesiones de análisis. Le recomendamos que cree un perfil diferente (con varios objetos de análisis, métodos de análisis y otros parámetros) para cada uno de los análisis que realice con frecuencia.

Para crear un perfil nuevo, abra Configuración avanzada > **Motor de detección** > **Análisis de malware** > **Análisis a petición** > **Lista de perfiles** > **Editar**. En la ventana **Administrador de perfiles** encontrará el menú desplegable **Perfil seleccionado** con los perfiles de análisis existentes y la opción para crear uno nuevo. Si necesita ayuda para crear un perfil de análisis que se adecúe a sus necesidades, consulte la sección ThreatSense para ver una

descripción de los diferentes parámetros de la configuración del análisis.

> Supongamos que desea crear su propio perfil de análisis y parte de la configuración de **Análisis del ordenador** es adecuada; sin embargo, no desea analizar los empaquetadores en tiempo real ni las aplicaciones potencialmente peligrosas y, además, quiere aplicar la opción **Reparar la detección siempre**. Introduzca el nombre del nuevo perfil en la ventana **Administrador de perfiles** y haga clic en **Agregar**. Seleccione un perfil nuevo en el menú desplegable **Perfil seleccionado**, ajuste los demás parámetros según sus requisitos y haga clic en **Aceptar** para guardar el nuevo perfil.

Objetos de análisis

En el menú desplegable **Objetos de análisis**, puede seleccionar objetos predefinidos para el análisis.

- **Por configuración de perfil**: selecciona los objetos especificados por el perfil de análisis seleccionado.
- **Medios extraíbles**: selecciona los disquetes, dispositivos de almacenamiento USB, CD y DVD.
- **Unidades locales**: selecciona todas las unidades de disco del sistema.
- **Unidades de red**: selecciona todas las unidades de red asignadas.
- **Selección personalizada**: cancela todas las selecciones anteriores.

La estructura (de árbol) de carpetas también contiene objetos de análisis específicos.

- **Memoria operativa**: analiza todos los procesos y datos que actualmente utiliza la memoria operativa.
- **Sectores de inicio/UEFI**: analiza los sectores de inicio y la UEFI en busca de malware. Puede obtener más información sobre el análisis UEFI en el glosario.
- **Base de datos de WMI**: analiza toda la base de datos de Windows Management Instrumentation (WMI), todos los espacios de nombres, todas las instancias de clase y todas las propiedades. Busca referencias a archivos infectados o malware incrustados como datos.
- **Registro del sistema**: analiza todo el registro del sistema, todas las claves y todas las subclaves. Busca referencias a archivos infectados o malware incrustados como datos. Durante la desinfección de las detecciones, la referencia permanece en el registro para garantizar que no se pierda ningún dato importante.

Para ir rápidamente a un objeto de análisis (archivo o carpeta), escriba su ruta en el campo de texto que aparece debajo de la estructura de árbol. La ruta distingue entre mayúsculas y minúsculas. Para incluir el objeto en el análisis, marque su casilla de verificación en la estructura de árbol.

Análisis en estado inactivo

Puede activar el análisis en estado inactivo en Configuración avanzada > **Motor de detección** > **Análisis de malware** > **Análisis en estado inactivo**.

Análisis en estado inactivo

Active el interruptor situado junto a **Activar el análisis de estado inactivo** para activar esta función. Cuando el ordenador se encuentra en estado inactivo, se lleva a cabo un análisis silencioso del ordenador en todas las unidades locales.

De forma predeterminada, el análisis en estado inactivo no se ejecutará si el ordenador (portátil) funciona con

batería. Para anular este ajuste, active el interruptor situado junto a **Ejecutar aunque el ordenador esté funcionando con la batería** en Configuración avanzada.

Active el interruptor situado junto a **Activar el registro de sucesos** de la configuración avanzada para guardar un informe del análisis del ordenador en la sección Archivos de registro (en la ventana principal del programa, haga clic en **Herramientas** > **Archivos de registro** y seleccione **Análisis del ordenador** en el menú desplegable **Registro**).

Detección de estado inactivo

Consulte Activadores de la detección del estado inactivo para ver una lista completa de condiciones que se deben cumplir para activar el análisis de estado inactivo.

ThreatSense: opciones de configuración avanzada, como las extensiones de archivo que desea controlar y los métodos de detección utilizados. Consulte ThreatSense para obtener más información.

Detección de estado inactivo

Los ajustes de detección de estado inactivo se pueden configurar en Configuración avanzada > **Motor de detección** > **Análisis de malware** > **Análisis de estado inactivo** > **Detección de estado inactivo**. Estos ajustes especifican un activador para el Análisis de estado inactivo:

- **Pantalla apagada o con protector de pantalla**
- **Bloqueo del ordenador**
- **Cierre de sesión de usuario**

Utilice el interruptor de cada estado para activar o desactivar los distintos activadores de la detección del estado inactivo.

Análisis en el inicio

De forma predeterminada, la comprobación automática de los archivos en el inicio se realizará al iniciar el sistema o durante actualizaciones del motor de detección. Este análisis depende de las tareas y la configuración de Tareas programadas.

Las opciones de análisis en el inicio forman parte de la tarea **Verificación de archivos en el inicio del sistema** del Planificador de tareas. Para modificar su configuración, desplácese hasta **Herramientas** > **Tareas programadas**, haga clic en **Verificación de la ejecución de archivos en el inicio** y, a continuación, haga clic en **Modificar**. En el último paso, aparece la ventana Verificación de la ejecución de archivos en el inicio. Para obtener instrucciones detalladas acerca de la creación y gestión de tareas del Planificador de tareas, consulte Creación de tareas nuevas.

ThreatSense: opciones de configuración avanzada, como las extensiones de archivo que desea controlar y los métodos de detección utilizados. Consulte ThreatSense para obtener más información.

Comprobación de la ejecución de archivos en el inicio

Al crear una tarea programada de comprobación de archivos en el inicio del sistema, tiene varias opciones para ajustar los siguientes parámetros:

El menú desplegable **Analizar destinos** especifica la profundidad de análisis de los archivos ejecutados al iniciar el sistema basado en un sofisticado algoritmo. Los archivos se organizan en orden descendente de acuerdo con los siguientes criterios:

- **Todos los archivos registrados** (se analiza el mayor número de archivos)
- **Archivos usados pocas veces**
- **Archivos usados ocasionalmente**
- **Archivos usados frecuentemente**
- **Solo los archivos usados con más frecuencia** (se analiza el menor número de archivos)

También se incluyen dos grupos específicos:

- **Archivos ejecutados antes del inicio de sesión del usuario**: contiene archivos de ubicaciones a las que se puede tener acceso sin que el usuario haya iniciado sesión (incluye casi todas las ubicaciones de inicio como servicios, objetos auxiliares del navegador, notificación del registro de Windows, entradas del Planificador de tareas de Windows, archivos dll conocidos, etc.).
- **Archivos en ejecución después del registro del usuario**: contiene archivos de ubicaciones a las que solo se puede tener acceso cuando el usuario se ha registrado (incluye archivos que solo ejecuta un usuario específico, generalmente los archivos de *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Las listas de los archivos que se analizan son fijas para cada grupo de los anteriores. Si elige una profundidad de análisis inferior para los archivos ejecutados al iniciar el sistema, los archivos no analizados se analizarán cuando se abran o se ejecuten.

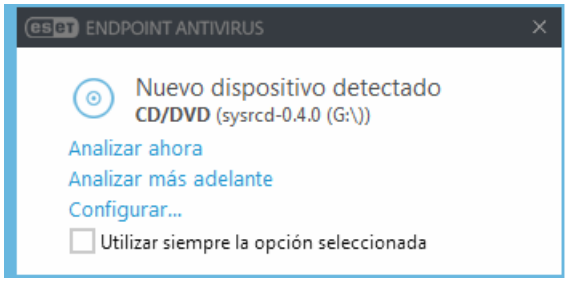
Prioridad de análisis: el nivel de prioridad empleado para determinar cuándo se iniciará un análisis:

- **Cuando el procesador esté desocupado**: la tarea se ejecutará solo cuando el sistema esté inactivo.
- **Muy baja**: cuando la carga del sistema es la más baja posible.
- **Baja**: con poca carga del sistema.
- **Normal**: con carga media del sistema.

Unidades extraíbles

ESET Endpoint Antivirus permite analizar los medios extraíbles (CD, DVD, USB, etc.) de forma automática cuando se insertan en un ordenador. Esto puede ser útil cuando el administrador del ordenador quiere impedir que los usuarios utilicen medios extraíbles con contenido no solicitado.

Cuando se inserta un medio extraíble y se establece **Mostrar las opciones de análisis** en Configuración avanzada > **Motor de detección** > **Análisis de malware** > **Medios extraíbles**, aparece la siguiente ventana:



Opciones de este cuadro de diálogo:

- **Analizar ahora**: activa el análisis del medio extraíble.
- **No analizar**: no se analizarán los medios extraíbles.
- **Configuración**: abre la configuración avanzada.
- **Utilizar siempre la opción seleccionada**: cuando se seleccione esta opción, se realizará la misma acción la próxima vez que se introduzca un medio extraíble.

Además, ESET Endpoint Antivirus presenta funciones de control de dispositivos, lo que le permite definir reglas para el uso de dispositivos externos en un ordenador dado. Encontrará más detalles sobre el control de dispositivos en la sección Control de dispositivos.

Para acceder a los ajustes para el análisis de medios extraíbles, abra Configuración avanzada > **Motor de detección** > **Análisis de malware** > **Medios extraíbles**.

Acción que debe efectuarse cuando se inserten medios extraíbles: seleccione la acción predeterminada que se realizará cuando se inserte un medio extraíble en el ordenador (CD, DVD o USB). Elija la acción deseada al insertar un medio extraíble en un ordenador:

- **No analizar**: no se realizará ninguna acción y no se abrirá la ventana **Nuevo dispositivo detectado**.
- **Análisis automático del dispositivo**: se realizará un análisis del ordenador del medio extraíble insertado.
- **Análisis forzado del dispositivo**: se realizará un análisis del ordenador del medio extraíble insertado, que no se puede cancelar.
- **Mostrar las opciones de análisis**: abre la sección de configuración de **medios extraíbles**.

Protección de documentos

La característica de protección de documentos analiza los documentos de Microsoft Office antes de que se abran y los archivos descargados automáticamente con Internet Explorer como, por ejemplo, elementos de Microsoft ActiveX. La protección de documentos proporciona un nivel de protección adicional a la protección en tiempo real del sistema de archivos, y se puede desactivar para mejorar el rendimiento en sistemas que no gestionan a un volumen elevado de documentos de Microsoft Office.

Para activar Protección de documentos, abra Configuración avanzada > **Motor de detección** > **Análisis de malware** > **Protección de documentos** y haga clic en la barra deslizante situada junto a **Activar la protección de documentos**.

ThreatSense: opciones de configuración avanzada, como las extensiones de archivo que desea controlar y los métodos de detección utilizados. Consulte ThreatSense para obtener más información.

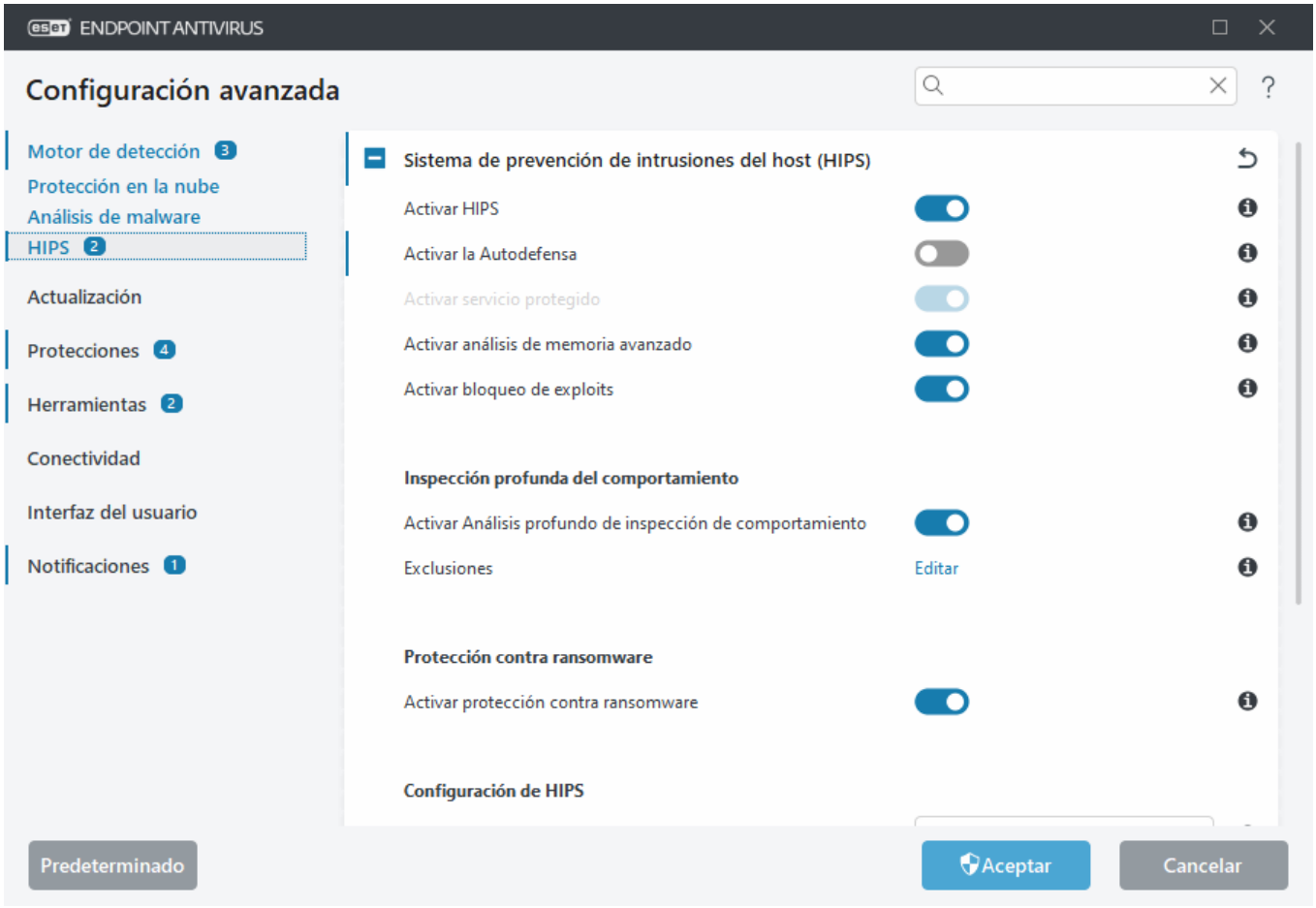
Esta función se activa mediante aplicaciones que utilizan Microsoft Antivirus API (por ejemplo, Microsoft Office 2000 y posteriores o Microsoft Internet Explorer 5.0 y posteriores).

HIPS: Sistema de prevención de intrusiones del host)

Solo debe modificar la configuración de HIPS si es un usuario experimentado. Una configuración incorrecta de los parámetros de HIPS puede provocar inestabilidad en el sistema.

El Sistema de prevención de intrusiones del host (HIPS) protege el sistema frente a código malicioso o cualquier actividad no deseada que intente menoscabar la seguridad del ordenador. Este sistema combina el análisis avanzado del comportamiento con funciones de detección del filtro de red para controlar los procesos, archivos y claves de registro. HIPS es diferente de la protección del sistema de archivos en tiempo real y no es un cortafuegos; solo supervisa los procesos que se ejecutan dentro del sistema operativo.

Puede configurar los ajustes del HIPS en Configuración avanzada > **Motor de detección** > **HIPS** > **Sistema de prevención de intrusiones del host**. El estado de HIPS (activado/desactivado) se muestra en la ventana principal de ESET Endpoint Antivirus, dentro de **Configuración** > **Ordenador**.



Sistema de prevención de intrusiones basado en el host

Activar HIPS: HIPS está activado de forma predeterminada en ESET Endpoint Antivirus. Si desactiva HIPS, se desactivarán las demás características de HIPS, como Bloqueador de exploits.

Activar la Autodefensa: ESET Endpoint Antivirus utiliza la tecnología de **Autodefensa** integrada como parte del HIPS para impedir que software malicioso dañe o desactive su protección antivirus y antiespía. La autodefensa

evita la manipulación de procesos, claves de registro y archivos cruciales del sistema y de ESET. ESET Management Agent también se protege cuando se instala.

Activar servicio protegido: activa la protección para ESET Service (ekrn.exe). Cuando está activado, el servicio se inicia como un proceso de Windows protegido para defenderle de ataques de malware. Esta opción está disponible en Windows 8.1 y Windows 10.

Activar análisis de memoria avanzado: funciona en combinación con Bloqueador de exploits para reforzar la protección contra malware diseñado para evitar su detección mediante productos antimalware gracias al uso de ofuscación o cifrado. El análisis avanzado de memoria está activado de forma predeterminada. Puede obtener más información sobre este tipo de protección en el glosario.

Activar bloqueo de exploits: se ha diseñado para fortalecer los tipos de aplicaciones que sufren más ataques, como navegadores, lectores de PDF, clientes de correo electrónico y componentes de MS Office. El bloqueador de exploits está activado de forma predeterminada. Puede obtener más información sobre este tipo de protección en el glosario.

Análisis profundo de inspección de comportamiento

Habilitar Análisis profundo de inspección de comportamiento: es otra capa de protección que funciona como parte de la función HIPS. Esta extensión del HIPS analiza el comportamiento de todos los programas que se ejecutan en el ordenador y le advierte si el comportamiento del proceso es malicioso.

Las Exclusiones del HIPS del Análisis profundo de inspección de comportamiento le permiten excluir procesos del análisis. Para garantizar que se analicen todos los procesos en busca de posibles amenazas, le recomendamos que solo cree exclusiones cuando sea absolutamente necesario.

Protección contra ransomware

Activar protección contra ransomware: es otra capa de protección que funciona como parte de la característica HIPS. Para que la protección contra ransomware funcione, debe tener activado el sistema de reputación ESET LiveGrid®. Más información sobre este tipo de protección.

Activar Intel® Threat Detection Technology: ayuda a detectar ataques de ransomware mediante la telemetría de la CPU Intel exclusiva para aumentar la eficacia de detección, reducir las alertas de falsos positivos y ampliar la visibilidad para capturar técnicas de evasión avanzadas. Consulte los procesadores compatibles.

Activar modo de auditoría: todo lo que detecta la protección contra ransomware no se bloquea automáticamente, sino que se registra con una advertencia de severidad y se envía a la consola de administración con el indicador "MODO DE AUDITORÍA". El administrador puede decidir excluir dicha detección para evitar una posterior detección, o mantenerla activa, lo que significa que una vez que finalice el modo de auditoría, esta se bloqueará o eliminará. La activación o desactivación del modo de auditoría también se registrará en ESET Endpoint Antivirus. Esta opción está disponible solo en el editor de configuración de políticas de ESET PROTECT.

Configuración de HIPS

El **Modo de filtrado** se puede realizar en uno de los siguientes modos:

Modo de filtrado	Descripción
Modo automático	Las operaciones están activadas, con la excepción de aquellas bloqueadas mediante reglas predefinidas que protegen el sistema.

Modo de filtrado	Descripción
Modo inteligente	Solo se informará al usuario de los sucesos muy sospechosos.
Modo interactivo	El usuario debe confirmar las operaciones.
Modo basado en reglas	Bloquea todas las operaciones no definidas por una regla específica que las permita.
Modo de aprendizaje	Las operaciones están activadas y se crea una regla después de cada operación. Las reglas creadas en este modo se pueden ver en el Editor de **reglas del HIPS**, pero su prioridad es inferior a la de las reglas creadas manualmente o en el modo automático. Si selecciona el **Modo de aprendizaje** en el menú desplegable **Modo de filtrado**, el ajuste **El modo de aprendizaje finalizará a las** estará disponible. Seleccione el periodo de tiempo durante el que desea activar el modo de aprendizaje; la duración máxima es de 14 días. Cuando transcurra la duración especificada se le pedirá que modifique las reglas creadas por el HIPS mientras estaba en modo de aprendizaje. También puede elegir un modo de filtrado distinto o posponer la decisión y seguir usando el modo de aprendizaje.

Modo establecido tras conocer la caducidad del modo: seleccione el modo de filtrado que se utilizará cuando caduque el modo de aprendizaje. Tras el vencimiento, la opción **Preguntar al usuario** requiere privilegios administrativos para realizar un cambio en el modo de filtrado de HIPS.

El sistema HIPS supervisa los sucesos del sistema operativo y reacciona en consecuencia basándose en reglas similares a las que utiliza el cortafuegos. Haga clic en **Editar** junto a **Reglas** para abrir el editor de **reglas de HIPS**. En la ventana de reglas de HIPS puede seleccionar, agregar, editar o quitar reglas. Puede obtener más información sobre la creación de reglas y las operaciones de HIPS en Editar una regla de HIPS.

Exclusiones del HIPS

Las exclusiones le permiten excluir procesos del Análisis profundo de inspección de comportamiento que ofrece el HIPS.

Para editar exclusiones de HIPS, abra Configuración avanzada > **Motor de detección** > **HIPS** > **Sistema de prevención de intrusiones del host (HIPS) Exclusiones** > **Editar**.

> No se debe confundir con Extensiones de archivo excluidas, Exclusiones de detección, Exclusiones de rendimiento ni Exclusiones de procesos.

Para excluir un objeto, haga clic en **Agregar** e introduzca la ruta de acceso de un objeto o selecciónelo en la estructura de árbol. También puede Editar o Eliminar las entradas seleccionadas.

Configuración avanzada de HIPS

Las opciones siguientes son útiles para depurar y analizar el comportamiento de una aplicación:

Controladores con carga siempre autorizada: los controladores seleccionados pueden cargarse siempre sea cual sea el modo de filtrado configurado, a menos que la regla del usuario los bloquee de forma explícita.

Registrar todas las operaciones bloqueadas: las operaciones bloqueadas se escribirán en el registro de HIPS. Utilice esta función solo para resolver problemas o cuando el equipo de soporte técnico de ESET lo solicite, ya que puede generar un archivo de registro muy grande y ralentizar su ordenador.

Notificar cuando se produzcan cambios en las aplicaciones de inicio: muestra una notificación en el escritorio cada vez que se agrega o se elimina una aplicación del inicio del sistema.

Controladores con carga siempre autorizada

Los controladores que aparezcan en esta lista podrán cargarse siempre, sea cual sea el modo de filtrado de HIPS, a menos que una regla del usuario los bloquee de forma específica.

Agregar: agrega un nuevo controlador.

Modificar: modifica el controlador seleccionado.

Quitar: quita un controlador de la lista.

Restablecer: carga de nuevo una serie de controladores del sistema.

Haga clic en **Restablecer** si no desea incluir los controladores que ha agregado manualmente. Esto puede resultar útil si ha agregado varios controladores y no puede eliminarlos de la lista manualmente.

Tras la instalación, la lista de controladores está vacía. ESET Endpoint Antivirus rellena la lista automáticamente a medida que pasa el tiempo.

Los controladores con carga siempre autorizada son específicos de cada dispositivo y no se pueden editar con la política de ESET PROTECT. Tras la instalación, la lista de controladores está vacía. ESET Endpoint Antivirus rellena la lista automáticamente a medida que pasa el tiempo.

Ventana interactiva de HIPS

La ventana de notificación de HIPS le permite crear una regla basada en nuevas acciones que detecta HIPS y, a continuación, definir las condiciones en las que se permitirá o bloqueará esa acción.

Las reglas creadas en la ventana de notificación se consideran equivalentes a las reglas creadas manualmente. Una regla creada en una ventana de notificación puede ser menos específica que la regla que desencadenó esa ventana de diálogo. Esto significa que, después de crear una regla en el cuadro de diálogo, la misma operación puede desencadenar la misma ventana. Si desea obtener más información, consulte Prioridad de las reglas de HIPS.

Si la acción predeterminada para una regla es **Preguntar siempre**, se mostrará una ventana de diálogo cada vez que se desencadene la regla. Puede seleccionar **Bloquear** o **Permitir** la operación. Si no selecciona una acción en el tiempo indicado, se seleccionará una nueva acción basada en las reglas.

Recordar hasta el cierre de la aplicación provoca que se use la acción (**Permitir/Bloquear**) hasta que se cambien las reglas o el modo de filtrado, se actualice el módulo HIPS o se reinicie el sistema. Después de cualquiera de estas tres acciones, las reglas temporales se eliminarán.

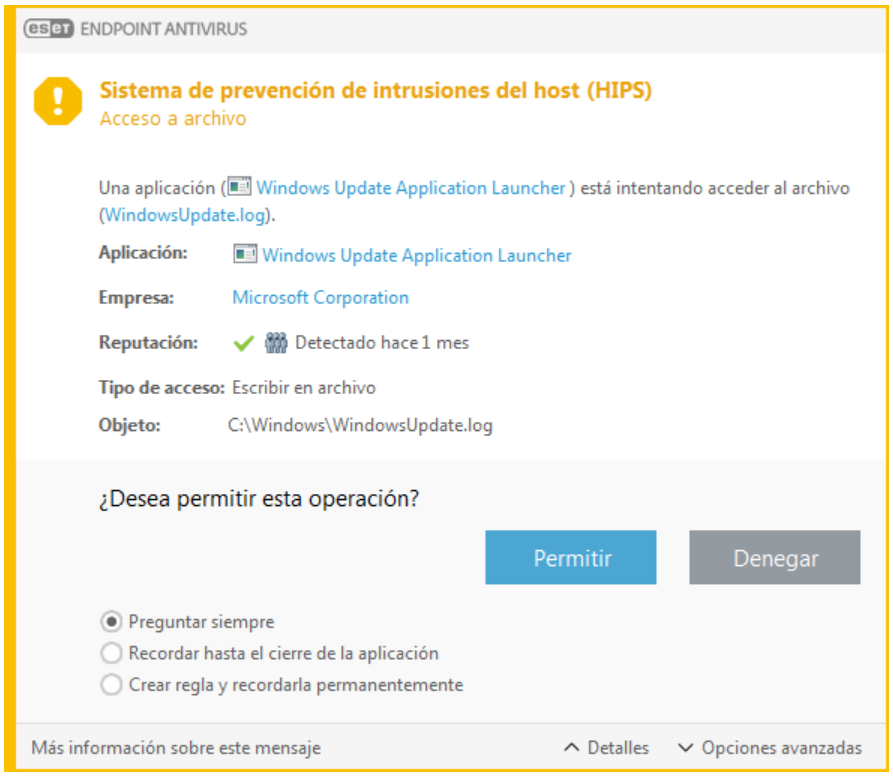
La opción **Crear regla y recordar permanentemente** creará una nueva regla de HIPS que podrá modificarse más tarde en la sección Gestión de reglas de HIPS (requiere privilegios de administración).

Haga clic en **Detalles** en la parte inferior para ver qué aplicación desencadena la operación, la reputación del archivo o el tipo de operación que debe permitir o bloquear.

Para acceder a los ajustes de los parámetros más detallados de la regla, haga clic en **Opciones avanzadas**. Las siguientes opciones están disponibles si selecciona **Crear regla y recordar permanentemente**:

- **Crear una regla válida solo para esta aplicación**: si desactiva esta casilla de verificación, la regla se creará para todas las aplicaciones de origen.
- **Solo para la operación**: seleccione las operaciones de archivo/aplicación/registro de la regla. Consulte las descripciones de todas las operaciones de HIPS.
- **Solo para el destino**: seleccione los destinos de archivo/aplicación/registro de la regla.

Para que dejen de aparecer las notificaciones, cambie el modo de filtrado a **Modo automático** en Configuración avanzada > **Motor de detección** > **HIPS** > **Básico**.



Se ha detectado un comportamiento potencial de ransomware

Esta ventana interactiva aparecerá cuando se detecte un comportamiento potencial de ransomware. Puede seleccionar **Bloquear** o **Permitir** la operación.

Haga clic en **Detalles** para ver parámetros de detección concretos. La ventana de diálogo le permite **Enviar para su análisis** o **Excluir de la detección**.

Para que la protección contra ransomware funcione correctamente, ESET LiveGrid® debe estar activado.

Gestión de reglas de HIPS

Esta es una lista de reglas del sistema HIPS agregadas automáticamente y definidas por el usuario. Encontrará más detalles sobre la creación de reglas y las operaciones de HIPS en el capítulo Configuración de reglas de HIPS. Consulte también Principio general de HIPS.

Columnas

Regla: nombre de la regla definido por el usuario o seleccionado automáticamente.

Activado: desactive esta opción si desea conservar la regla en la lista, pero no desea utilizarla.

Acción: la regla especifica una acción (**Permitir**, **Bloquear** o **Preguntar**) que debe realizarse cuando se cumplen las condiciones.

Orígenes: la regla solo se utilizará si una aplicación activa el suceso.

Objetos: la regla solo se usará si la operación está relacionada con un archivo, una aplicación o una entrada del registro específicos.

Registro de severidad: si activa esta opción, la información acerca de esta regla se anotará en el registro de HIPS.

Notificar: cuando se desencadena un suceso, aparece una notificación en la esquina inferior derecha.

Elementos de control

Agregar: crea una nueva regla.

Modificar: le permite modificar las entradas seleccionadas.

Eliminar: quita las entradas seleccionadas.

Prioridad de las reglas de HIPS

No hay opciones para ajustar el nivel de prioridad de las reglas de HIPS con los botones arriba/abajo.

- Todas las reglas que cree tendrán la misma prioridad
- Cuanto más específica sea la regla, mayor será su prioridad (por ejemplo, la regla para una aplicación específica tiene más prioridad que la regla para todas las aplicaciones)
- Internamente, HIPS contiene reglas de mayor prioridad a las que usted no puede acceder (por ejemplo, no puede anular las reglas de Autodefensa definidas)
- Si crea una regla que podría bloquear su sistema operativo, dicha regla no se aplicará (tendrá la prioridad más baja)

Configuración de regla de HIPS

En primer lugar, consulte Gestión de reglas de HIPS.

Nombre de la regla: nombre de la regla definido por el usuario o seleccionado automáticamente.

Acción: especifica la acción (**Permitir**, **Bloquear** o **Preguntar**) que debe realizarse si se cumplen las condiciones.

Operaciones afectadas: debe seleccionar el tipo de operación a la que se aplicará la regla. La regla solo se utilizará para este tipo de operación y para el destino seleccionado.

Activado: desactive esta barra deslizante si desea conservar la regla en la lista pero no aplicarla.

Registro de severidad: si activa esta opción, la información acerca de esta regla se anotará en el registro de HIPS.

Notificar al usuario: cuando se desencadena un suceso, aparece una notificación en la esquina inferior derecha.

La regla consta de partes que describen las condiciones que activan esta regla:

Aplicaciones de origen: la regla solo se utilizará si esta aplicación activa el suceso. Seleccione **Aplicaciones específicas** en el menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas, o puede seleccionar **Todas las aplicaciones** en el menú desplegable para agregar todas las aplicaciones.

Archivos de destino: la regla solo se utilizará si la operación está relacionada con este destino. Seleccione **Archivos específicos** en el menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas, o puede seleccionar **Todos los archivos** en el menú desplegable para agregar todas los archivos.

Aplicaciones: la regla solo se utilizará si la operación está relacionada con este destino. Seleccione **Aplicaciones específicas** en el menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas, o puede seleccionar **Todas las aplicaciones** en el menú desplegable para agregar todas las aplicaciones.

Entradas del registro: la regla solo se utilizará si la operación está relacionada con este destino. Seleccione **Entradas específicas** en el menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas, o puede seleccionar **Todas las entradas** en el menú desplegable para agregar todas las aplicaciones.

> Algunas operaciones de reglas específicas predefinidas por HIPS no se pueden bloquear y se admiten de forma predeterminada. Además, HIPS no supervisa todas las operaciones del sistema. Sino que supervisa las operaciones que considera peligrosas.

> Cuando se especifica una ruta de acceso, C:\example afecta a las acciones con la propia carpeta y C:\example*.* afecta a los archivos de la carpeta.

Operaciones de la aplicación

- **Depurar otra aplicación**: conexión de un depurador al proceso. Durante el proceso de depuración de una aplicación es posible ver y modificar muchos aspectos de su comportamiento, así como acceder a sus datos.
- **Interceptar sucesos de otra aplicación**: la aplicación de origen está intentando capturar sucesos dirigidos a una aplicación concreta (por ejemplo un registrador de pulsaciones que intenta capturar sucesos del navegador).
- **Terminar/suspender otra aplicación**: suspende, reanuda o termina un proceso (se puede acceder a esta operación directamente desde el Process Explorer o el panel Procesos).
- **Iniciar una aplicación nueva**: inicia aplicaciones o procesos nuevos.
- **Modificar el estado de otra aplicación**: la aplicación de origen está intentando escribir en la memoria de la aplicación de destino o ejecutar código en su nombre. Esta función puede ser de utilidad para proteger una aplicación fundamental mediante su configuración como aplicación de destino en una regla que bloquee el uso de esta operación.

Operaciones del registro

- **Modificar la configuración del inicio**: cambios realizados en la configuración que definan las aplicaciones que se ejecutarán al iniciar Windows. Estos cambios se pueden buscar, por ejemplo, buscando la clave Run en el Registro de Windows.
- **Eliminar del registro**: elimina una clave del registro o su valor.
- **Cambiar el nombre de la clave del registro**: cambia el nombre de las claves del registro.
- **Modificar el registro**: crea valores nuevos para las claves del registro, modifica los valores existentes, mueve los datos en el árbol de la base de datos o configura los permisos de usuarios y grupos en las claves del registro.

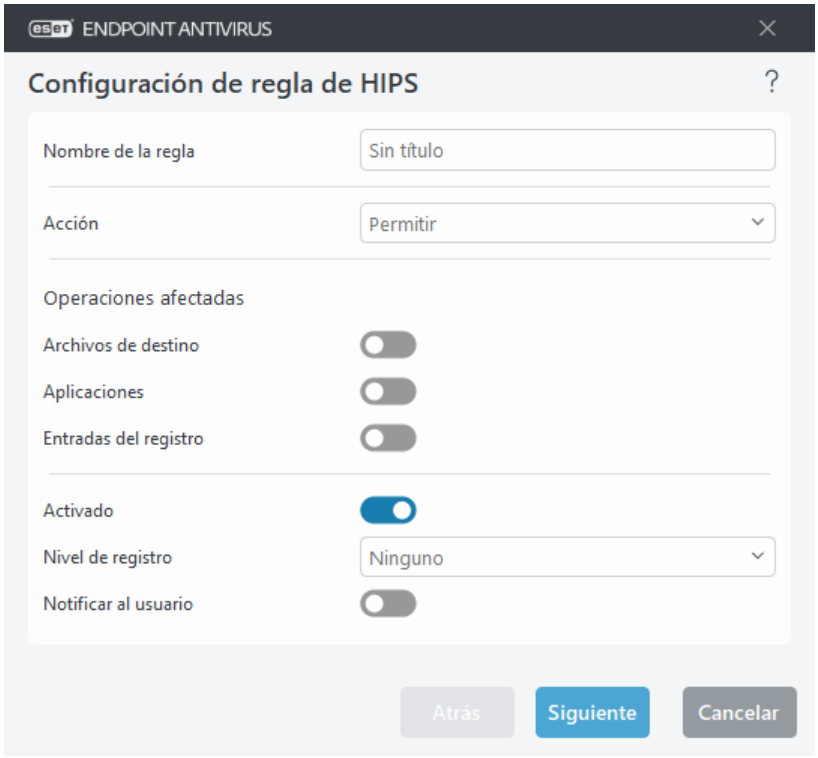
Uso de comodines en las reglas
En el caso de las reglas, el asterisco solo puede utilizarse para sustituir una clave específica, como por ejemplo "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start". El resto de uso de comodines no son compatibles.

Creación de reglas para la clave HKEY_CURRENT_USER
Esta clave no es más que un vínculo a la subclave de HKEY_USERS, que es específica para el usuario identificado por el SID (identificador seguro). Para crear una regla únicamente para el usuario actual, en lugar de utilizar una ruta de acceso a HKEY_CURRENT_USER, utilice una ruta de acceso que le dirija a HKEY_USERS\%SID%. Puede utilizar un asterisco en lugar de SID para aplicar la regla a todos los usuarios.

Si crea una regla muy genérica, se mostrará una advertencia sobre este tipo de regla.

En el siguiente ejemplo, mostraremos cómo restringir comportamientos no deseados de una aplicación específica:

1. Asigne un nombre a la regla y seleccione **Bloquear** (o **Preguntar** si prefiere decidir más tarde) en el menú desplegable **Acción**.
2. Active el conmutador **Advertir al usuario** para mostrar una notificación siempre que se aplique una regla.
3. Seleccione al menos una operación en la sección **Operaciones afectadas** a la que se le aplicará la regla.
4. Haga clic en **Siguiente**.
5. En la ventana **Aplicaciones de origen**, seleccione **Aplicaciones específicas** en el menú desplegable para aplicar la nueva regla a todas las aplicaciones que intenten realizar cualquiera de las operaciones de aplicación seleccionadas en las aplicaciones especificadas.
6. Haga clic en **Agregar** y, a continuación, en **…** para elegir una ruta de acceso de una aplicación específica y, a continuación, pulse **Aceptar**. Agregue más aplicaciones si lo prefiere.
   Por ejemplo: *C:\Program Files (x86)\Untrusted application\application.exe*
7. Seleccione la operación **Escribir en archivo**.
8. Seleccione **Todos los archivos** en el menú desplegable. Cuando una aplicación seleccionada en el paso anterior intente escribir en un archivo, se bloqueará dicho intento.
9. Haga clic en **Finalizar** para guardar la nueva regla.



Agregar ruta de acceso de aplicación/registro para el HIPS

Haga clic en la opción **...** para seleccionar la ruta de acceso a la aplicación de un archivo. Si selecciona una carpeta, se incluirán todas las aplicaciones que se encuentren en esa ubicación.

La opción **Abrir editor del registro** iniciar el editor del registro de Windows (regedit). Si añade la ruta de acceso de un registro, introduzca la ubicación correcta en el campo **Valor**.

Ejemplos de ruta de acceso a un archivo o registro:

- *C:\Archivos de programa\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

Actualización

Las opciones de configuración de la actualización están disponibles en Configuración avanzada > **Actualización**. En esta sección se especifica la información del origen de la actualización, como los servidores de actualización utilizados y sus datos de autenticación.

Para que las actualizaciones se descarguen correctamente, es esencial cumplimentar correctamente todos los parámetros de actualización. Si utiliza un cortafuegos, asegúrese de que su programa de ESET goza de permiso para comunicarse con Internet (por ejemplo, comunicación HTTPS).

Actualización

El perfil de actualización que se está utilizando se muestra en el menú desplegable **Seleccionar perfil de**

actualización predeterminado.

Para crear un nuevo perfil, consulte la sección Perfiles de actualización.

Configurar notificaciones de actualización: haga clic en Modificar para seleccionar las notificaciones de aplicaciones que se muestran. Puede elegir para las notificaciones las opciones Mostrar en el escritorio o Enviar por correo electrónico.

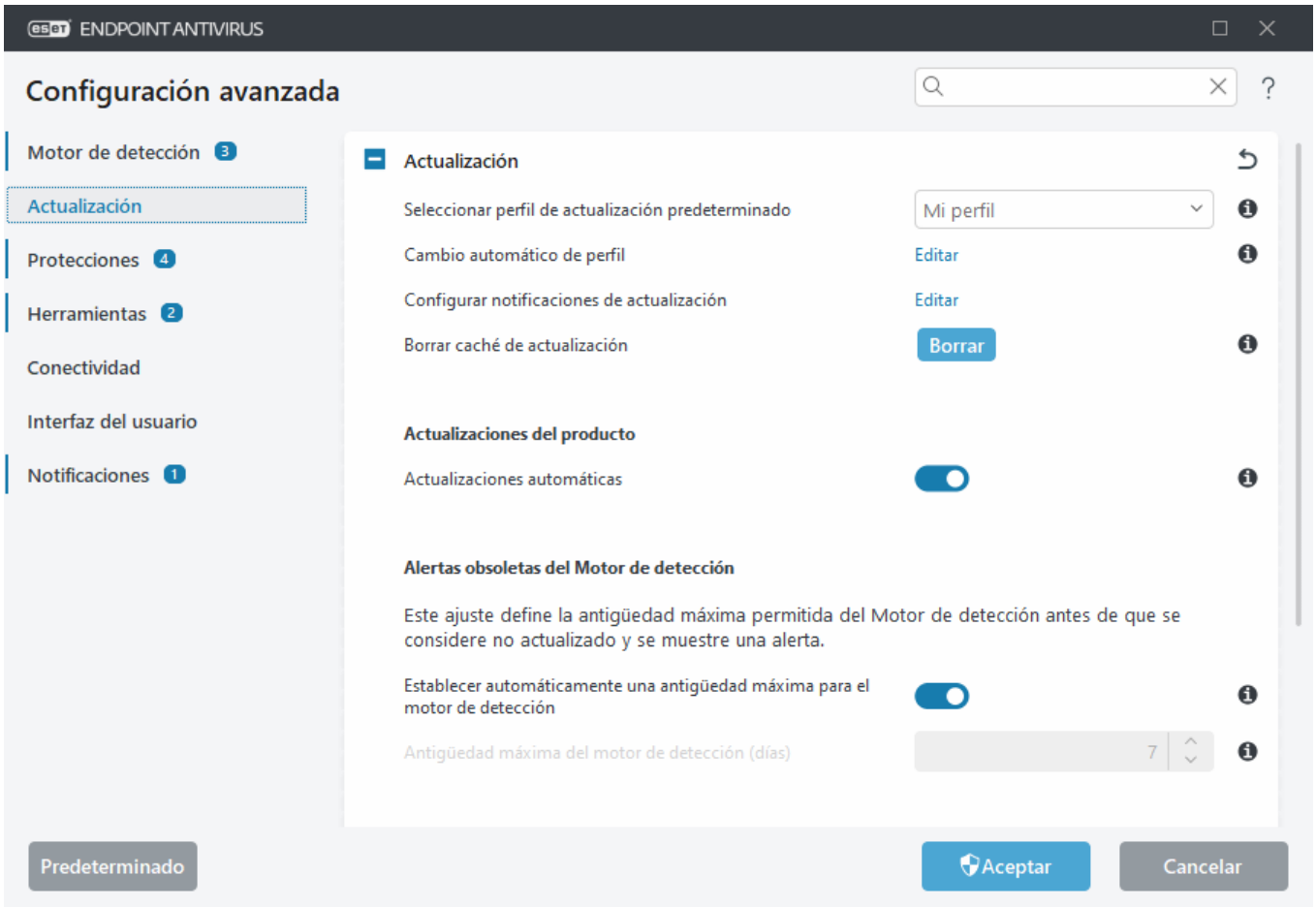
Si tiene problemas al descargar actualizaciones de los módulos, haga clic en **Borrar** junto a **Borrar caché de actualización** para borrar la memoria caché/los archivos de actualización temporales.

Alertas del motor de detección obsoletas

Establecer automáticamente una antigüedad máxima para el motor de detección: permite establecer el tiempo máximo (en días) tras el que el motor de detección se considerará desactualizado. El valor predeterminado de **Antigüedad máxima para el motor de detección (días)** es 7.

Reversión del módulo

Si sospecha que una nueva actualización del motor de detección o de los módulos del programa puede ser inestable o estar dañada, puede revertir a la versión anterior y desactivar las actualizaciones durante un periodo de tiempo definido.



Perfiles

Se pueden crear perfiles de actualización para diferentes tareas y configuraciones de actualización. Estos perfiles son especialmente útiles para los usuarios móviles, que necesitan un perfil alternativo para las propiedades de conexión a Internet que cambian periódicamente.

El menú desplegable **Seleccione el perfil que desea modificar** muestra el perfil seleccionado actualmente y está configurado como **Mi perfil** de forma predeterminada.

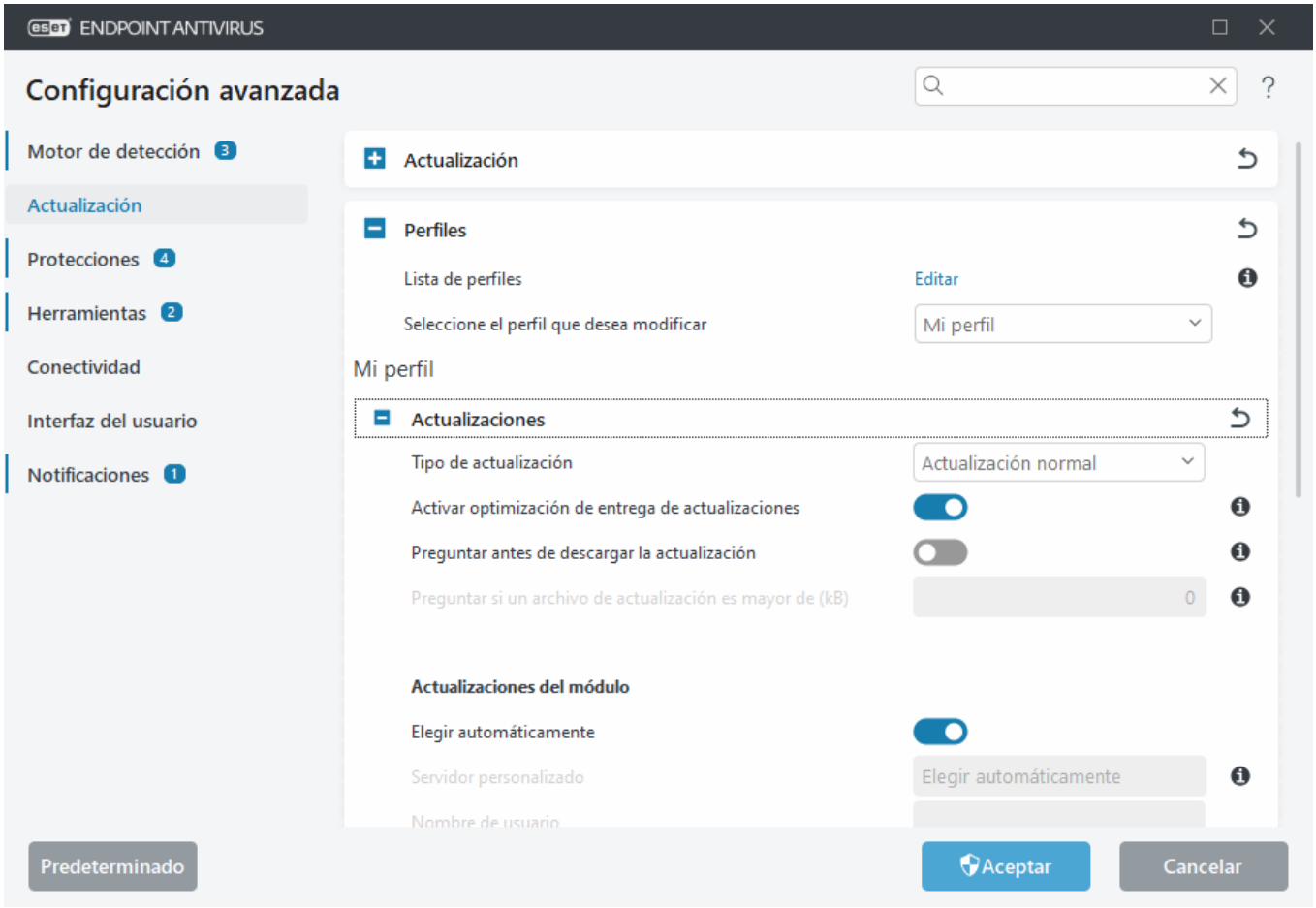
Para crear un perfil nuevo, haga clic en **Editar** junto a **Lista de perfiles**, introduzca su **Nombre de perfil** y, a continuación, haga clic en **Agregar**.

Actualizaciones

De forma predeterminada, el menú **Tipo de actualización** está definido en **Actualización normal** para garantizar que todos los archivos de actualización se descarguen automáticamente del servidor de ESET cuando la carga de red sea menor. Las actualizaciones de prueba (opción **Actualización de prueba**) son actualizaciones que han superado rigurosas pruebas internas y estarán pronto disponibles. Puede beneficiarse de activar las actualizaciones de prueba mediante el acceso a los métodos y soluciones de detección más recientes. No obstante, la actualización de prueba no siempre es estable, por lo que NO debe utilizarse en servidores de producción y estaciones de trabajo que requieran un elevado nivel de disponibilidad y estabilidad. Actualización retrasada permite actualizar desde servidores de actualización especiales que ofrecen nuevas versiones de bases de firmas de virus con un retraso de al menos X horas (es decir, de bases de firmas comprobadas en un entorno real y que, por lo tanto, se consideran estables).

Activar optimización de entrega de actualizaciones: si se activa, los archivos de actualización se pueden descargar de CDN (red de distribución de contenido). Desactivar este ajuste puede causar interrupciones y ralentizaciones de las descargas cuando los servidores de actualización de ESET están sobrecargados. Desactivar este ajuste es útil cuando un cortafuegos está limitado a acceder solo a las direcciones IP de los servidores de actualización de ESET o cuando no funciona una conexión a los servicios de CDN.

Preguntar antes de descargar la actualización: el programa mostrará una notificación en la que podrá confirmar o rechazar las descargas de archivos de actualización. Si el tamaño del archivo de actualización es superior al valor especificado en el campo Preguntar si un archivo de actualización es mayor de (KB), el programa mostrará un cuadro de diálogo de confirmación. Si el tamaño del archivo de actualización se establece en 0 kB, el programa siempre mostrará un cuadro de diálogo de confirmación.



Actualizaciones del módulo

La opción **Elegir automáticamente** está activada de forma predeterminada. La opción **Servidor personalizado** es la ubicación en la que se almacenan las actualizaciones. Si utiliza un servidor de actualización de ESET, le recomendamos que deje seleccionada la opción predeterminada.

Activar actualizaciones más frecuentes de firmas de detección: las firmas de detección se actualizarán en intervalos más cortos. Desactivar este ajuste puede afectar negativamente a la velocidad de detección.

Permitir actualizaciones del módulo desde soportes extraíbles: le permite actualizar desde un medio extraíble si contiene el servidor mirror creado. Cuando se selecciona la opción Automático, la actualización se ejecutará en segundo plano. Si quiere mostrar los cuadros de diálogo de actualización, seleccione Preguntar siempre.

Cuando se utiliza un servidor local HTTP, también conocido como Mirror, el servidor de actualización debe configurarse de la forma siguiente:
http://nombre_o_dirección_IP_del_ordenador:2221

Cuando se utiliza un servidor local HTTP con SSL, el servidor de actualización debe configurarse de la forma siguiente:
https://nombre_o_dirección_IP_del_ordenador:2221

Cuando se utiliza una carpeta local compartida, el servidor de actualización debe configurarse de la forma siguiente:
\\nombre_o_dirección_IP_del_ordenador\carpeta_compartida

> Número de puerto del servidor HTTP especificado en los ejemplos anteriores depende del puerto en el que su servidor HTTP/HTTPS recibe las conexiones.

Actualizaciones del producto

Consulte Actualizaciones del producto.

Opciones de conexión

Consulte Opciones de conexión.

Actualizar reflejo

Consulte Mirror de actualización.

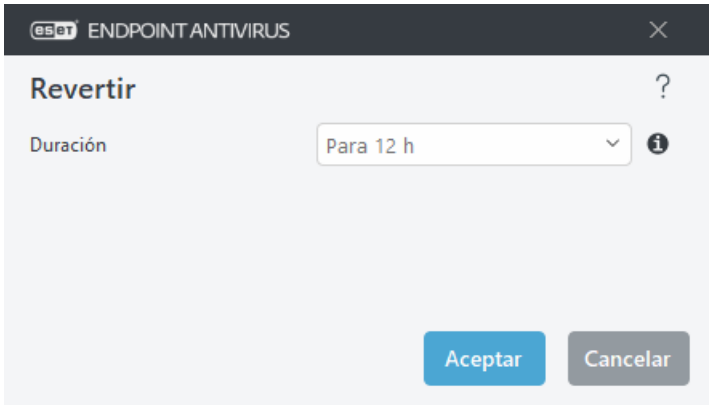
Reversión de actualización

Si sospecha que un nuevo módulo del programa o una nueva actualización del motor de detección pueden ser inestables o estar dañados, puede revertir a la versión anterior y desactivar las actualizaciones temporalmente. También puede activar actualizaciones desactivadas con anterioridad si las había pospuesto indefinidamente.

ESET Endpoint Antivirus registra instantáneas del motor de detección y los módulos del programa para usarlas con la función de reversión. Para crear instantáneas de la base de datos de virus, deje activada la opción **Crear instantáneas de los módulos**. Cuando la opción **Crear instantáneas de los módulos** está activada, se crea la primera instantánea durante la primera actualización. La siguiente se crea después de 48 horas. El campo **Número de instantáneas almacenadas localmente** define el número de instantáneas del motor de detección almacenadas.

> Cuando se alcanza la cantidad máxima de instantáneas (por ejemplo, tres), se sustituye la instantánea más antigua por una nueva cada 48 horas. ESET Endpoint Antivirus revierte las versiones de actualización del motor de detección y de los módulos del programa a la instantánea más antigua.

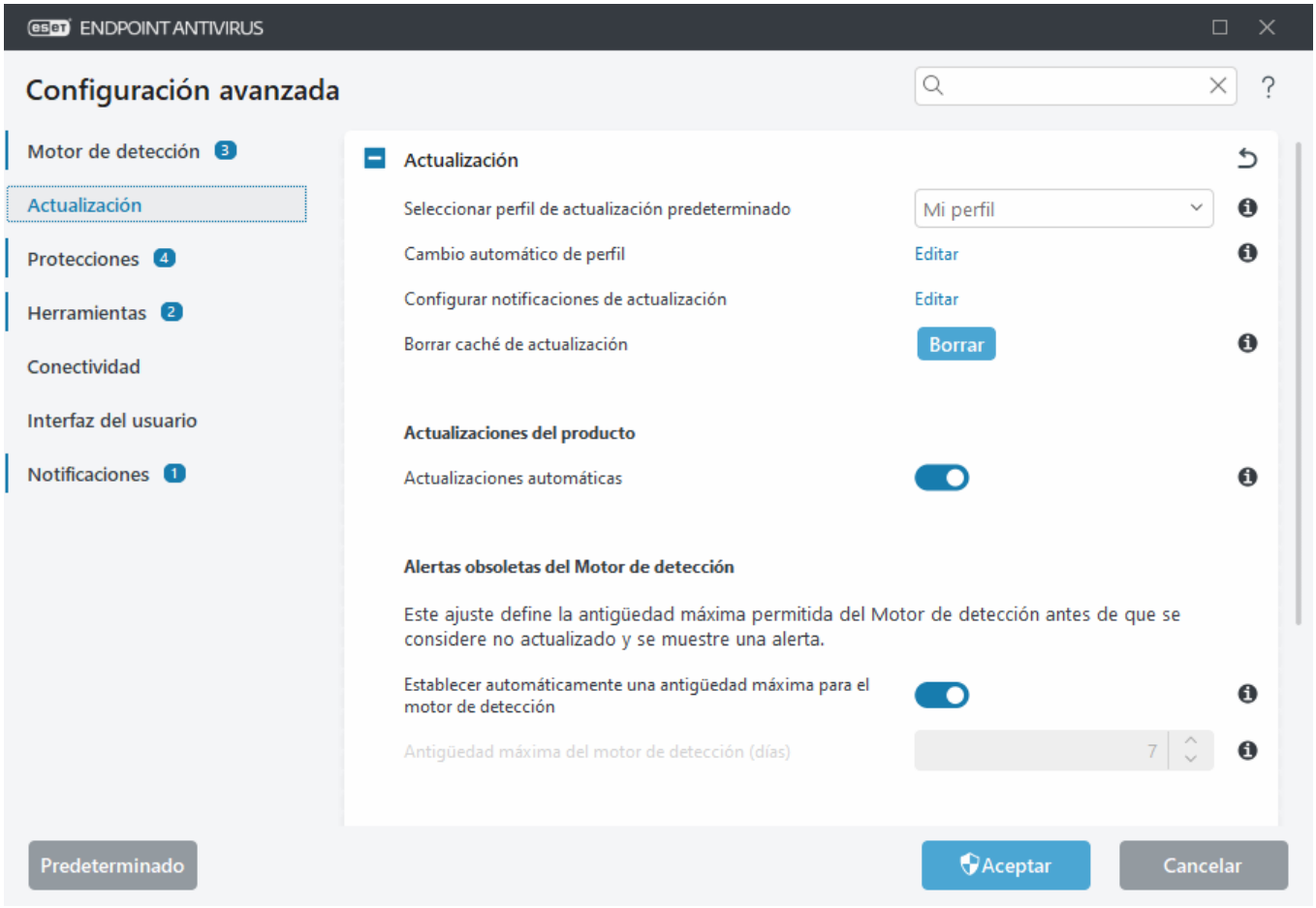
Abra Configuración avanzada > **Actualizaciones** > **Actualizaciones** > **Reversión de módulos** > **Reversión** para seleccionar un intervalo de tiempo desde el menú desplegable **Duración**.



Seleccione **Hasta que se revoque** si desea posponer las actualizaciones periódicas indefinidamente hasta que restaure la funcionalidad manualmente. Como esto representa un riesgo de seguridad potencial, no recomendamos que se seleccione esta opción.

Si se lleva a cabo una reversión, el botón **Revertir** cambia a **Permitir actualizaciones**. No se permitirán actualizaciones para el intervalo de tiempo seleccionado en el menú desplegable **Suspender actualizaciones**. La versión del motor de detección se degrada a la más antigua disponible y se almacena como instantánea en el

sistema de archivos del equipo local.



Suponga que 22700 es el número de versión del motor de detección más reciente, y que 22698 y 22696 están almacenadas como instantáneas del motor de detección. Tenga en cuenta que 22697 no está disponible. En este ejemplo, el equipo se desactivó durante la actualización de 22697 y se puso a disposición de los usuarios una actualización más reciente antes de que se descargara 22697. Si el campo **Número de instantáneas almacenadas de forma local** es dos y hace clic en **Revertir**, el motor de detección (incluidos los módulos del programa) se restaura a la versión número 22696. Este proceso puede llevar cierto tiempo. Compruebe que la versión del motor de detección se haya degradado en la pantalla Actualización.

Actualizaciones del producto

La sección **Actualizaciones del producto** contiene opciones relacionadas con las actualizaciones del producto. El programa le permite predefinir su comportamiento cuando hay nuevas actualizaciones del producto disponibles.

Las actualizaciones del producto presentan nuevas características o realizan cambios en las que ya existen de versiones anteriores. Se pueden realizar de manera automática, sin la intervención del usuario, o puede elegir que se le envíen notificaciones. Después de instalar actualizaciones del producto, puede que sea necesario reiniciar el ordenador.

Actualizaciones automáticas: al pausar las actualizaciones automáticas para perfiles de actualización específicos temporalmente, se desactivan las actualizaciones automáticas de componentes de los programas durante las conexiones a Internet en las que se utilizan otras redes o conexiones de uso medido. Mantenga activado este ajuste para tener acceso constante a las funciones más recientes y la mayor protección posible. Si desea más información sobre las actualizaciones automáticas, consulte Preguntas frecuentes sobre actualizaciones

automáticas.

De forma predeterminada, las actualizaciones del producto se descargan de los servidores de repositorio de ESET. En entornos de oficina grandes o sin conexión, el tráfico se puede distribuir para permitir el almacenamiento en caché interno de los archivos del producto.

Definición de un servidor personalizado para las actualizaciones de componentes del programa

1. Defina la ruta de acceso a las actualizaciones del producto en el campo **Servidor personalizado**.
Puede ser un vínculo HTTP(S), una ruta de acceso a un recurso compartido de red SMB, una ruta de acceso a una unidad de disco local o una ruta de acceso a un medio extraíble. Si se trata de una unidad de red, utilice la ruta de acceso UNC en lugar de una letra de unidad asignada.
2. Mantenga **Nombre de usuario** y **Contraseña** en blanco, si no se necesitan.
Si se necesitan, defina las credenciales adecuadas aquí para la autenticación HTTP en el servidor web personalizado.
3. Confirme los cambios y compruebe si hay actualizaciones del producto con una actualización de ESET Endpoint Antivirus estándar.

La selección de la opción más adecuada depende de la estación de trabajo donde se vaya a aplicar la configuración. Tenga en cuenta que existen ciertas diferencias entre las estaciones de trabajo y los servidores; por ejemplo, el reinicio automático del servidor tras una actualización del producto podría causar daños graves a su empresa.

Opciones de conexión

Para acceder a las opciones de configuración del servidor proxy para un perfil de actualización específico, abra Configuración avanzada > **Actualización** > **Perfiles** > **Actualizaciones** > **Opciones de conexión**.

Servidor proxy

Haga clic en el menú desplegable **Modo proxy** y seleccione una de las tres opciones siguientes:

- No usar servidor Proxy
- Conexión a través de un servidor Proxy específico
- Utilizar la configuración predeterminada

Seleccione **Usar la configuración global del servidor proxy** para utilizar la configuración del servidor proxy ya especificada en la sección Configuración avanzada > **Conectividad** > **Servidor proxy**.

Seleccione **No usar servidor Proxy** para especificar que no se utilice ningún servidor Proxy para actualizar ESET Endpoint Antivirus.

La opción **Conexión a través de un servidor proxy** debe seleccionarse si:

- Se utiliza un servidor proxy distinto del definido en **Herramientas** > **Servidor proxy** para actualizar ESET Endpoint Antivirus. En esta configuración, la información del nuevo proxy se debe especificar en **Servidor proxy**: dirección, **Puerto** de comunicación (3128 de forma predeterminada), **Nombre de usuario** y **Contraseña** del servidor proxy, en caso de ser necesarios.
- La configuración del servidor proxy no se ha definido globalmente, pero ESET Endpoint Antivirus se conecta a un servidor proxy para las actualizaciones.
- El ordenador se conecta a Internet mediante un servidor Proxy. La configuración se obtiene de navegador

durante la instalación del programa; no obstante, si se modifica (por ejemplo, al cambiar de proveedor de Internet), asegúrese de que la configuración del servidor proxy que aparece en esta ventana es la correcta. De lo contrario, el programa no se podrá conectar a los servidores de actualización.

La configuración predeterminada del servidor Proxy es **Utilizar la configuración predeterminada**.

Usar conexión directa si el proxy no está disponible: si no puede accederse al proxy durante la actualización, se omitirá.

Recursos compartidos de Windows

Para realizar una actualización desde un servidor local con una versión del sistema operativo Windows NT, es necesario autenticar todas las conexiones de red de forma predeterminada.

Para configurar una cuenta de este tipo, seleccione en el menú desplegable **Conectarse a la LAN como**:

- **Cuenta del sistema (predeterminado)**.
- **Usuario actual**.
- **Usuario especificado**.

Seleccione **Cuenta de sistema (predeterminado)** para utilizar la cuenta del sistema para la autenticación. Normalmente, no se realiza ningún proceso de autenticación si no se proporcionan datos en la sección de configuración de actualizaciones.

Para garantizar que el programa se autentique con la cuenta de un usuario registrado actualmente, seleccione **Usuario actual**. El inconveniente de esta solución es que el programa no se puede conectar al servidor de actualizaciones si no hay ningún usuario registrado.

Seleccione **Especificar usuario** si desea que el programa utilice una cuenta de usuario específica para la autenticación. Utilice este método cuando falle la conexión predeterminada con la cuenta del sistema. Recuerde que la cuenta del usuario especificado debe tener acceso al directorio de archivos actualizados del servidor local. De lo contrario, el programa no podrá establecer ninguna conexión ni descargar las actualizaciones.

Los campos **Nombre de usuario** y **Contraseña** son opcionales.

⚠ Cuando se selecciona **Usuario actual** o **Especificar usuario**, puede producirse un error al cambiar la identidad del programa para el usuario deseado. Por este motivo, se recomienda que introduzca los datos de autenticación de la red local en la sección principal de configuración de actualizaciones. Donde los datos de autenticación se deben introducir de la forma siguiente: *nombre_dominio**usuario* (si es un grupo de trabajo, escriba *nombre_grupo de trabajo**nombre*) y la contraseña. Cuando se actualiza desde la versión HTTP del servidor local, no es necesaria ninguna autenticación.

Seleccione **Desconectar** del servidor tras la actualización para forzar la desconexión si una conexión al servidor permanece activa incluso después de descargar las actualizaciones.

Actualizar reflejo

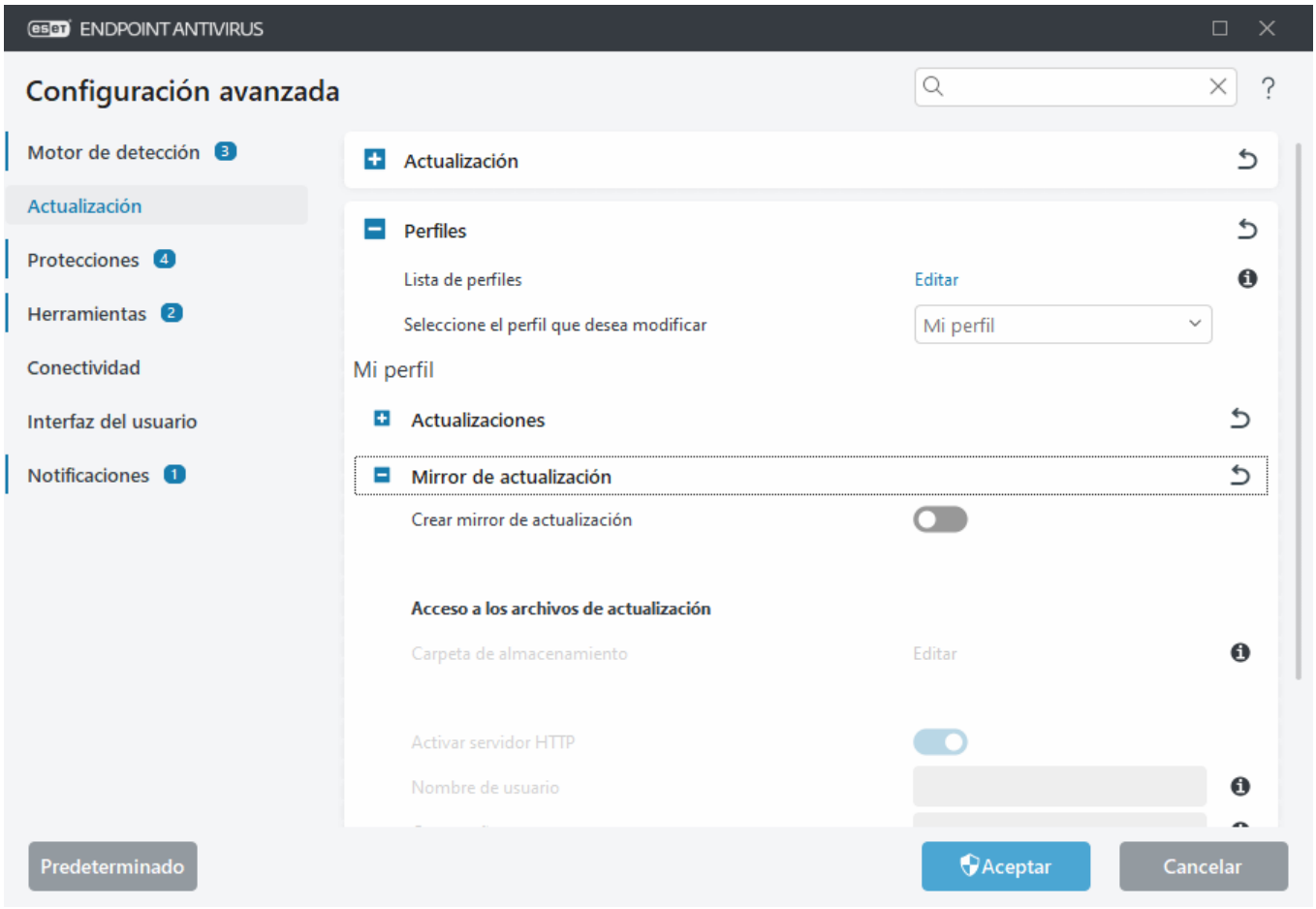
ESET Endpoint Antivirus le permite crear copias de los archivos de actualización, que puede utilizar para actualizar otras estaciones de trabajo de la red. El uso de un "mirror": es conveniente realizar una copia de los archivos de actualización del entorno de red local, dado que no necesitan descargarse del servidor de actualización del

proveedor varias veces ni que los descarguen todas las estaciones de trabajo. Las actualizaciones se descargan de manera centralizada en el servidor mirror local y, a continuación, se distribuyen a todas las estaciones de trabajo para evitar el riesgo de sobrecargar el tráfico de red. La actualización de estaciones de trabajo cliente desde un mirror optimiza el equilibrio de carga de la red y ahorra ancho de banda de la conexión a Internet.

El mirror de actualización crea copias de los archivos de actualización que se pueden usar para actualizar estaciones de trabajo que ejecutan la misma generación de ESET Endpoint Antivirus para Windows (por ejemplo, ESET Endpoint Antivirus para Windows versión 10.x crea archivos de actualización solo para la versión 10.x ESET Endpoint Antivirus para Windows y ESET Endpoint Security para Windows).

Para minimizar el tráfico de Internet en las redes en las que ESET PROTECT se utiliza para administrar un gran número de clientes, se recomienda utilizar ESET Bridge en lugar de configurar un cliente como Mirror. ESET Bridge se puede instalar con ESET PROTECT mediante el instalador todo en uno o como componente independiente. Para obtener más información y conocer las diferencias entre ESET Bridge, el proxy HTTP Apache, la herramienta Mirror y la conectividad directa, consulte la página de ayuda en línea de ESET PROTECT.

Las opciones de configuración del servidor Mirror local están en Configuración avanzada > **Actualizaciones** > **Perfiles** > **Mirror de actualización**.



Si desea crear un mirror en una estación de trabajo cliente, active la opción **Crear mirror de actualización**. Al activar dicha opción se activan otras opciones de configuración del Mirror, como la forma de acceder a los archivos actualizados y la ruta de actualización de los archivos replicados.

Acceso a los archivos de actualización

Activar servidor HTTP: si se activa esta opción, es posible acceder a los archivos de actualización a través de HTTP sin necesidad de credenciales.

En la sección Actualización desde el servidor Mirror se describen exhaustivamente los métodos de acceso al servidor Mirror. Existen dos métodos básicos para acceder al servidor Mirror: la carpeta que contiene los archivos de actualización se puede presentar como una carpeta de red compartida o los clientes pueden acceder al Mirror situado en un servidor HTTP.

La carpeta destinada a almacenar los archivos de actualización para el servidor Mirror se define en la sección **Carpeta para guardar archivos replicados**. Para elegir una carpeta diferente, haga clic en **Borrar** para eliminar la carpeta predefinida *C:\ProgramData\ESET\ESET Endpoint Antivirus\mirror* y haga clic en **Editar** para buscar una carpeta en el ordenador local o en la carpeta de red compartida. Si es necesaria una autorización para la carpeta especificada, deberá especificar los datos de autenticación en los campos **Nombre de usuario** y **Contraseña**. Si la carpeta de destino seleccionada se encuentra en un disco de red que ejecuta los sistemas operativos Windows NT, 2000 o XP, el nombre de usuario y la contraseña especificados deben contar con privilegios de escritura para la carpeta seleccionada. El nombre de usuario debe introducirse con el formato *Dominio/Usuario* o *Grupo de trabajo/Usuario*. No olvide que debe introducir las contraseñas correspondientes.

Servidor HTTP y SSL para el servidor Mirror

En la sección **Servidor HTTP** de la ficha **Mirror** puede especificar el **Puerto del servidor** en el que escuchará el servidor HTTP, así como el tipo de **Autenticación** utilizado por el servidor HTTP. De forma predeterminada, el puerto del servidor está establecido en **2221**.

Autenticación: define el método de autenticación utilizado para acceder a los archivos de actualización. Están disponibles las opciones siguientes: **Ninguna**, **Básica** y **NTLM**. Seleccione **Básica** para utilizar la codificación base64 con la autenticación básica de nombre de usuario y contraseña. La opción **NTLM** proporciona la codificación a través de un método seguro. Para la autenticación, se utilizará el usuario creado en la estación de trabajo que comparte los archivos actualizados. La configuración predeterminada es **Ninguna** y concede acceso a los archivos de actualización sin necesidad de autenticación.

Los datos de autenticación, como el **Nombre de usuario** y la **Contraseña**, solo están pensados para acceder al servidor HTTP mirror. Complete estos campos solo si son necesarios un nombre de usuario y una contraseña.

Si desea ejecutar el servidor HTTP con compatibilidad HTTPS (SSL), agregue el **archivo de cadena de certificados** o genere un certificado autofirmado. Están disponibles los siguientes **tipos de certificado**: ASN, PEM y PFX. Para una mayor seguridad, puede utilizar el protocolo HTTPS para descargar los archivos de actualización. Resulta casi imposible hacer un seguimiento de las transferencias de datos y credenciales de inicio de sesión utilizando este protocolo. La opción **Tipo de clave privada** está establecida de forma predeterminada en **Integrada** (y, por lo tanto, la opción **Archivo de clave privada** está desactivada de forma predeterminada). Esto significa que la clave privada forma parte del archivo de cadena de certificados seleccionado.

Certificados autofirmados para el Mirror HTTPS
Si está utilizando un servidor Mirror HTTPS, tendrá que importar su certificado en el almacén raíz de confianza de todos los equipos cliente. Consulte Instalación del certificado raíz de confianza en Windows.

Actualización desde el servidor Mirror

El servidor Mirror es básicamente un repositorio en el que los clientes pueden descargar los archivos de actualización. Existen dos métodos de configuración básicos de este tipo de servidor. La carpeta que contiene los archivos de actualización puede presentarse como una carpeta de red compartida o como un servidor HTTP.

El mirror de actualización crea copias de los archivos de actualización que se pueden usar para actualizar estaciones de trabajo que ejecutan la misma generación de ESET Endpoint Antivirus para Windows (por ejemplo, ESET Endpoint Antivirus para Windows versión 10.x crea archivos de actualización solo para la versión 10.x ESET Endpoint Antivirus para Windows y ESET Endpoint Security para Windows).

Acceso al servidor Mirror mediante un servidor HTTP interno

Esta es la configuración predeterminada especificada en la configuración predefinida del programa. Para permitir el acceso al Mirror mediante el servidor HTTP, diríjase a Configuración avanzada > **Actualización** > **Perfiles** > **Mirror de actualización** y seleccione **Crear mirror de actualización**.

En la sección **Servidor HTTP** de la ficha **Mirror** puede especificar el **Puerto del servidor** en el que escuchará el servidor HTTP, así como el tipo de **Autenticación** utilizado por el servidor HTTP. De forma predeterminada, el puerto del servidor está establecido en **2221**.

Autenticación: define el método de autenticación utilizado para acceder a los archivos de actualización. Están disponibles las opciones siguientes: **Ninguna**, **Básica** y **NTLM**. Seleccione **Básica** para utilizar la codificación base64 con la autenticación básica de nombre de usuario y contraseña. La opción **NTLM** proporciona la codificación a través de un método seguro. Para la autenticación, se utilizará el usuario creado en la estación de trabajo que comparte los archivos actualizados. La configuración predeterminada es **Ninguna** y concede acceso a los archivos de actualización sin necesidad de autenticación.

Si desea permitir el acceso a los archivos de actualización a través del servidor HTTP, la carpeta Mirror debe encontrarse en el mismo ordenador que la instancia de ESET Endpoint Antivirus que vaya a crearla.

Si se realizan varios intentos sin éxito de actualización desde el servidor Mirror, en el panel Actualización del menú principal aparecerá el error **Nombre de usuario o contraseña no válidos**. Le recomendamos que acceda a Configuración avanzada > **Actualización** > **Perfiles** > **Mirror de actualización** y compruebe el nombre de usuario y la contraseña. Este error suele estar provocado por la introducción incorrecta de los datos de autenticación.

Una vez que haya configurado su servidor Mirror, debe agregar el nuevo servidor de actualización a las estaciones de trabajo cliente. Para hacerlo, siga estos pasos:

- Abra la Configuración avanzada y haga clic en **Actualización** > **Perfiles** > **Actualizaciones** > **Actualizaciones del módulo**.
- Desactivar **Elegir automáticamente** y agregue un servidor nuevo al campo **Servidor de actualización** con uno de los siguientes formatos:
  http://dirección_IP_de_su_servidor:2221
  https://dirección_IP_de_su_servidor:2221 (si se utiliza SSL)

Acceso al servidor Mirror mediante el uso compartido del sistema

En primer lugar, es necesario crear una carpeta compartida en un dispositivo local o de red. A la hora de crear la carpeta para el servidor mirror, es necesario proporcionar acceso de "escritura" al usuario que va a guardar los archivos en la carpeta y acceso de "lectura" a todos los usuarios que vayan a actualizar ESET Endpoint Antivirus desde la carpeta Mirror.

A continuación, configure el acceso al servidor Mirror en la sección Configuración avanzada > **Actualización** > **Perfiles** > ficha **Mirror de actualización** desactivando **Activar servidor HTTP**. Esta opción se activa, de forma predeterminada, en el paquete de instalación del programa.

Si la carpeta compartida se encuentra en otro ordenador de la red, debe especificar los datos de autenticación para acceder al otro ordenador. Para especificar los datos de autenticación, abra la Configuración avanzada y haga clic en **Actualización** > **Perfiles** > **Actualizaciones** > **Opciones de conexión** > **Recursos compartidos de Windows** > **Conectarse a la LAN como**. Esta configuración es la misma que se aplica a las actualizaciones, tal como se describe en la sección Conectarse a la LAN como.

Para acceder a la carpeta de mirror, debe realizar esta acción con la misma cuenta que ha utilizado para registrarse en el ordenador en el que se ha creado el mirror. Si el ordenador se encuentra en un dominio, debe utilizar el nombre de usuario "dominio\usuario". Si el ordenador no se encuentra en un dominio, debe utilizar "dirección_IP_de_su_servidor\usuario" o "nombre_de_cliente\usuario".

Cuando haya terminado de configurar el servidor Mirror, en las estaciones de trabajo cliente, siga los pasos que se indican a continuación para establecer *UNC**RUTA* como servidor de actualización:

1. Abra la Configuración avanzada de y haga clic en **Actualización** > **Perfiles** > **Actualizaciones**.
2. Desactivar **Elegir automáticamente** junto a **Actualizaciones del módulo** y escriba un nuevo servidor en el campo **Servidor de actualización** con el formato *UNC**PATH*.

Para que las actualizaciones funcionen correctamente, es necesario especificar la ruta a la carpeta Mirror como una ruta UNC. Es posible que las actualizaciones de las unidades asignadas no funcionen.

Creación de la replicación con la herramienta Mirror
La herramienta Mirror crea una estructura de carpetas diferente de la que crea la herramienta Mirror de Endpoint. Cada carpeta contiene archivos de actualización para un grupo de productos. Debe especificar la ruta de acceso completa a la carpeta correcta en la configuración de actualización del producto que usa el mirror.
Por ejemplo, para actualizar ESET PROTECT desde el Mirror, establezca el Servidor de actualizaciones en (según la ubicación raíz de su servidor HTTP):
`http://your_server_address/mirror/eset_upd/ep10`

La última sección controla los componentes del programa (PCU). De forma predeterminada, los componentes del programa descargados se preparan para copiarse en el Repositorio local. Si la opción **Actualizaciones del producto** está activada, no es necesario hacer clic en **Actualizar** porque los archivos se copian en el Repositorio local automáticamente cuando se encuentran disponibles. Consulte Modo de actualización para obtener más información acerca de las actualizaciones del producto.

Resolución de problemas de actualización del Mirror

En la mayoría de los casos, los problemas durante la actualización desde un servidor Mirror se deben a una de estas causas: la especificación incorrecta de las opciones de la carpeta Mirror, la introducción de datos de

autenticación no válidos para la carpeta Mirror, la configuración incorrecta de las estaciones de trabajo que intentan descargar archivos de actualización del Mirror o una combinación de los motivos anteriores. A continuación, se ofrece información general acerca de los problemas más frecuentes durante la actualización desde el Mirror:

ESET Endpoint Antivirus notifica un error al conectarse al servidor de imagen: suele deberse a la especificación incorrecta del servidor de actualización (ruta de red a la carpeta Mirror) desde el que se actualizan las descargas de las estaciones de trabajo locales. Para verificar la carpeta, haga clic en el menú **Inicio** de Windows y en **Ejecutar**, introduzca el nombre de la carpeta y haga clic en **Aceptar**. A continuación, debe mostrarse el contenido de la carpeta.

ESET Endpoint Antivirus requiere un nombre de usuario y una contraseña: probablemente se deba a la presencia de datos de autenticación incorrectos (nombre de usuario y contraseña) en la sección de actualización. El nombre de usuario y la contraseña se utilizan para conceder acceso al servidor de actualización desde el que se actualiza el programa. Asegúrese de que los datos de autenticación son correctos y se introducen en el formato adecuado. Por ejemplo, Dominio/Nombre de usuario o Grupo de trabajo/Nombre de usuario, más las contraseñas correspondientes. Si "Todos" pueden acceder al servidor Mirror, debe ser consciente de que esto no quiere decir que cualquier usuario tenga acceso. "Todos" no hace referencia a cualquier usuario no autorizado, tan solo significa que todos los usuarios del dominio pueden acceder a la carpeta. Por ello, si "Todos" pueden acceder a la carpeta, será igualmente necesario introducir un nombre de usuario y una contraseña en la sección de configuración de actualizaciones.

ESET Endpoint Antivirus notifica un error al conectarse al servidor de imagen: la comunicación del puerto definida para acceder a la versión HTTP del Mirror está bloqueada.

ESET Endpoint Antivirus notifica un error al descargar archivos de actualización: suele deberse a una especificación incorrecta del servidor de actualización (ruta de acceso de red a la carpeta Mirror) desde el que se descargan las actualizaciones las estaciones de trabajo locales.

Protecciones

La protección protege contra ataques maliciosos al sistema mediante el control de las comunicaciones por Internet, el correo electrónico y los archivos. Por ejemplo, si se detecta un objeto clasificado como malware, se inicia la corrección. Las protecciones pueden eliminar este objeto bloqueándolo primero y, a continuación, desinfectándolo, eliminándolo o poniéndolo en cuarentena.

Para configurar las protecciones en detalle, abra Configuración avanzada > **Protecciones**.

Solo debe modificar Protecciones si es un usuario experimentado. Una configuración incorrecta de los ajustes puede provocar un menor nivel de protección.

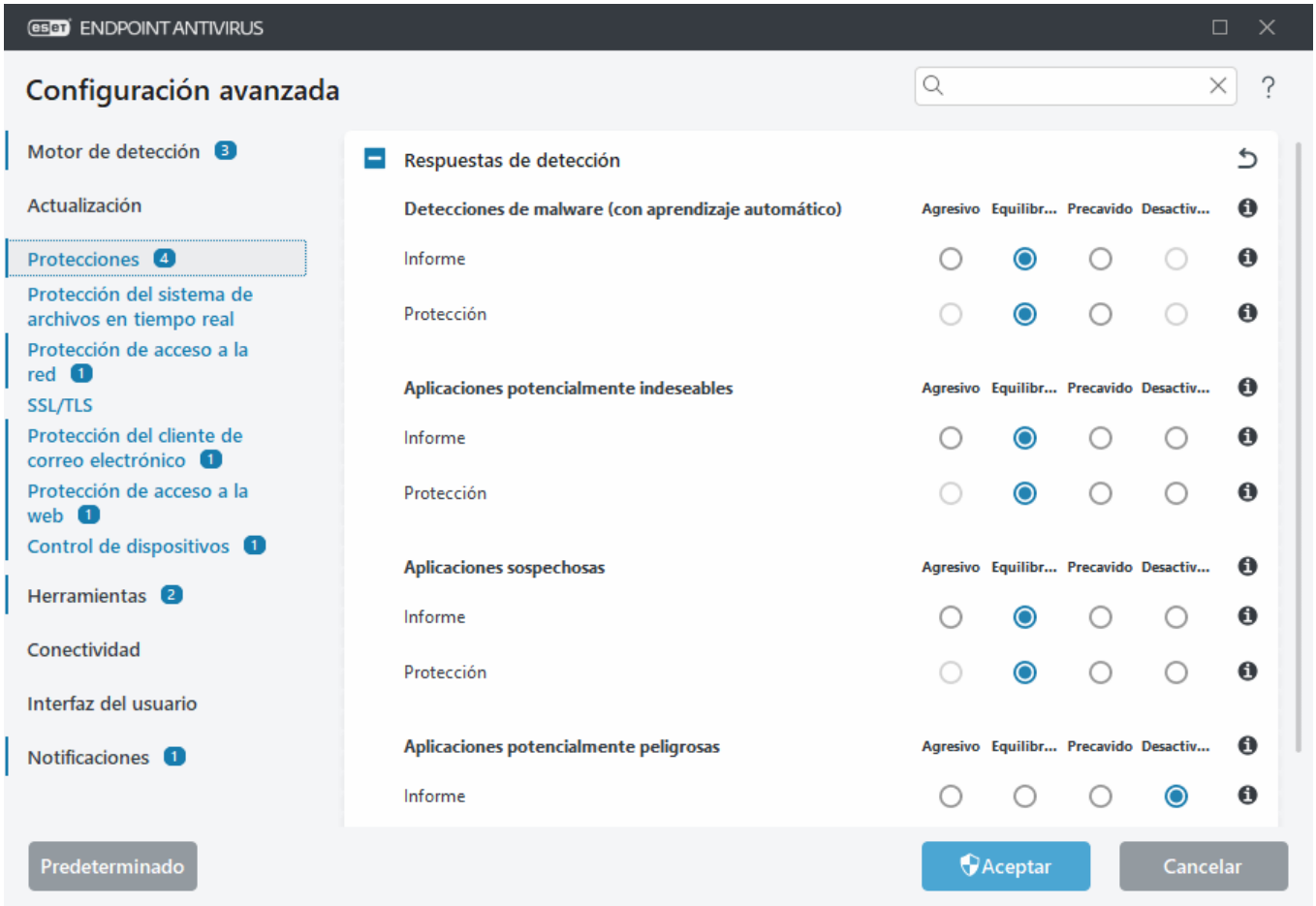
En esta sección:

- Respuestas de detección
- Configuración de informes
- Configuración de la protección

Respuestas de detección

Las respuestas de detección permiten configurar niveles de informes y protección para las siguientes categorías:

- **Detecciones de malware (con aprendizaje automático**: un virus informático es un código malicioso que puede agregarse al principio o al final de archivos existentes en su ordenador. Sin embargo, el término "virus" suele utilizarse de forma inadecuada. "Malware" (software malicioso) es un término más exacto. La detección de malware la realiza el módulo del motor de detección en combinación con el componente de aprendizaje automático. Puede obtener más información sobre estos tipos de aplicaciones en el Glosario.
- **Aplicaciones potencialmente indeseables**: el grayware, o aplicaciones potencialmente indeseables (PUA), es una amplia categoría de software no inequívocamente malicioso, al contrario de lo que sucede con otros tipos de malware, como virus o troyanos. Sin embargo, puede instalar software adicional indeseable, cambiar el comportamiento del dispositivo digital o realizar actividades no aprobadas o esperadas por el usuario. Puede obtener más información sobre estos tipos de aplicaciones en el Glosario.
- Entre las **aplicaciones sospechosas** se incluyen los programas comprimidos con empaquetadores o protectores. Los autores de código malicioso con frecuencia aprovechan estos tipos de protectores para evitar que se detecte.
- **Aplicaciones potencialmente peligrosas**: hace referencia a software comercial legítimo que puede utilizarse con fines maliciosos. Entre los ejemplos de este tipo de aplicaciones potencialmente peligrosas (PUA) encontramos herramientas de acceso remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que registran cada tecla pulsada por un usuario). Puede obtener más información sobre estos tipos de aplicaciones en el Glosario.



Protección mejorada

Aprendizaje automático avanzado forma ahora parte de las protecciones como capa avanzada de protección que mejora la detección con aprendizaje automático. Lea más información sobre este tipo de protección en el glosario.

Configuración de informes

Cuando se produce una detección (por ejemplo, se encuentra una amenaza y se clasifica como malware), se registra información en el Registro de detecciones, y se producen Notificaciones en el escritorio si está configurado en ESET Endpoint Antivirus.

Se configura el umbral de informes para cada categoría (denominada "CATEGORÍA"):

1. Detecciones de malware
2. Aplicaciones potencialmente indeseables
3. Potencialmente peligrosas
4. Aplicaciones sospechosas

Se realizan informes con el motor de detección, incluido el componente de aprendizaje automático. Puede establecer un umbral de informes más alto que el umbral de protección actual. Estos ajustes de informes no influyen en la acción de bloquear, desinfectar o eliminar objetos.

Lea lo siguiente antes de modificar un umbral (o nivel) de informes de CATEGORÍA:

Umbral	Explicación
Agresivo	Informes de CATEGORÍA configurados con la máxima sensibilidad. Se informa de más detecciones. El ajuste **Agresivo** pude identificar falsos positivos de CATEGORÍA.
Equilibrado	Informes de CATEGORÍA configurados como equilibrados. Este ajuste está optimizado para equilibrar el rendimiento y la precisión de las detecciones y el número de falsos positivos notificados.
Precavido	Informes de CATEGORÍA configurados para reducir al mínimo los falsos positivos a la vez que se mantiene un nivel de protección suficiente. Solo se informa de los objetos cuando la probabilidad es evidente y coincide con el comportamiento de CATEGORÍA.
Desactivado	Los informes de CATEGORÍA no están activos, y no se encuentran, notifican ni desinfectan detecciones de este tipo. Por lo tanto, este ajuste desactiva la protección frente a este tipo de detecciones. Desactivado no está disponible para los informes de malware y es el valor predeterminado para las aplicaciones potencialmente peligrosas.

Disponibilidad de los módulos de protección de ESET Endpoint Antivirus

La disponibilidad (activado o desactivado) de un módulo de protección de un umbral de CATEGORÍA seleccionado es la siguiente:

	Agresivo	Equilibrado	Precavido	Desactivado*
Módulo de aprendizaje automático avanzado	✓ (modo agresivo)	✔ (modo conservador)	X	X
Módulo del motor de detección	✔	✔	✔	X
Otros módulos de protección	✔	✔	✔	X

* No recomendado

Determinar versión del producto, versiones de los módulos del programa y fechas de compilación

1. Haga clic en **Ayuda y asistencia técnica** > **Acerca de ESET Endpoint Antivirus**.
2. En la pantalla **Acerca de**, la primera línea de texto muestra el número de versión de su producto ESET.
3. Haga clic en **Componentes instalados** para acceder a información sobre módulos específicos.

Notas

Varias notas útiles a la hora de configurar un umbral apropiado para su entorno:

- El umbral **Equilibrado** es el recomendado para la mayoría de las configuraciones.
- El umbral **Precavido** se recomienda para entornos en los que la prioridad sea reducir al mínimo los falsos positivos del software de seguridad.
- Cuando más alto sea el umbral de informes, mayor será el número de detecciones, pero también será mayor la posibilidad de que se produzcan falsos positivos.
- Desde la perspectiva del mundo real, no se pueden garantizar el 100 % de detección ni el 0 % de falsos positivos.
- Mantenga ESET Endpoint Antivirus y sus módulos actualizados para optimizar el equilibrio entre rendimiento y precisión en la detección y el número de falsos positivos.

Configuración de la protección

Si se informa de un objeto clasificado como CATEGORÍA, el programa bloquea el objeto y, a continuación, lo desinfecta, elimina o mueve a Cuarentena.

Lea lo siguiente antes de modificar un umbral (o nivel) de protección de CATEGORÍA:

Umbral	Explicación
Agresivo	Las detecciones de nivel agresivo (o inferior) de las que se informa se bloquean, y se inicia la corrección automática (es decir, la desinfección). Este ajuste se recomienda cuando se han analizado todos los puntos de conexión con ajustes agresivos y se han agregado los falsos positivos a las exclusiones de detección.
Equilibrado	Las detecciones de nivel equilibrado (o inferior) se bloquean, y se inicia la corrección automática (es decir, la desinfección).
Precavido	Las detecciones de nivel precavido se bloquean, y se inicia la corrección automática (es decir, la desinfección).
Desactivado	Útil para identificar y excluir falsos positivos. Desactivado no está disponible para la protección contra malware y es el valor predeterminado para las aplicaciones potencialmente peligrosas.

Prácticas recomendadas

NO ADMINISTRADA (estación de trabajo cliente individual)

Mantenga los valores recomendados predeterminados tal cual.

ENTORNO ADMINISTRADO

Estos ajustes se suelen aplicar a las estaciones de trabajo mediante una política.

1. Fase inicial

Esta fase puede durar hasta una semana.

- Configure todos los umbrales de **Informe** en **Equilibrado**.
  NOTA: Si es necesario, configúrelos en **Agresivo**.
- Configure o conserve **Protección** frente a malware como **Equilibrado**.
- Configure **Protección** frente a otras CATEGORÍAS como **Precavido**.
  NOTA: No se recomienda configurar el umbral de **Protección** como **Agresivo** en esta fase porque todas las detecciones encontradas se corregirían, incluidos los falsos positivos.
- Identifique los falsos positivos en Registro de detecciones y agréguelos a Exclusiones de detección.

2. Fase de transición

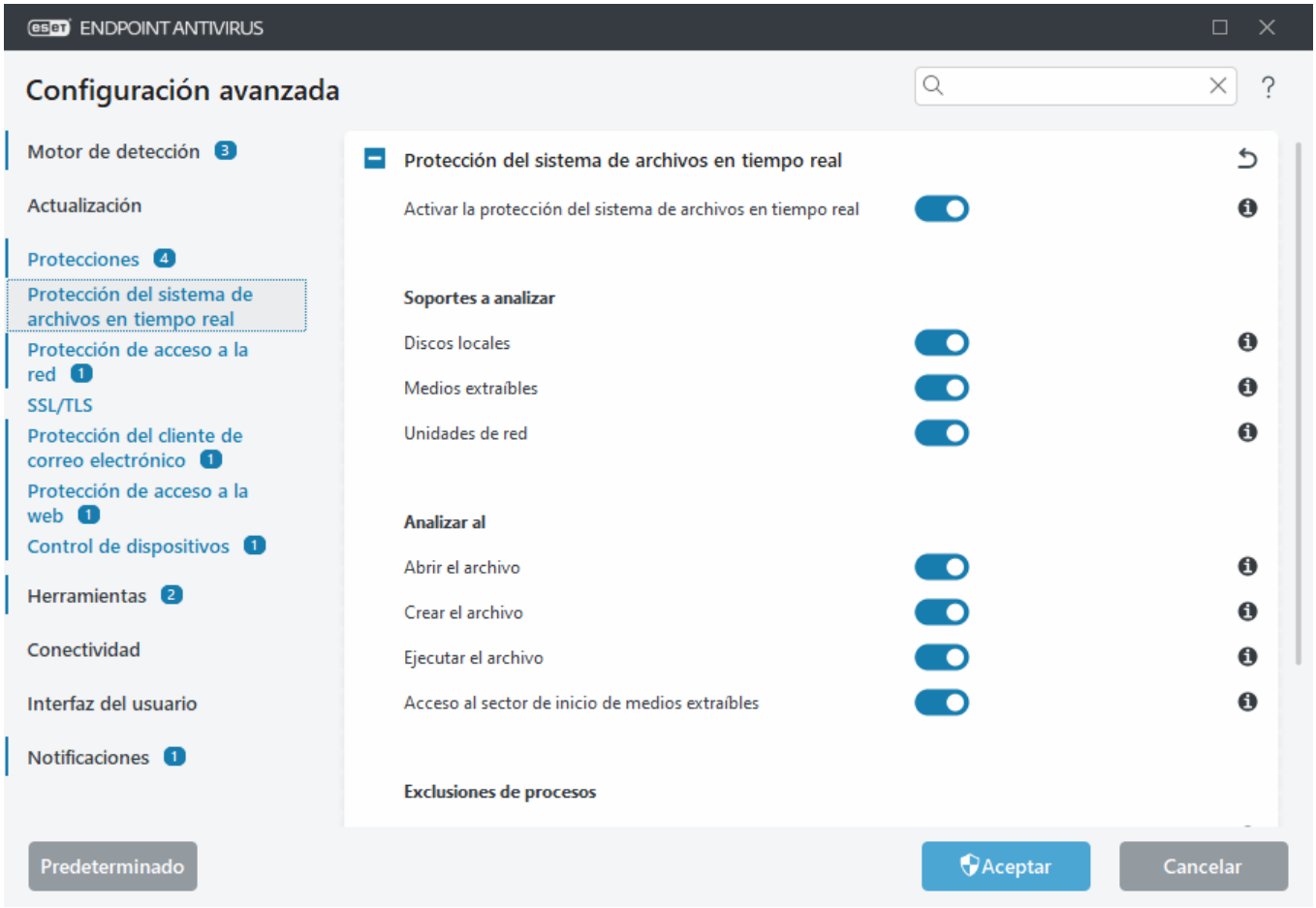
- Implemente la "Fase de producción" en algunas estaciones de trabajo a modo de prueba (no en todas las estaciones de trabajo de la red).

3. Fase de producción

- Configure todos los umbrales de **Protección** como **Equilibrado**.
- En la administración remota, use una política predefinida de antivirus apropiada para ESET Endpoint Antivirus.
- El umbral de protección **Agresivo** se puede seleccionar si se requieren los más altos índices de detección y se aceptan falsos positivos.
- Compruebe en el Registro de detecciones o los informes de ESET PROTECT que no falte ninguna detección.

Protección del sistema de archivos en tiempo real

Protección del sistema de archivos en tiempo real controla todos los archivos del sistema para garantizar que no contengan código malicioso al abrirlos, crearlos o ejecutarlos.



La protección del sistema de archivos en tiempo real comienza de forma predeterminada cuando se inicia el sistema y proporciona un análisis ininterrumpido. No recomendamos desactivar **Activar la protección del sistema de archivos en tiempo real** en Configuración avanzada > **Protecciones** > **Protección del sistema de archivos en tiempo real** > **Protección del sistema de archivos en tiempo real**.

Objetos a analizar

De forma predeterminada, se buscan posibles amenazas en todos los tipos de objetos:

- **Unidades locales**: analiza todos los discos duros del sistema (ejemplo: *C:*\, *D:*\).
- **Medios extraíbles**: analiza CD/DVD, almacenamiento USB, tarjetas de memoria, etc.
- **Unidades de red**: analiza todas las unidades de red asignadas (ejemplo: *H:*\ como *store04*) o las unidades de red de acceso directo (ejemplo: *store08*).

Recomendamos que esta configuración predeterminada se modifique solo en casos específicos como, por ejemplo, cuando el control de ciertos objetos ralentiza significativamente las transferencias de datos.

Analizar al

De forma predeterminada, se analizan todos los archivos cuando se crean, se abren o se ejecutan. Le recomendamos que mantenga esta configuración predeterminada, ya que ofrece el máximo nivel de protección en tiempo real para su ordenador:

- **Abrir el archivo**: analiza cuándo se abre un archivo.
- **Crear el archivo**: analiza un archivo creado o modificado.
- **Ejecutar el archivo**: analiza cuándo se ejecuta un archivo.

- **Acceso al sector de inicio de medios extraíbles**: cuando se insertan en el dispositivo medios extraíbles que contienen un sector de inicio, el sector de inicio se analiza inmediatamente. Esta opción no activa el análisis de archivos de medios extraíbles. El análisis de archivos de medios extraíbles está en **Medios que se analizarán** > **Medios extraíbles**. Para que **Acceso al sector de inicio de medios extraíbles** funcione correctamente, mantenga activado **Sectores de inicio/UEFI** en ThreatSense.

Exclusiones de procesos

Ver Exclusiones de procesos.

ThreatSense

La protección del sistema de archivos en tiempo real comprueba todos los tipos de medios y se activa con varios sucesos del sistema como, por ejemplo, cuando se accede a un archivo. Si se utilizan métodos de detección con la tecnología **ThreatSense** (tal como se describe en la sección ThreatSense), la protección del sistema de archivos en tiempo real se puede configurar para que trate de forma diferente los archivos recién creados y los archivos existentes. Por ejemplo, puede configurar la protección del sistema de archivos en tiempo real para que supervise más detenidamente los archivos recién creados.

Con el fin de que el impacto en el sistema sea mínimo cuando se utiliza la protección en tiempo real, los archivos que ya se analizaron no se vuelven a analizar (a no ser que se hayan modificado). Los archivos se analizan de nuevo inmediatamente tras cada actualización del motor de detección. Este comportamiento se controla con la opción **Optimización inteligente**. Si la opción **Optimización inteligente** está desactivada, se analizan todos los archivos cada vez que se accede a ellos. Para modificar esta configuración, abra Configuración avanzada > **Protecciones** > **Protecciones del sistema de archivos en tiempo real**. Haga clic en **ThreatSense** > **Otros** y seleccione o anule la selección de **Activar la optimización inteligente**.

La protección del sistema de archivos en tiempo real también le permite configurar parámetros ThreatSense adicionales.

Exclusiones de procesos

La característica Exclusiones de procesos le permite excluir procesos de aplicación de Protección del sistema de archivos en tiempo real. Para aumentar la velocidad de la copia de seguridad, la integridad de los procesos y la disponibilidad del servicio, se utilizan durante la copia de seguridad algunas técnicas que entran en conflicto con la protección contra malware a nivel de archivo. La única forma eficaz de evitar estas situaciones es desactivar el software antimalware. Al excluir un proceso específico (por ejemplo, un proceso de la solución de copia de seguridad), todas las operaciones de archivo atribuidas a dicho proceso excluido se ignoran y consideran seguras, lo que reduce al mínimo las interferencias con el proceso de copia de seguridad. Le recomendamos tener precaución al crear exclusiones: una herramienta de copia de seguridad excluida puede acceder a archivos infectados sin desencadenar una alerta, por lo que los permisos extendidos solo se permiten en el módulo de protección en tiempo real.

> No se debe confundir con Extensiones de archivo excluidas, Exclusiones del HIPS, Exclusiones de detección ni Exclusiones de rendimiento.

Las exclusiones de procesos ayudan a reducir al mínimo el riesgo de conflictos potenciales y mejoran el rendimiento de las aplicaciones excluidas, lo que, a su vez, tiene un efecto positivo sobre el rendimiento y la estabilidad generales del sistema operativo. La exclusión de un proceso/una aplicación es una exclusión de su archivo ejecutable (*.exe*).

Puede agregar archivos ejecutables a la lista de procesos excluidos en Configuración avanzada > **Protecciones** > **Protección del sistema de archivos en tiempo real** > **Protección del sistema de archivos en tiempo real** > **Exclusiones de procesos**.

Esta característica se diseñó para excluir herramientas de copia de seguridad. Excluir del análisis el proceso de la herramienta de copia de seguridad no solo garantiza la estabilidad del sistema, sino que, además, no afecta al rendimiento de la copia de seguridad, pues esta no se ralentiza durante su ejecución.

Haga clic en **Editar** para abrir la ventana de gestión **Exclusiones de procesos**, en la que puede agregar exclusiones y buscar el archivo ejecutable (por ejemplo, *Backup-tool.exe*) que se excluirá del análisis. En cuanto el archivo *.exe* se agrega a las exclusiones, ESET Endpoint Antivirus deja de supervisar la actividad de este proceso y no se ejecuta ningún análisis en ninguna de las operaciones de archivo realizadas por este proceso.

Si no utiliza la función de examinar al seleccionar el ejecutable del proceso, debe introducir manualmente una ruta de acceso completa del ejecutable. De lo contrario, la exclusión no funcionará correctamente y HIPS puede informar de errores.

También puede **Editar** procesos existentes o **Eliminar** dichos procesos de las exclusiones.

Protección de acceso a la web no tiene en cuenta esta exclusión, de modo que, si excluye el archivo ejecutable de su navegador, los archivos descargados se analizan de todas formas. Así, las infiltraciones pueden detectarse igualmente. Este caso es solo un ejemplo, y no le recomendamos crear exclusiones para navegadores.

Agregar o modificar exclusiones de procesos

Este cuadro de diálogo le permite **agregar** procesos excluidos del motor de detección. Las exclusiones de procesos ayudan a reducir al mínimo el riesgo de conflictos potenciales y mejoran el rendimiento de las aplicaciones excluidas, lo que, a su vez, tiene un efecto positivo sobre el rendimiento y la estabilidad generales del sistema operativo. La exclusión de un proceso/una aplicación es una exclusión de su archivo ejecutable (*.exe*).

Para seleccionar la ruta de acceso del archivo de una aplicación que es una excepción, haga clic en … (por ejemplo, *C:\Program Files\Firefox\Firefox.exe*). No escriba el nombre de la aplicación. En cuanto el archivo *.exe* se agrega a las exclusiones, ESET Endpoint Antivirus deja de supervisar la actividad de este proceso y no se ejecuta ningún análisis en ninguna de las operaciones de archivo realizadas por este proceso.

Si no utiliza la función de examinar al seleccionar el ejecutable del proceso, debe introducir manualmente una ruta de acceso completa del ejecutable. De lo contrario, la exclusión no funcionará correctamente y HIPS puede informar de errores.

También puede **Editar** procesos existentes o **Eliminar** dichos procesos de las exclusiones.

Modificación de la configuración de protección en tiempo real

La protección en tiempo real es el componente más importante para mantener un sistema seguro. Por lo que debe tener cuidado cuando modifique los parámetros correspondientes. Es aconsejable que los modifique

únicamente en casos concretos.

Una vez instalado ESET Endpoint Antivirus, se optimizará toda la configuración para proporcionar a los usuarios el máximo nivel de seguridad del sistema. Para restaurar la configuración predeterminada, haga clic en ↩ junto a Configuración avanzada > **Protecciones** > **Respuestas de detección**.

Análisis de protección en tiempo real

Para verificar que la protección en tiempo real funciona y detecta virus, use un archivo de prueba de eicar.com. Este archivo de prueba es un archivo inofensivo que pueden detectar todos los programas antivirus. El archivo lo ha creado la empresa EICAR (European Institute for Computer Antivirus Research) para probar la funcionalidad de los programas antivirus.

Puede descargar el archivo aquí: http://www.eicar.org/download/eicar.com.
Tras escribir esta URL en el navegador, debe ver el mensaje de que la amenaza se ha eliminado.

Qué debo hacer si la protección en tiempo real no funciona

En este capítulo, describimos los problemas que pueden surgir cuando se utiliza la protección en tiempo real y cómo resolverlos.

Protección en tiempo real desactivada

Si un usuario desactiva sin darse cuenta la protección en tiempo real, debe reactivar la función. Para reactivar la protección en tiempo real, vaya a **Configuración** en la ventana principal del programa y haga clic en **Ordenador** > **Protección del sistema de archivos en tiempo real**.

Si la protección en tiempo real no se activa al iniciar el sistema, probablemente se deba a que la opción **Activar la protección del sistema de archivos en tiempo real** está desactivada. Para asegurarse de que esta opción está activada, abra Configuración avanzada > **Protecciones** > **Protección del sistema de archivos en tiempo real**.

Si la protección en tiempo real no detecta ni desinfecta amenazas

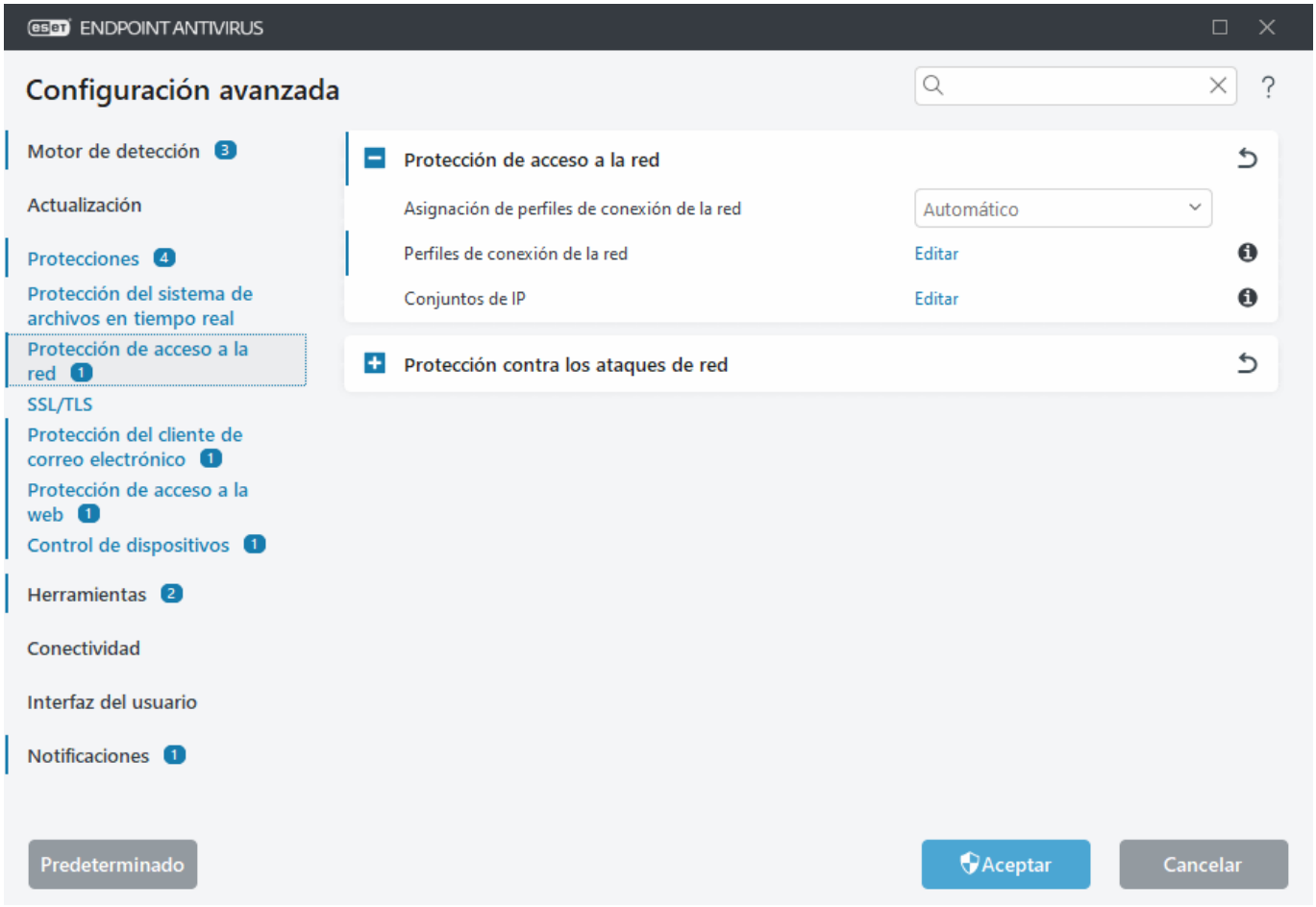
Asegúrese de que no tiene instalados otros programas antivirus en el ordenador. Si dos programas antivirus están instalados simultáneamente, pueden entrar en conflicto entre sí. Recomendamos que desinstale del sistema cualquier otro programa antivirus que haya en el sistema antes de instalar ESET.

La protección en tiempo real no se inicia

Si la protección en tiempo real no se activa al iniciar el sistema (y la opción **Activar la protección del sistema de archivos en tiempo real** está activada), es posible que se deba a conflictos con otros programas. Para resolver el problema, cree un registro del ESET SysInspector y envíelo al servicio de soporte técnico de ESET para que lo analice.

Protección de acceso a la red

La protección de acceso a la red le permite configurar todas las conexiones de red. De forma predeterminada, ESET Endpoint Antivirus tiene reglas de protección de acceso a la red configuradas para ofrecer la máxima seguridad. Sin embargo, es posible que determinados entornos necesiten una configuración personalizada. Solo los usuarios experimentados deben cambiar la configuración predeterminada.



Puede configurar los siguientes ajustes en Configuración avanzada > **Protecciones** > **Protección de acceso a la red** (haga clic en los vínculos siguientes para obtener una descripción detallada de cada opción de protección de acceso a la red):

Protección de acceso a la red

Perfiles de conexión de red: los perfiles se pueden utilizar para controlar la protección de acceso a la red para conexiones de red concretas.

Conjuntos de IP: puede definir colecciones de direcciones IP que creen un grupo de direcciones IP lógicas que, posteriormente, se pueden agregar como zona de confianza o excluir de Protección contra los ataques de red.

Protección contra los ataques de red

Perfiles de conexión de la red

Los perfiles se pueden utilizar para controlar el comportamiento de la Protección de acceso a la red de ESET Endpoint Antivirus para conexiones de red específicas. Al crear o editar reglas de IDS, reglas de protección contra ataques de fuerza bruta, puede asignarla a un perfil concreto o aplicarla a todos los perfiles. Cuando hay un perfil activo en una conexión de red, solo se aplican las reglas globales (que no tienen un perfil especificado) y las reglas que se han asignado a dicho perfil.

Puede configurar los perfiles y las asignaciones de conexión de red en Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Protección de acceso a la red**.

Asignación de perfiles de conexión de red: le permite elegir si a las conexiones de red recién descubiertas se les asigna automáticamente (seleccione **Automático** en el menú desplegable) un perfil predefinido o personalizado basado en Activadores configurados en perfiles de conexión de red o si desea que se le solicite (seleccione **Preguntar** en el menú desplegable) que Configure la protección de red y asigne un perfil manualmente cada vez que se detecte una nueva conexión de red.

También puede asignar manualmente un perfil de conexión de red específico en la ventana principal del programa > **Configurar** > **Red** > **Conexiones de red**. Desplácese sobre una conexión de red específica y haga clic en el icono ⋮ > **Editar** del menú para abrir la ventana Configurar protección de red y seleccionar un perfil.

Perfiles de conexión de red: haga clic en **Editar** para agregar o editar perfiles de conexión de red.

Los siguientes perfiles están predefinidos y no se pueden editar/eliminar:

Privado: para una red de confianza (red doméstica o de oficina). El ordenador y los archivos compartidos almacenados en el ordenador son visibles para otros usuarios de la red, y los recursos del sistema están disponibles para otros usuarios de la red (el acceso a los archivos y las impresoras compartidos está activado, la comunicación RPC entrante está activada y el escritorio remoto compartido está disponible). Se recomienda utilizar esta configuración al acceder a una red local segura. Este perfil se asigna automáticamente a una conexión de red si está configurado como Dominio o Red privada en Windows.

Pública: para una red que no es de confianza (red pública). Los archivos y las carpetas de su sistema no se comparten ni son visibles para otros usuarios de la red, y el uso compartido de recursos del sistema está desactivado. Se recomienda utilizar esta configuración al acceder a las redes inalámbricas. Este perfil se asigna automáticamente a cualquier conexión de red que no esté configurada como Dominio o Red privada en Windows.

Cuando el conexión de red cambia de perfil, se muestra una notificación en la esquina inferior derecha de la pantalla.

Agregar o editar perfiles de conexión de red

Puede agregar o editar perfiles de conexión de red en Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Protección de acceso a la red** > **Perfiles de conexión de red** > **Editar**. Para editar un perfil, debe seleccionarse en la lista de **Perfiles de conexión de red**.

Los siguientes perfiles están predefinidos y no se pueden editar/eliminar:

Privado: para una red de confianza (red doméstica o de oficina). El ordenador y los archivos compartidos almacenados en el ordenador son visibles para otros usuarios de la red, y los recursos del sistema están

disponibles para otros usuarios de la red (el acceso a los archivos y las impresoras compartidos está activado, la comunicación RPC entrante está activada y el escritorio remoto compartido está disponible). Se recomienda utilizar esta configuración al acceder a una red local segura. Este perfil se asigna automáticamente a una conexión de red si está configurado como Dominio o Red privada en Windows.

Pública: para una red que no es de confianza (red pública). Los archivos y las carpetas de su sistema no se comparten ni son visibles para otros usuarios de la red, y el uso compartido de recursos del sistema está desactivado. Se recomienda utilizar esta configuración al acceder a las redes inalámbricas. Este perfil se asigna automáticamente a cualquier conexión de red que no esté configurada como Dominio o Red privada en Windows.

Superior/Arriba/Abajo/Inferior  : permite ajustar el nivel de prioridad de los perfiles de conexión de red (los perfiles de conexión de red se evalúan y aplican según la prioridad. Siempre se aplica el primer perfil coincidente).

Agregar o editar un perfil

El perfil de conexión de red personalizado permite aplicar reglas de protección contra ataques de fuerza bruta y definir ajustes adicionales para conexiones de red concretas. En la sección Activadores, se especifica a qué conexiones de red debe asignarse el perfil personalizado.

Para abrir el editor de perfiles, en la ventana **Perfiles de conexión de red**:

- Haga clic en **Agregar**.
- Seleccione uno de los perfiles existentes y haga clic en **Editar**.
- Seleccione uno de los perfiles existentes y haga clic en **Copiar**.

Nombre: nombre personalizado de su perfil.

Descripción: descripción del perfil para ayudar a identificarlo.

Direcciones de confianza adicionales: las direcciones definidas aquí se agregan a la zona de confianza de la conexión de red a la que se aplica este perfil (independientemente del tipo de protección de la red).

Conexión de confianza: el ordenador y los archivos compartidos almacenados en el ordenador son visibles para otros usuarios de la red, y los recursos del sistema están disponibles para otros usuarios de la red (el acceso a los archivos y las impresoras compartidos está activado, la comunicación RPC entrante está activada y el escritorio remoto compartido está disponible). Se recomienda usar esta configuración al crear un perfil para una conexión de red local segura. Todas las subredes de red conectadas directamente también se consideran de confianza. Por ejemplo, si un adaptador de red está conectado a esta red con la dirección IP 192.168.1.5 y la máscara de subred 255.255.255.0, la subred 192.168.1.0/24 se agrega a la red de confianza de la conexión de red de dicho adaptador. Si el adaptador tiene más direcciones/subredes, todas serán de confianza.

Informe sobre cifrado WiFi débil: ESET Endpoint Antivirus mostrará una notificación en el escritorio cuando se conecte a una red inalámbrica no protegida o a una red con un nivel de protección débil.

Activadores: condiciones personalizadas que deben cumplirse para asignar este perfil de conexión de red a una conexión de red. Consulte Activadores para obtener una explicación detallada.

Activadores

Los activadores son condiciones personalizadas que deben cumplirse para asignar un Perfil de conexión de red a una conexión de red. Si la red conectada tiene los mismos atributos definidos en activadores para un perfil de red conectado, el perfil se aplicará a la red. Un perfil de conexión de red puede tener uno o varios activadores. Si hay varios activadores, se aplica la lógica OR (se debe cumplir al menos una condición). Puede definir activadores en el editor de perfil de conexión de red. La creación de perfiles de conexión de red personalizados debe ser realizada por un usuario experimentado.

Están disponibles los siguientes activadores:

Adaptador

Tipo de adaptador: aplique el perfil si la conexión de red se establece en el tipo de adaptador seleccionado.
Nombre del adaptador: aplique el perfil si el nombre del adaptador de red coincide.
IP del adaptador: aplique el perfil si la dirección IP del adaptador de red coincide.

DNS

Sufijo DNS: aplique el perfil si el nombre de dominio coincide.
IP DNS: aplique el perfil si la dirección IP del servidor DNS coincide.

WINS

Aplique el perfil si la Windows Internet Name Service (WINS) dirección IP asignada coincide.

DHCP

IP DHCP: coincide con la dirección IP del servidor DHCP.

Puerta de enlace predeterminada

IP: aplique el perfil si la dirección IP de la puerta de enlace predeterminada coincide.
Dirección MAC: aplique el perfil si la dirección MAC de la puerta de enlace predeterminada coincide.

Wi-Fi

SSID:: aplique el perfil si el SSID (nombre de la red Wi-Fi) coincide.
Nombre de perfil: aplique el perfil si el nombre del perfil de Wi-Fi coincide.
Tipo de seguridad: aplique el perfil si el tipo de seguridad coincide con el seleccionado en el menú desplegable. (Si desea hacer coincidir más de uno, cree otro activador).
Tipo de cifrado: aplique el perfil si el tipo de cifrado coincide con el seleccionado en el menú desplegable. Si desea hacer coincidir más de uno, cree otro activador.
Seguridad de red: aplique el perfil si la red está **abierta**/**protegida**.

Perfil de Windows

Aplicar perfil si la red está configurada en Windows como **Dominio**/**Privado**/**Público**.

Autenticación

La autenticación de red busca un servidor específico de la red y utiliza el cifrado asimétrico (RSA) para autenticar al servidor. El nombre de la red que se autentica debe coincidir con el nombre establecido en la configuración del servidor de autenticación. El nombre distingue entre mayúsculas y minúsculas. El nombre del servidor se puede escribir como una dirección IP, DNS o nombre NetBios.
Descargue ESET Authentication Server
La clave pública se puede importar con cualquiera de estos tipos de archivo:
• Clave pública cifrada PEM (.pem); puede generar esta clave utilizando ESET Authentication Server
• Clave pública cifrada.
• Certificado de clave pública (.crt).
Haga clic en **Probar** para probar su configuración. Si la autenticación es correcta, aparecerá Autenticación del servidor correcta. Si la autenticación no está configurada correctamente, aparecerá uno de los mensajes de error siguientes:
Error en la autenticación del servidor. Firma no válida o no concordante.
La firma del servidor no coincide con la clave pública introducida.
Error en la autenticación del servidor. El nombre de la red no coincide.
El nombre de la red configurada no se corresponde con el nombre del red del servidor de autenticación. Repase ambos nombres y asegúrese de que son idénticos.
Error en la autenticación del servidor. El servidor no respondió o la respuesta no es válida.
Si el servidor no se está ejecutando o no está accesible, el usuario no recibe ninguna respuesta. Puede recibir una respuesta no válida si hay otro servidor HTTP ejecutándose en la dirección especificada.
Clave pública introducida no válida.
Compruebe que el archivo de clave pública que ha introducido no esté dañado.

Conjuntos de IP

Un conjunto de IP es una colección de direcciones IP que forman un grupo lógico de direcciones IP y que resulta útil cuando se reutiliza el mismo conjunto de direcciones en varias reglas de protección contra ataques de fuerza bruta. ESET Endpoint Antivirus también contiene conjuntos de IP predefinidos para los que se aplican reglas internas. Un ejemplo de dicho grupo es una **Zona de confianza**. Zona de confianza representa un grupo de direcciones de red donde su ordenador y los archivos compartidos almacenados en el ordenador son visibles para otros usuarios de la red, y los recursos del sistema están disponibles para otros usuarios de la red.

Para agregar un conjunto de IP:

1. Abra Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Conjuntos de IP** > **Editar**.
2. Haga clic en **Agregar**, escriba un **Nombre** y una **Descripción** para la zona, y escriba una dirección IP remota en **Dirección del ordenador remoto (IPv4/IPv6, intervalo, máscara)**.
3. Haga clic en **Aceptar**.

Para obtener más información, consulte Editar conjuntos de IP.

Editar conjuntos de IP

Para obtener más información acerca de los conjuntos de IP, consulte Conjuntos de IP.

Columnas

Nombre: nombre de un grupo de ordenadores remotos.

Descripción: descripción general del grupo.

Direcciones IP: direcciones IP remotas que pertenecen a un conjunto de IP.

Elementos de control

Al **agregar** o **editar** un conjunto de IP, los siguientes campos están disponibles:

Nombre: nombre de un grupo de ordenadores remotos.

Descripción: descripción general del grupo.

Dirección del ordenador remoto (IPv4, IPv6, intervalo, máscara): le permite agregar una dirección remota, un rango de direcciones o una subred.

Eliminar: quita una zona de la lista.

Los conjuntos de IP predefinidos no se pueden quitar.

Ejemplos de direcciones IP

Agregar dirección IPv4:
Dirección única: agrega una dirección IP de un equipo individual (por ejemplo, *192.168.0.10*).
Rango de direcciones: especifique las direcciones IP inicial y final para delimitar el intervalo de direcciones de varios ordenadores (por ejemplo, *192.168.0.1-192.168.0.99*).
Subred: grupo de ordenadores definido por una dirección IP y una máscara. Por ejemplo, 255.255.255.0 es la máscara de red para la subred 192.168.1.0. Para excluir todo el tipo de subred en *192.168.1.0/24*.
Agregar dirección IPv6:
Dirección única: agrega la dirección IP de un ordenador individual (por ejemplo, *2001:718:1c01:16:214:22ff:fec9:ca5*).
Subred: grupo de ordenadores definido por una dirección IP y una máscara (por ejemplo, *2002:c0a8:6301:1::1/64*).

Protección contra los ataques de red (IDS)

La protección contra los ataques de red (IDS) mejora la detección de ataques de vulnerabilidades conocidas. Obtenga más información sobre la protección contra los ataques de red en el Glosario. Para configurar la protección contra ataques de red, abra Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Protección contra ataques de red**.

Activar Protección contra ataques en la red (IDS): analiza el contenido del tráfico de red y le protege contra posibles ataques de red. Se bloqueará todo el tráfico que se considere dañino.

Activar la protección contra botnets: detecta y bloquea las comunicaciones con servidores de control y comando maliciosos basándose en patrones habituales cuando el ordenador está infectado y un bot intenta establecer comunicación. Lea más sobre la protección contra botnets en el glosario.

Reglas de IDS: esta opción le permite configurar opciones de filtro avanzadas para detectar varios tipos de ataques y exploits que se pueden usar para dañar su ordenador.

Todos los sucesos importantes detectados por la protección de la red se guardan en un archivo de registro. Consulte el registro de protección de la red para obtener más información.

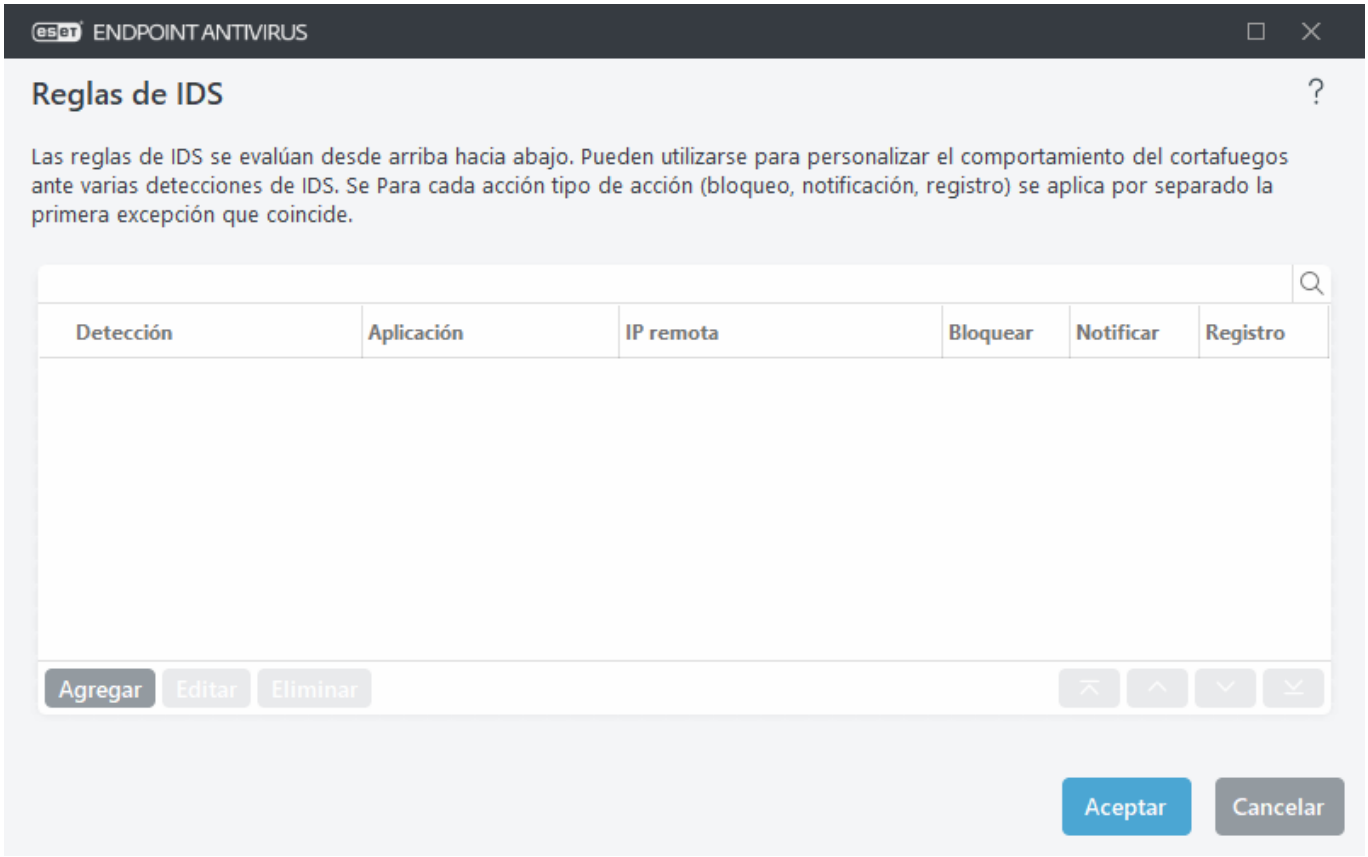
Reglas de IDS

En algunas situaciones, el Servicio de detección de intrusiones (IDS) puede detectar la comunicación entre routers u otros dispositivos de red internos como un ataque potencial. Por ejemplo, puede agregar la dirección segura conocida a las Direcciones excluidas de la zona de IDS para ignorar el IDS.

Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:
- Crear reglas de IDS en estaciones de trabajo cliente en ESET Endpoint Antivirus
- Crear reglas de IDS para estaciones de trabajo cliente en ESET PROTECT

Administración de reglas de IDS

- **Agregar**: haga clic aquí para crear una nueva regla de IDS.
- **Modificar**: haga clic aquí para modificar una regla de IDS.
- **Quitar**: seleccione y haga clic aquí para quitar una regla de la lista de reglas de IDS.
- **Superior/Arriba/Abajo/Inferior**: le permite ajustar el nivel de prioridad de las reglas (las excepciones se evalúan de arriba abajo).



Las ficha **Exclusiones** se mostrará si un administrador crea exclusiones de IDS en ESET PROTECT Web Console. Las exclusiones de IDS solo pueden contener reglas de permiso y se evalúan antes de las reglas de IDS.

Editor de reglas

Detección: tipo de detección.

Nombre de amenaza: puede especificar un nombre de amenaza para algunas de las detecciones disponibles.

Aplicación: para seleccionar la ruta de acceso del archivo de una aplicación que es una excepción, haga clic en … (por ejemplo, *C:\Program Files\Firefox\Firefox.exe*). No escriba el nombre de la aplicación.

Dirección IP remota: una lista de direcciones/rangos/subredes IPv4 o IPv6 remotos. Las direcciones deben separarse mediante comas.

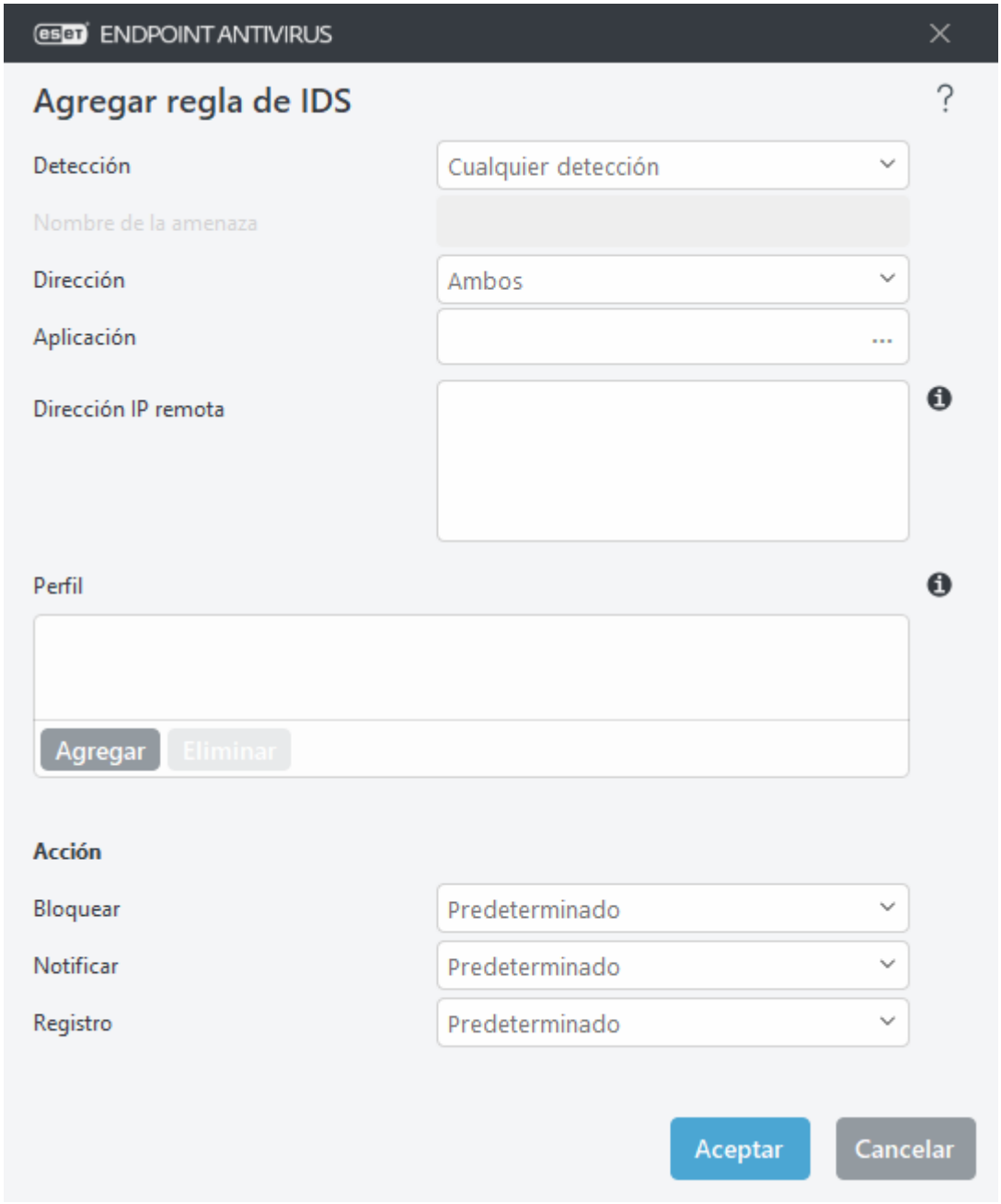
Perfil: puede elegir un perfil de conexión de red al que se aplicará esta regla.

Acción

Bloquear: cada proceso del sistema tiene su propio comportamiento predeterminado y su propia acción asignada (bloquear o permitir). Si desea anular el comportamiento predeterminado de ESET Endpoint Antivirus, puede elegir la acción de bloquearlo o la acción de permitirlo en el menú desplegable.

Notificar: seleccione Sí para mostrar Notificaciones en el escritorio en su ordenador. Seleccione No si no desea notificaciones en el escritorio. Los valores disponibles son Predeterminado/Sí/No.

Registrar: seleccione **Sí** para registrar sucesos en los archivos de registro de ESET Endpoint Antivirus. Seleccione **No** si no desea registrar sucesos. Los valores disponibles son **Predeterminado**/**Sí**/**No**.



Desea mostrar una notificación y recopilar un registro cada vez que se produzca el suceso:

1. Haga clic en **Agregar** para agregar una nueva regla de IDS.
2. Seleccione una alerta específica en el menú desplegable **Detección**.
3. Haga clic en **…** y seleccione la ruta de acceso del archivo de la aplicación a la que desee aplicar la notificación.
4. Deje **Predeterminado** en el menú desplegable **Bloquear**. Se heredará la acción predeterminada aplicada por ESET Endpoint Antivirus.
5. Seleccione en el menú desplegable **Notificar** y en el menú desplegable **Registrar** la opción **Sí**.
6. Haga clic en **Aceptar** para guardar esta notificación.

Desea quitar las notificaciones recurrentes para un tipo de detección que no considere una amenaza:
1. Haga clic en **Agregar** para agregar una nueva excepción de IDS.
2. Seleccione una alerta concreta en el menú desplegable **Detección**, por ejemplo, **Sesión SMB sin extensiones de seguridad**.
3. Seleccione **En** en el menú desplegable de dirección si el origen es una comunicación entrante.
4. En el menú desplegable **Notificar**, seleccione la opción **No**.
5. En el menú desplegable **Registrar**, seleccione la opción **Sí**.
6. Deje **Aplicación** en blanco.
7. Si la comunicación no procede de una dirección IP concreta, deje **Direcciones IP remotas** en blanco.
8. Haga clic en **Aceptar** para guardar esta notificación.

Protección contra ataques de fuerza bruta

La protección contra ataques con fuerza bruta bloquea los ataques para adivinar contraseñas en los servicios RDP y SMB. Un ataque con fuerza es un método para descubrir una contraseña objetivo que consiste en probar de forma sistemática todas las combinaciones de letras, números y símbolos. Para configurar la protección contra ataques de fuerza bruta, abra Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Protección contra los ataques de red** > **Protección contra ataques de fuerza bruta**.

Activar la protección contra ataques de fuerza bruta: ESET Endpoint Antivirus inspecciona el contenido del tráfico de red y bloquea los intentos de ataques para adivinar contraseñas.

Reglas: permiten crear, editar y ver reglas para las conexiones de red entrantes y salientes. Para obtener más información, consulte Reglas.

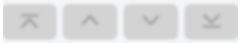
Exclusiones: lista de detecciones excluidas definidas por una dirección IP o una ruta de acceso de la aplicación. Puede crear y editar exclusiones en la ESET PROTECT. Para obtener más información, consulte Exclusiones.

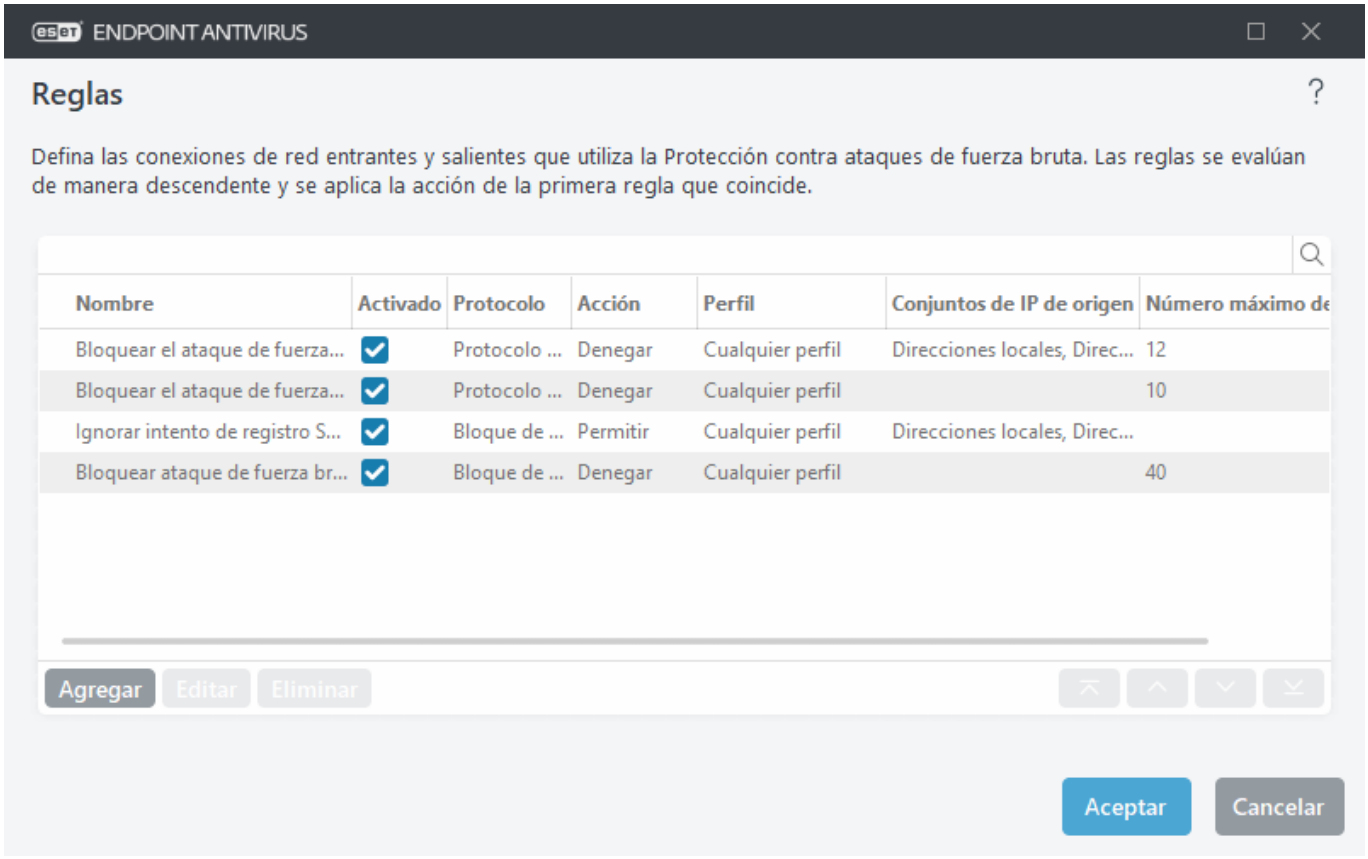
Para obtener más información sobre la protección contra ataques de fuerza bruta, consulte el artículo de la Guía de seguridad digital de ESET.

Reglas

Las reglas de protección contra ataques de fuerza bruta le permiten crear, editar y ver reglas para las conexiones de red entrantes y salientes. Las reglas predefinidas no se pueden editar ni eliminar.

Administración de reglas de protección contra ataques de fuerza bruta

- **Agregar**: haga clic para crear una nueva regla de protección contra ataques de fuerza bruta.
- **Editar**: haga clic para editar una regla de protección contra ataques de fuerza bruta.
- **Quitar**: seleccione y haga clic aquí para quitar una excepción de la lista de reglas de IDS.
-  **Superior/Arriba/Abajo/Inferior:** ajusta el nivel de prioridad de las reglas.



Para garantizar la máxima protección posible, se aplica la regla de bloqueo con el valor de **Número máximo de intentos** más bajo, aunque la regla esté situada más abajo en la lista de reglas cuando varias reglas de bloqueo cumplen las condiciones de detección.

Editor de reglas

Nombre: nombre de la regla.

Activado: desactive esta barra deslizante si desea conservar la regla en la lista pero no aplicarla.

Acción: elija si desea **denegar** o **permitir** la conexión si se cumple la configuración de regla.

Protocolo: el protocolo de comunicación que inspeccionará esta regla.

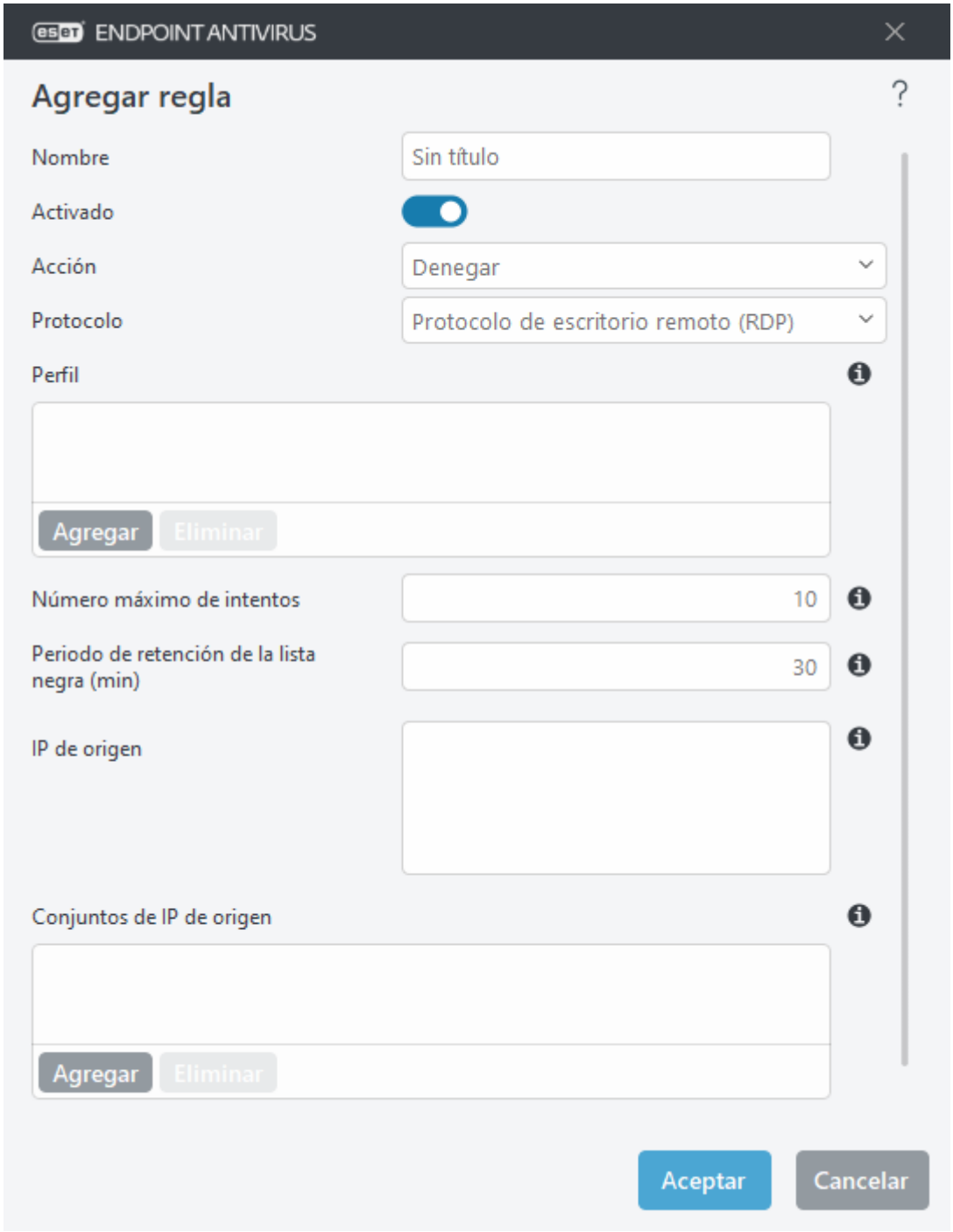
Perfil: puede elegir un perfil de conexión de red al que se aplicará esta regla.

Número máximo de intentos – El número máximo de intentos permitidos de repetición de ataque hasta que la dirección IP se bloquea y se agrega a la lista negra.

Periodo de retención de la lista negra (min): establece el tiempo para que la dirección caduque en la lista negra.

IP de origen: una lista de direcciones IP, rangos o subredes. Las direcciones deben separarse mediante comas.

Conjuntos de IP de origen: conjunto de direcciones IP que ya ha definido en conjuntos de IP.



Exclusiones

Las exclusiones de fuerza bruta se pueden usar para suprimir la detección de fuerza bruta con criterios específicos. Estas exclusiones se crean en ESET PROTECT basadas en la detección de fuerza bruta.

Columnas

- **Detección**: tipo de detección.
- **Aplicación**: para seleccionar la ruta de acceso del archivo de una aplicación que es una excepción, haga clic en … (por ejemplo, *C:\Program Files\Firefox\Firefox.exe*). No escriba el nombre de la aplicación.
- **IP remota**: una lista de direcciones/rangos/subredes IPv4 o IPv6 remotos. Las direcciones deben separarse mediante comas.

Administración de exclusiones

Las exclusiones se mostrarán si un administrador crea exclusiones de fuerza bruta en la consola web de ESET PROTECT. Las exclusiones solo pueden contener reglas de permiso y se evalúan antes que las reglas de IDS.

Opciones avanzadas

En Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Protección contra ataques de red** > **Opciones avanzadas**, puede habilitar o deshabilitar la detección de varios tipos de ataques y vulnerabilidades que pueden dañar su equipo.

En algunos casos no recibirá una notificación de amenaza sobre las comunicaciones bloqueadas. En la sección Registro y creación de reglas o excepciones del registro encontrará instrucciones para ver todas las comunicaciones bloqueadas en el registro del cortafuegos.

La disponibilidad de determinadas opciones de esta ventana puede variar en función del tipo o la versión de su producto de ESET y el módulo Cortafuegos, así como de la versión de su sistema operativo.

Detección de intrusiones

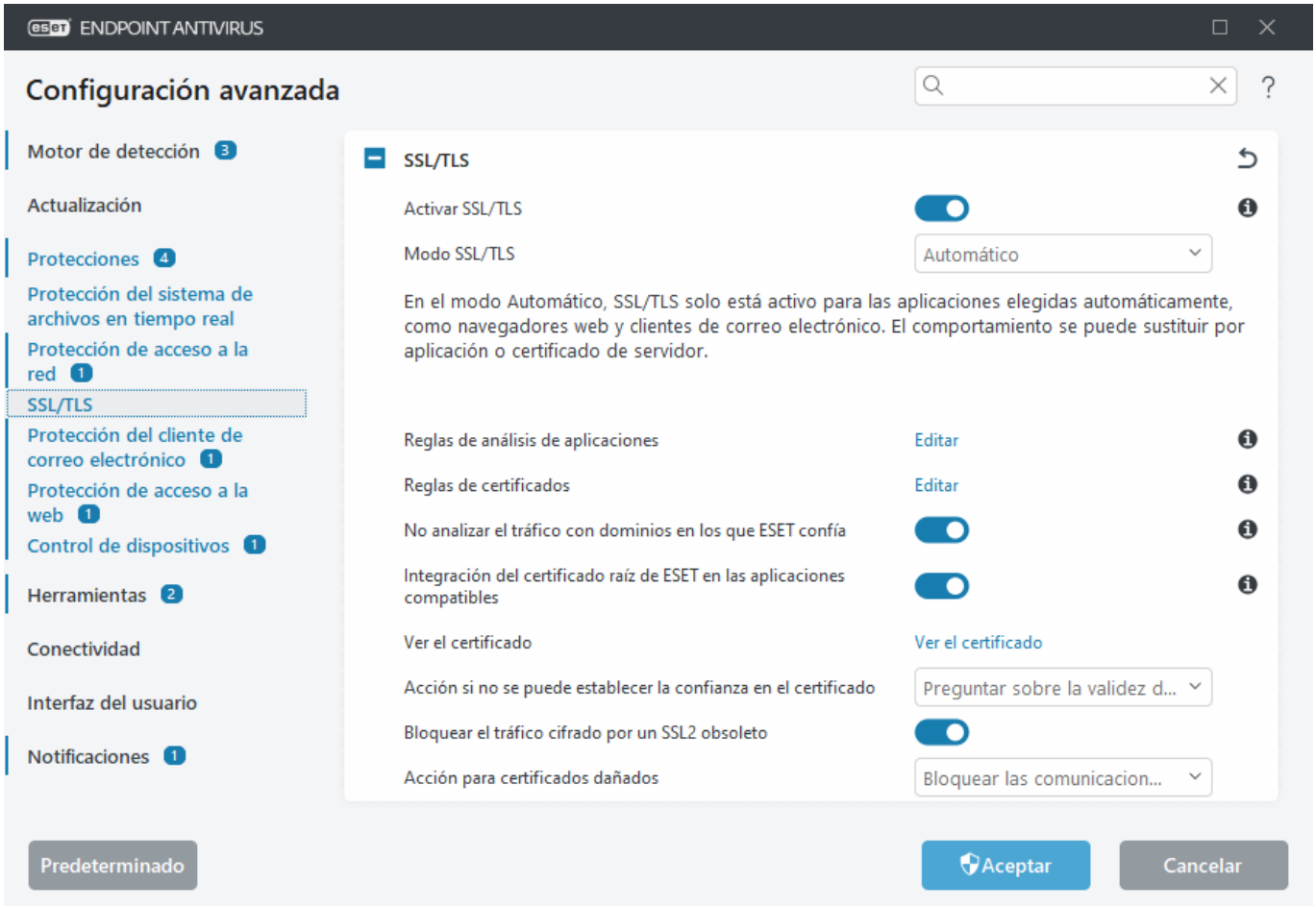
- **Protocolo SMB**: detecta y bloquea los problemas de seguridad del protocolo SMB que se indican a continuación:
- **Detección de autenticación de ataque por desafío malicioso al servidor**: esta opción le protege frente a un ataque que utilice un desafío malicioso durante la autenticación para obtener las credenciales del usuario.
- **Detección de evasión del sistema de detección de intrusos durante apertura de acceso con nombre**: detección de técnicas de evasión conocidas usadas para aperturas de acceso con nombre MSRPC en el protocolo SMB.
- **Detección de CVE** (Common Vulnerabilities and Exposures, vulnerabilidades y exposiciones comunes): métodos de detección implementados de diversos ataques, formularios, vulnerabilidades de seguridad y exploits a través del protocolo SMB. Consulte el sitio web de CVE en cve.mitre.org para obtener más información sobre los identificadores de CVE (CVE).
- **Protocolo RPC**: detecta y bloquea varios identificadores de CVE en el sistema de llamadas de procedimiento remoto desarrollado para el Entorno de computación distribuida (DCE).
- **Protocolo RDP**: detecta y bloquea varios identificadores de CVE en el protocolo RDP (consulte la información previa).
- **Bloquear la dirección no segura una vez detectado el ataque**: las direcciones IP que se han detectado como fuentes de ataques se agregan a la lista negra para evitar la conexión durante un determinado periodo de tiempo. Puede definir el **período de retención de la lista negra**, que establece el tiempo durante cuánto tiempo se bloqueará la dirección después de la detección del ataque.
- **Mostrar notificación tras la detección de un ataque**: activa el área de notificación de Windows en la esquina inferior derecha de la pantalla.
- **Mostrar notificaciones al recibir ataques que aprovechen de fallos de seguridad**: le avisa si se detectan ataques contra vulnerabilidades de seguridad o si una amenaza intenta acceder al sistema a través de este método.

Comprobación de paquetes

- **Permitir una conexión entrante para intercambio de admin en el protocolo de SMB**: los recursos compartidos administrativos (recursos compartidos del administrador) son los recursos compartidos de red predeterminados que comparten particiones del disco duro (*C$*, *D$*, etc.) en el sistema con la carpeta del sistema (*ADMIN$*). La desactivación de la conexión a los recursos compartidos del administrador debería mitigar muchos riesgos de seguridad. Por ejemplo, el gusano Conficker realiza ataques por diccionario para conectarse a recursos compartidos del administrador.
- **Denegar dialectos SMB anteriores (no compatibles)**: permite denegar sesiones de SMB que utilicen un dialecto SMB antiguo e incompatible con IDS. Los sistemas operativos Windows modernos son compatibles con dialectos SMB antiguos gracias a la compatibilidad con versiones anteriores de sistemas operativos antiguos como Windows 95. El atacante puede utilizar un dialecto antiguo en una sesión de SMB para evadir la inspección de tráfico. Deniegue dialectos SMB antiguos si su ordenador no necesita compartir archivos (o utilice la comunicación SMB en general) con un ordenador con una versión antigua de Windows.
- **Denegar la seguridad de SMB sin extensiones de seguridad**: la seguridad ampliada se puede utilizar durante la negociación de la sesión de SMB para proporcionar un mecanismo de autenticación más seguro que la autenticación de desafío o respuesta de LAN Manager (LM). El esquema de LM se considera débil, por lo que no se recomienda su uso.
- **Permitir la comunicación con el servicio Security Account Manager**: para obtener más información sobre este servicio, consulte [MS-SAMR].
- **Permitir la comunicación con el servicio Local Security Authority**: para obtener más información sobre este servicio, consulte [MS-LSAD] y [MS-LSAT].
- **Permitir la comunicación con el servicio Remote Registry**: para obtener más información sobre este servicio, consulte [MS-RRP].
- **Permitir la comunicación con el servicio Services Control Manager**: para obtener más información sobre este servicio, consulte [MS-SCMR].
- **Permitir la comunicación con el Server Service**: para obtener más información sobre este servicio, consulte [MS-SRVS].
- **Permitir la comunicación con los otros servicios**: otros servicios de MSRPC. MSRPC es la implementación de Microsoft del mecanismo DCE RPC. Además, MSRPC puede utilizar aperturas de acceso con nombre en el protocolo SMB (intercambio de archivos en la red) para el transporte (transporte ncacn_np). Los servicios de MSRPC proporcionan interfaces para acceder a sistemas Windows y administrarlos de forma remota. Se han detectado y aprovechado varias vulnerabilidades de seguridad en estado salvaje en el sistema MSRPC de Windows (gusano Conficker, gusano Sasser…). Desactive la comunicación con los servicios de MSRPC que no necesite proporcionar para mitigar muchos riesgos de seguridad (como la ejecución de código remoto o los ataques por fallo del servicio).

SSL/TLS

ESET Endpoint Antivirus puede comprobar si hay amenazas de comunicación que utilizan el protocolo SSL. Puede utilizar varios modos de filtrado para examinar las comunicaciones protegidas mediante el protocolo SSL: certificados de confianza, certificados desconocidos o certificados excluidos del análisis de comunicaciones protegidas mediante el protocolo SSL. Para editar la configuración de SSL/TLS, abraConfiguración avanzada > **Protecciones** > **SSL / TLS**.



Habilitar SSL/TLS: si está desactivado, ESET Endpoint Antivirus no analizará la comunicación a través de SSL/TLS.

El modo SSL/TLS ofrece las siguientes opciones:

Modo de filtrado	Descripción
Automático	El modo predeterminado solo analizará las aplicaciones correspondientes, como navegadores de Internet y clientes de correo. Puede anularlo seleccionando las aplicaciones donde se analiza la comunicación.
Interactivo	Si entra en un sitio nuevo protegido mediante SSL (con un certificado desconocido), se muestra un cuadro de diálogo con las acciones posibles. Este modo le permite crear una lista de aplicaciones o certificados SSL que se excluirán del análisis.
Basado en políticas	Seleccione esta opción para analizar todas las comunicaciones protegidas mediante el protocolo SSL, excepto las protegidas por certificados excluidos del análisis. Si se establece una comunicación nueva que utiliza un certificado firmado desconocido, no se le informará y la comunicación se filtrará automáticamente. Si accede a un servidor con un certificado que no sea de confianza pero que usted ha marcado como de confianza (se encuentra en la lista de certificados de confianza), se permite la comunicación con el servidor y se filtra el contenido del canal de comunicación.

Reglas de análisis de aplicaciones: permite personalizar el comportamiento ESET Endpoint Antivirus de aplicaciones específicas.

Reglas de certificados: permite personalizar el comportamiento de ESET Endpoint Antivirus para certificados SSL específicos.

No analizar el tráfico con dominios de confianza de ESET: cuando está habilitado, la comunicación con dominios

de confianza se excluirá del análisis. Una lista blanca integrada administrada por ESET determina la confiabilidad de un dominio.

Integración del certificado raíz de ESET en las aplicaciones compatibles: para que la comunicación SSL funcione correctamente en los navegadores y clientes de correo electrónico, es fundamental que el certificado raíz de ESET se agregue a la lista de certificados raíz conocidos (editores). Cuando esté activada, ESET Endpoint Antivirus agregará el certificado ESET SSL Filter CA a los navegadores conocidos (por ejemplo, Opera) de forma automática. En los navegadores que utilicen el almacén de certificados del sistema, el certificado se agregará automáticamente. Por ejemplo, Firefox está configurado automáticamente para confiar en entidades de certificación raíz del almacén de certificados del sistema.

Para aplicar el certificado en navegadores no admitidos, haga clic en **Ver certificado** > **Detalles** > **Copiar en archivo** y, a continuación, impórtelo manualmente en el navegador.

Acción si no se puede establecer la confianza del certificado: en algunos casos, un certificado de sitio web no se puede comprobar mediante el almacén de entidades de certificación raíz de confianza (TRCA) (por ejemplo, certificado caducado, certificado que no es de confianza, certificado no válido para el dominio específico o la firma que se puede analizar pero no firma el certificado correctamente). Los sitios web legítimos siempre utilizarán certificados de confianza. Si no están proporcionando uno, podría significar que un atacante está descifrando su comunicación o que el sitio web está experimentando dificultades técnicas.

Si se ha seleccionado **Preguntar sobre la validez del certificado** (predeterminada), se le pedirá que seleccione la acción cuando se establezca la comunicación cifrada. Se mostrará un cuadro de diálogo de selección que le permite marcar el certificado como de confianza o excluirlo. Si el certificado no se encuentra en la lista de TRCA, la ventana se mostrará en rojo. Si el certificado se encuentra en la lista de TRCA, la ventana se mostrará en verde.

Bloquear las comunicaciones que utilicen el certificado se puede seleccionar para que se terminen todas las conexiones cifradas con el sitio que utilicen un certificado sin verificar.

Bloquear tráfico cifrado por SSL2 obsoleto: la comunicación que utiliza la versión anterior del protocolo SSLse bloqueará automáticamente.

Acción para certificados dañados: un certificado dañado significa que el certificado utiliza un formato no reconocido por ESET Endpoint Antivirus o que se ha recibido dañado (por ejemplo, sobrescrito por datos aleatorios). En este caso, se recomienda dejar seleccionada la opción **Bloquear las comunicaciones que usan el certificado**. Si se selecciona **Preguntar sobre la validez del certificado**, se solicita al usuario que elija la acción que desea cuando se establezca la comunicación cifrada.

Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:
- Notificaciones de certificado en productos de ESET
- «Tráfico de red cifrado certificado no de confianza» se muestra al visitar páginas web

Reglas de la exploración de aplicaciones

Las **reglas de análisis de aplicaciones** se pueden utilizar para personalizar el comportamiento de ESET Endpoint Antivirus para determinadas aplicaciones, así como para recordar las acciones elegidas cuando el **Modo SSL/TLS** está en el **Modo interactivo**. La lista se puede ver y editar en Configuración avanzada > **Protecciones** > **SSL/TLS** > **Reglas de análisis de aplicaciones** > **Editar**.

La ventana **Reglas de análisis de aplicaciones** consta de:

Columnas

Aplicación: seleccione un archivo ejecutable en el árbol de directorios y haga clic en la opción **...**, o introduzca la ruta manualmente.

Acción de análisis: seleccione **Analizar** o **Ignorar** para analizar o ignorar la comunicación. Seleccione **Auto** para que el sistema realice el análisis en el modo automático y pregunte en el modo interactivo. Seleccione **Preguntar** para que el sistema siempre pregunte al usuario qué debe hacer.

Elementos de control

Agregar: agregue la aplicación filtrada.

Editar: seleccione la aplicación que desea configurar y haga clic en **Editar**.

Eliminar: seleccione la aplicación que desea eliminar y haga clic en **Eliminar**.

Importar/**Exportar**: importe aplicaciones desde un archivo o guarde la lista actual de aplicaciones en un archivo.

Aceptar/**Cancelar**: haga clic en **Aceptar** para guardar los cambios o en **Cancelar** para salir sin guardarlos.

Reglas de certificados

Las reglas de certificado se pueden usar para personalizar el comportamiento de ESET Endpoint Antivirus para certificados SSL específicos y para recordar las acciones elegidas cuando el **modo SSL/TLS** está en **modo interactivo**. La lista se puede ver y editar en Configuración avanzada > **Protecciones** > **SSL/TLS** > **Reglas de certificado** > **Editar**.

La ventana **Reglas de certificado** consta de:

Columnas

Nombre: nombre del certificado.

Emisor del certificado: nombre del creador del certificado.

Sujeto del certificado: en este campo se identifica a la entidad asociada a la clave pública almacenada en el campo de clave pública del asunto.

Acceso: seleccione **Permitir** o **Bloquear** como **Acción del acceso** para permitir o bloquear la comunicación que protege este certificado, independientemente de su fiabilidad. Seleccione **Auto** para permitir los certificados de confianza y preguntar cuando uno no sea de confianza. Seleccione **Preguntar** para que el sistema siempre pregunte al usuario qué debe hacer.

Analizar: seleccione **Analizar** o **Ignorar** como **Acción de análisis** para analizar o ignorar la comunicación que protege este certificado. Seleccione **Auto** para que el sistema realice el análisis en el modo automático y pregunte en el modo interactivo. Seleccione **Preguntar** para que el sistema siempre pregunte al usuario qué debe hacer.

Elementos de control

Agregar – agrega un certificado nuevo y ajusta su configuración de opciones de análisis y acceso.

Editar: seleccione el certificado que desea configurar y haga clic en **Editar**.

Eliminar: seleccione el certificado que desea eliminar y haga clic en **Quitar**.

Aceptar/Cancelar: haga clic en **Aceptar** para guardar los cambios o en **Cancelar** para salir sin guardarlos.

Tráfico de red cifrado

Si el sistema está configurado para utilizar el análisis SSL/TLS, se mostrará un cuadro de diálogo para solicitarle que seleccione una acción en dos situaciones diferentes:

En primer lugar, si un sitio web utiliza un certificado no válido o que no se puede verificar y ESET Endpoint Antivirus está configurado para preguntar al usuario en estos casos (la opción predeterminada es sí para los certificados que no se pueden verificar y no para los que no son válidos), se abre un cuadro de diálogo para preguntarle si desea **Permitir** o **Bloquear** la conexión. Si el certificado no está en el Trusted Root Certification Authorities store (TRCA), se considera no fiable.

En segundo lugar, si el **modo SSL/TLS** está establecido en **Modo interactivo**, se mostrará un cuadro de diálogo para cada sitio web para preguntarle si desea **Analizar** o **Ignorar** el tráfico. Algunas aplicaciones comprueban que nadie haya modificado ni inspeccionado su tráfico SSL en estos casos, ESET Endpoint Antivirus debe **Ignorar** el tráfico para que la aplicación siga funcionando.

> Ejemplos ilustrados.
> Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:
> • Notificaciones de certificado en productos para Windows de ESET
> • «Tráfico de red cifrado certificado no de confianza» se muestra al visitar páginas web

En ambos casos, el usuario tiene la opción de recordar la acción seleccionada. Las acciones guardadas se almacenan en las Reglas de certificados.

Protección del cliente de correo electrónico

Para configurar la protección del cliente de correo electrónico, abra Configuración avanzada > **Protecciones** > **Protección del cliente de correo electrónico** y elija una de las siguientes opciones de configuración:

- Protección del transporte de correo electrónico
- Protección de la casilla de correo
- ThreatSense

Protección del transporte de correo electrónico

Los protocolos IMAP(S) y POP3(S) son los más utilizados para recibir comunicaciones por correo electrónico en una aplicación de cliente de correo. El Protocolo de acceso a mensajes de Internet (IMAP) es otro protocolo de Internet para la recuperación de mensajes de correo electrónico. IMAP presenta algunas ventajas sobre POP3;

por ejemplo, permite la conexión simultánea de varios clientes al mismo buzón de correo y conserva la información de estado (si el mensaje se ha leído, contestado o eliminado). El módulo de protección que ofrece este control se inicia automáticamente al iniciar el sistema y, a continuación, está activo en la memoria.

ESET Endpoint Antivirus proporciona protección para estos protocolos, independientemente del cliente de correo electrónico utilizado, y sin necesidad de volver a configurar el cliente de correo electrónico. De forma predeterminada, se analiza toda la comunicación a través de los protocolos POP3 e IMAP, independientemente de los números de puerto POP3/IMAP predeterminados.
El protocolo MAPI no se analiza. Sin embargo, la comunicación con el servidor de Microsoft Exchange se puede analizar con el módulo de integración de clientes de correo electrónico como Microsoft Outlook.

> ESET Endpoint Antivirus también admite el análisis de los protocolos IMAPS (585, 993) y POP3S (995), que utilizan un canal cifrado para transferir información entre el servidor y el cliente. ESET Endpoint Antivirus comprueba la comunicación con los protocolos SSL (capa de sockets seguros) y TLS (seguridad de la capa de transporte).
> La comunicación cifrada se analizará de forma predeterminada. Para ver la configuración del análisis, abra Configuración avanzada > **Protecciones** SSL/TLS.

Para configurar Protección de transporte de correo, abra Configuración avanzada > **Protecciones** > **Protección de cliente de correo electrónico** > **Protección de transporte de correo**.

Activar protección de transporte de correo: cuando está activada, la comunicación de transporte de correo será analizada por ESET Endpoint Antivirus.

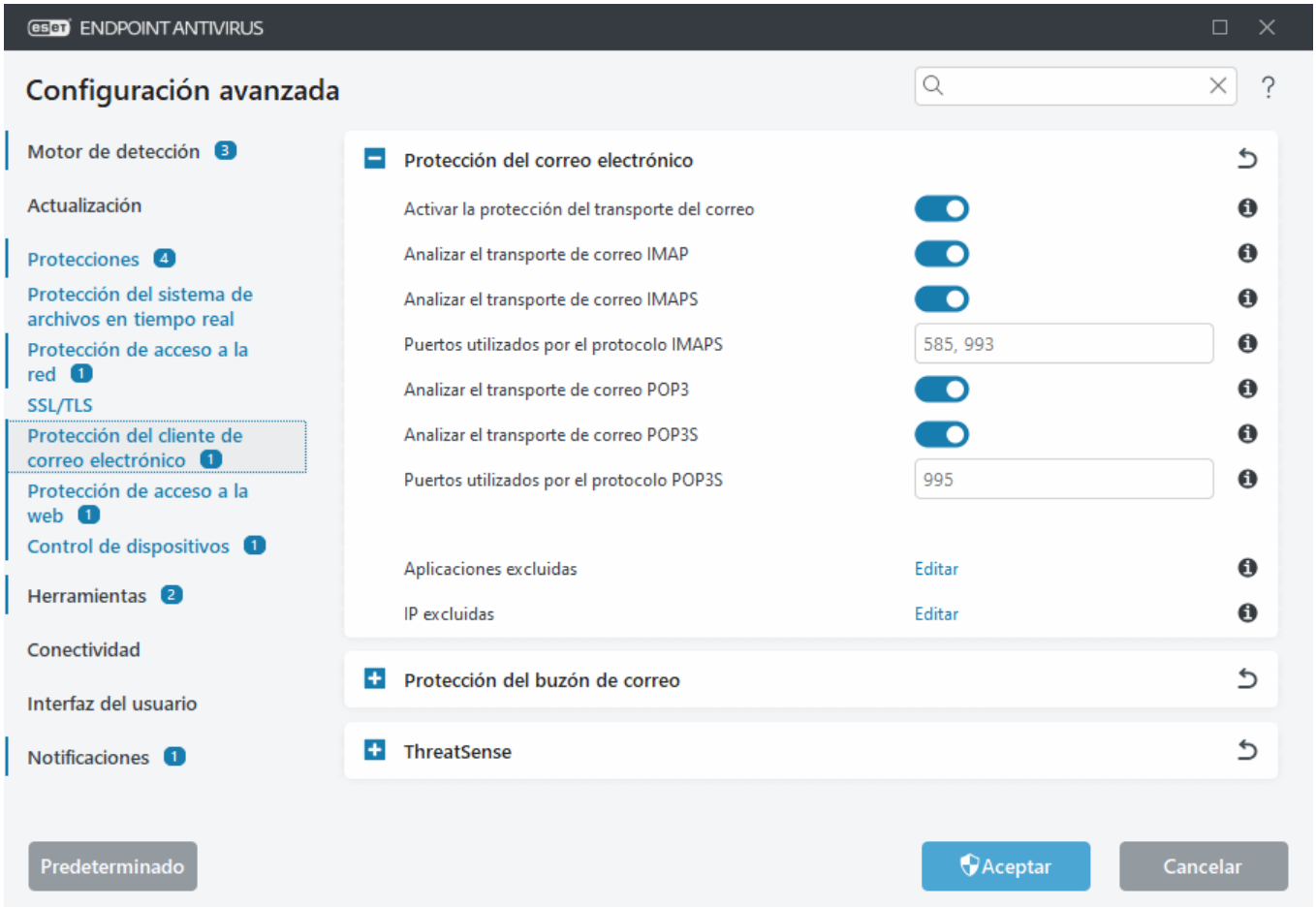
Puede elegir qué protocolos de transporte de correo se analizarán haciendo clic en el botón de alternancia situado junto a las siguientes opciones (de forma predeterminada, el análisis de todos los protocolos está habilitado):

- **Analizar el transporte de correo IMAP**
- **Analizar el transporte de correo IMAPS**
- **Analizar el transporte de correo POP3**
- **Analizar el transporte de correo POP3S**

De forma predeterminada, ESET Endpoint Antivirus escaneará la comunicación IMAPS y POP3S en los puertos estándar. Para agregar puertos personalizados para los protocolos IMAPS y POP3S, agréguelos al campo de texto junto a **Puertos utilizados por el protocolo IMAPS** o **Puertos utilizados por el protocolo POP3S**. Cuando haya varios números de puerto, deben delimitarse con una coma.

Aplicaciones excluidas: permite excluir aplicaciones específicas de ser analizadas por la protección de transporte de correo. Útil cuando la protección de acceso web causa problemas de compatibilidad.

IP excluidas: permite excluir direcciones remotas específicas de ser analizadas por la protección de transporte de correo. Útil cuando la protección de acceso web causa problemas de compatibilidad.



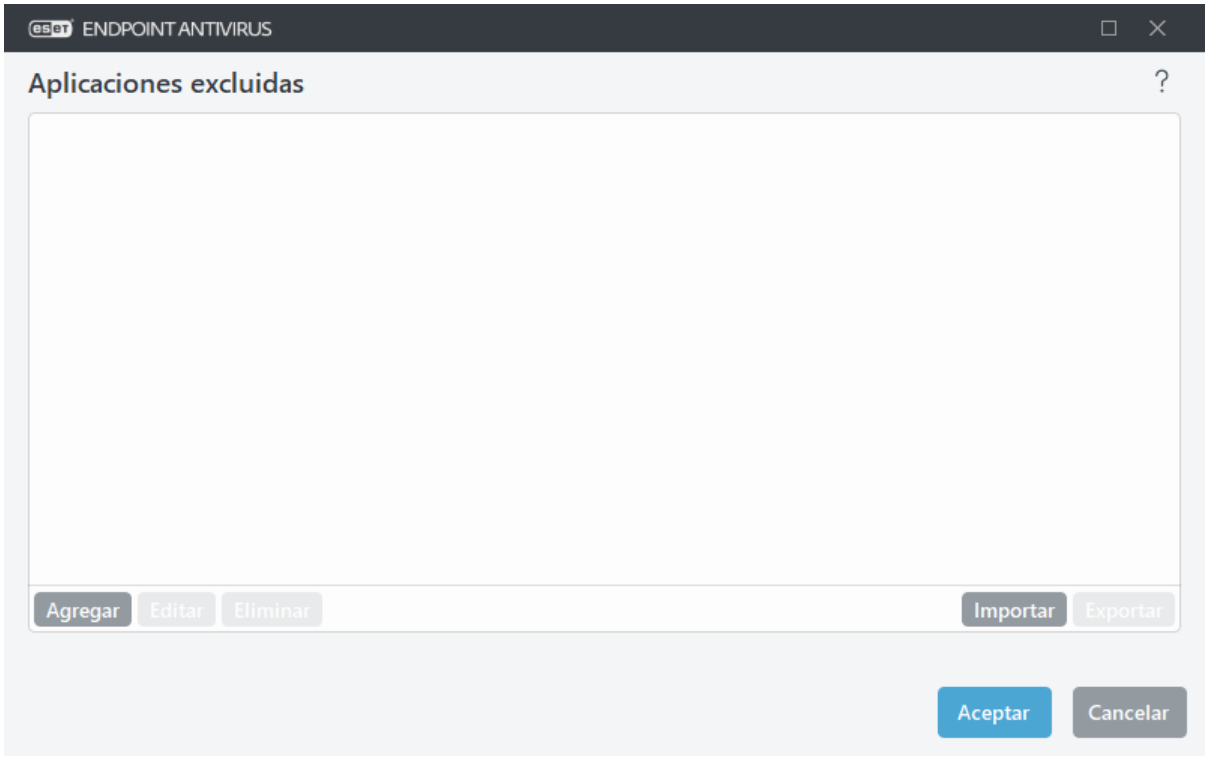
Aplicaciones excluidas

Para excluir el análisis de la comunicación para aplicaciones específicas, agréguelas a la lista. No se comprobará la presencia de amenazas en la comunicación HTTP(S)/POP3(S)/IMAP(S) de las aplicaciones seleccionadas. Se recomienda su uso únicamente en aplicaciones que no funcionen correctamente cuando se compruebe su comunicación.

Las aplicaciones y los servicios en ejecución estarán disponibles aquí de forma automática cuando haga clic en **Agregar**. Haga clic en **...** y navegue hasta una aplicación para agregar la exclusión manualmente.

Modificar: modifique las entradas seleccionadas de la lista.

Eliminado: elimina las entradas seleccionadas de la lista.



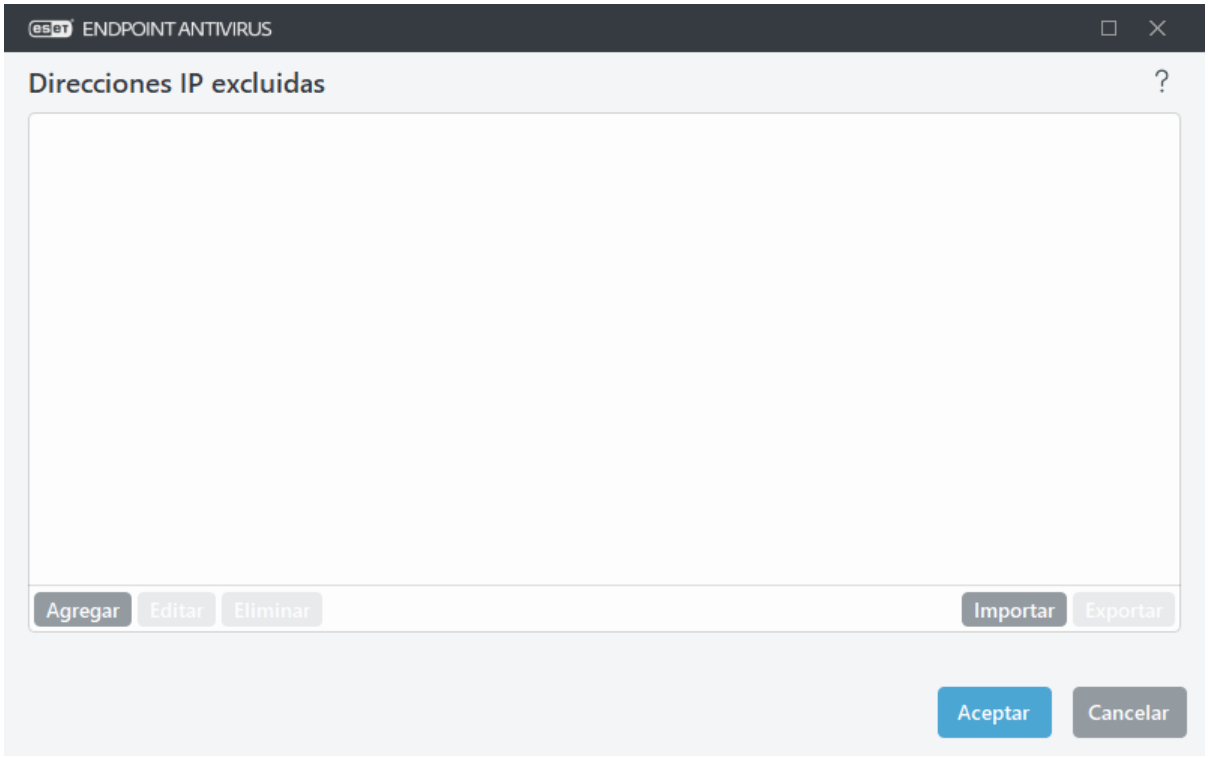
IP excluidas

Las entradas de la lista se excluirán del análisis. No se comprobará la presencia de amenazas en las comunicaciones HTTP(S)/POP3(S)/IMAP(S) entrantes y salientes de las direcciones seleccionadas. Esta opción se recomienda únicamente para direcciones que se sabe que son de confianza.

Agregar: haga clic para agregar una dirección IP, un intervalo de direcciones o una subred de un punto remoto al que se aplicará una regla.

Modificar: modifique las entradas seleccionadas de la lista.

Eliminado: elimina las entradas seleccionadas de la lista.



Ejemplos de direcciones IP

Agregar dirección IPv4:
Dirección única: agrega una dirección IP de un equipo individual (por ejemplo, *192.168.0.10*).
Rango de direcciones: especifique las direcciones IP inicial y final para delimitar el intervalo de direcciones de varios ordenadores (por ejemplo, *192.168.0.1-192.168.0.99*).
Subred: grupo de ordenadores definido por una dirección IP y una máscara. Por ejemplo, 255.255.255.0 es la máscara de red para la subred 192.168.1.0. Para excluir todo el tipo de subred en *192.168.1.0/24*.
Agregar dirección IPv6:
Dirección única: agrega la dirección IP de un ordenador individual (por ejemplo, *2001:718:1c01:16:214:22ff:fec9:ca5*).
Subred: grupo de ordenadores definido por una dirección IP y una máscara (por ejemplo, *2002:c0a8:6301:1::1/64*).

Protección de la casilla de correo

La integración de ESET Endpoint Antivirus con su buzón de correo aumenta el nivel de protección activa contra código malicioso en los mensajes de correo electrónico.

Para configurar la protección del buzón, abra Configuración avanzada > **Protecciones** > **Protección del cliente de correo electrónico** > **Protección del buzón**.

Activar protección del correo electrónico mediante complementos del cliente: cuando esta opción está desactivada, la protección mediante complementos del cliente de correo electrónico está desactivada.

Seleccione los mensajes de correo electrónico que desea analizar:

- **Correo electrónico recibido**
- **Correo electrónico enviado**
- **Correo electrónico leído**
- **Correo electrónico modificado**

Se recomienda mantener la opción **Activar protección del correo electrónico mediante complementos del cliente** activada. Aunque la integración no esté activada o no sea funcional, la comunicación por correo electrónico sigue estando protegida por Protección del transporte de correo electrónico (IMAP/IMAPS y POP3/POP3S).

Integraciones: le permite integrar la protección del buzón de correo en su cliente de correo electrónico. Consulte Integraciones para obtener más información.

Respuesta: le permite personalizar la gestión de los mensajes de spam. Consulte Respuesta para obtener más información.

Integraciones

La integración de ESET Endpoint Antivirus con su cliente de correo electrónico aumenta el nivel de protección activa contra código malicioso en los mensajes de correo electrónico. Si su cliente de correo electrónico es compatible, puede activar la integración en ESET Endpoint Antivirus. Cuando se integra en el cliente de correo electrónico, la barra de herramientas de ESET Endpoint Antivirus se inserta directamente en el cliente de correo electrónico, aumentando así la eficacia de la protección del correo electrónico. Para editar la configuración de integración, abra Configuración avanzada > **Protecciones** > **Protección del cliente de correo electrónico** > **Protección del buzón de correo** > **Integración**.

Integrar con Microsoft Outlook: actualmente, Microsoft Outlook es el único cliente de correo electrónico compatible. La protección de correo electrónico funciona como un plugin. La principal ventaja del complemento es el hecho de que es independiente del protocolo utilizado. Cuando el cliente de correo electrónico recibe un mensaje cifrado, este se descifra y se envía para el análisis de virus. Para ver una lista completa de versiones de Microsoft Outlook compatibles, consulte este artículo de la base de conocimiento de ESET.

Procesamiento avanzado del cliente de correo electrónico: procesa eventos de Outlook Messaging API (MAPI) adicionales: Objeto modificado (`fnevObjectModified`) y Objeto creado (`fnevObjectCreated`). Si el sistema funciona más lento de lo normal cuando trabaja con el cliente de correo electrónico, desactive esta opción.

Barra de herramientas de Microsoft Outlook

La protección de Microsoft Outlook funciona como un módulo de plugin. Una vez instalado ESET Endpoint Antivirus, esta barra de herramientas que contiene las opciones de la protección antivirus y el se agrega a Microsoft Outlook:

ESET Endpoint Antivirus: haga doble clic en el icono para abrir la ventana principal de ESET Endpoint Antivirus.

Analizar de nuevo los mensajes: le permite iniciar la comprobación del correo electrónico de forma manual. Puede especificar los mensajes que se comprobarán y activar un nuevo análisis del correo recibido. Para obtener más información, consulte Protección del buzón de correo.

Configuración del análisis: muestra las opciones de configuración de Protección del buzón de correo.

Cuadro de diálogo de confirmación

Esta notificación sirve para comprobar que el usuario realmente desea realizar la acción seleccionada, que debería eliminar los posibles errores.

Por otra parte, el cuadro de diálogo también ofrece la posibilidad de desactivar las confirmaciones.

Analizar de nuevo los mensajes

La barra de herramientas de ESET Endpoint Antivirus integrada en los clientes de correo electrónico permite a los usuarios especificar varias opciones de análisis del correo electrónico. La opción **Analizar de nuevo los mensajes** ofrece dos modos de análisis:

Todos los mensajes de la carpeta actual: analiza los mensajes de la carpeta que se muestra en ese momento.

Solo los mensajes seleccionados: analiza únicamente los mensajes marcados por el usuario.

La casilla de verificación **Volver a analizar los mensajes ya analizados** proporciona una opción para ejecutar otro análisis en mensajes ya analizados.

Respuesta

Según los resultados del análisis de mensajes, ESET Endpoint Antivirus puede mover los mensajes analizados o agregar texto personalizado al asunto. Puede configurar estas opciones en Configuración avanzada > **Protecciones** > **Protección del cliente de correo electrónico** > **Protección del buzón de correo** > **Respuesta**.

Si hay un mensaje que contiene detección, de forma predeterminada, ESET Endpoint Antivirus intenta desinfectar el mensaje. Si el mensaje no se puede desinfectar, puede elegir una **Acción a emprender si no es posible la desinfección**:

- **Sin acciones**: si esta opción está activada, el programa identificará los archivos adjuntos infectados, pero dejará los mensajes sin realizar ninguna acción.
- **Eliminar mensajes**: el programa informará al usuario sobre las amenazas y eliminará el mensaje.
- **Mover el correo electrónico a la carpeta de elementos eliminados**: los mensajes infectados se moverán automáticamente a la carpeta Elementos eliminados.
- **Mover mensajes a la carpeta** (acción predeterminada): los mensajes de correo electrónico infectados se moverán automáticamente a la carpeta especificada.

Carpeta: especifique la carpeta personalizada a la que desea mover el correo infectado que se detecte.

Después de analizar un mensaje de correo electrónico, se puede adjuntar al mensaje una notificación del análisis. Puede elegir entre las opciones **Notificar en los mensajes recibidos y leídos** o **Notificar en los mensajes enviados**. Tenga en cuenta que en ocasiones puntuales es posible que los mensajes con etiqueta se omitan en mensajes HTML problemáticos o que hayan sido falsificados por código malicioso. Los mensajes con etiqueta se pueden agregar a los mensajes recibidos y leídos, a los mensajes enviados o a ambos. Están disponibles las opciones siguientes:

- **Nunca**: no se agregará ningún mensaje de etiqueta.

- **Cuando se produce una detección**: únicamente se marcarán como analizados los mensajes que contengan software malicioso (opción predeterminada).
- **A todo el correo electrónico cuando se analiza**: el programa agregará un mensaje a todo el correo analizado.

Actualizar asunto de los correos electrónicos recibidos y leídos/Actualizar asunto de los correos electrónicos enviados: active esta opción para agregar texto personalizado especificado a continuación al mensaje.

Texto que se agrega al asunto de los correos electrónicos detectados: edite esta plantilla si desea modificar el formato de prefijo del asunto de un mensaje de correo electrónico infectado. Esta función sustituye el asunto del mensaje "Hello" por el siguiente formato: "[detection %DETECTIONNAME%] Hello". La variable %DETECTIONNAME% representa la amenaza detectada.

ThreatSense

ThreatSense consta de muchos métodos complejos de detección de amenazas. Esta tecnología es proactiva, lo que significa que también proporciona protección durante la fase inicial de expansión de una nueva amenaza. Utiliza una combinación de análisis de código, emulación de código, firmas genéricas y firmas de virus que funcionan de forma conjunta para mejorar en gran medida la seguridad del sistema. El motor de análisis es capaz de controlar varios flujos de datos de forma simultánea, de manera que maximiza la eficacia y la velocidad de detección. Además, la tecnología ThreatSense elimina eficazmente los programas peligrosos (rootkits).

Las opciones de configuración del motor de ThreatSense le permiten especificar varios parámetros de análisis:

- Los tipos de archivos y extensiones que se deben analizar
- La combinación de diferentes métodos de detección.
- Los niveles de desinfección, etc.

Para acceder a la ventana de configuración, haga clic en **ThreatSense** en la ventana Configuración avanzada de cualquier módulo que utilice la tecnología ThreatSense (consulte más abajo). Es posible que cada escenario de seguridad requiera una configuración diferente. Con esto en mente, ThreatSense se puede configurar individualmente para los siguientes módulos de protección:

- Protección del sistema de archivos en tiempo real
- Análisis de estado inactivo
- Análisis en el inicio
- Protección de documentos
- Protección del cliente de correo electrónico
- Protección del tráfico de Internet
- Análisis del ordenador

Los parámetros de ThreatSense están altamente optimizados para cada módulo y su modificación puede afectar al funcionamiento del sistema de forma significativa. Por ejemplo, la modificación de los parámetros para que siempre analicen empaquetadores de ejecución en tiempo real o la activación de la heurística avanzada en el módulo de protección del sistema de archivos en tiempo real podrían ralentizar el sistema (normalmente, con estos métodos solo se analizan los archivos recién creados). Se recomienda que no modifique los parámetros predeterminados de ThreatSense para ninguno de los módulos, a excepción de Análisis del ordenador.

Objetos a analizar

En esta sección se pueden definir los componentes y archivos del ordenador que se analizarán en busca de amenazas.

Memoria operativa: busca amenazas que ataquen a la memoria operativa del sistema.

Sectores de inicio/UEFI: analiza los sectores de inicio para detectar malware en el registro de inicio principal. Lea más sobre la UEFI en el glosario.

Archivos de correo: el programa admite las siguientes extensiones: DBX (Outlook Express) y EML.

Archivos comprimidos: el programa es compatible con las extensiones ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE y muchas más.

Archivos comprimidos autoextraíbles: los archivos comprimidos autoextraíbles (SFX) son archivos comprimidos que pueden extraerse por sí solos.

Empaquetadores en tiempo de ejecución: después de su ejecución, los empaquetadores en tiempo de ejecución (a diferencia de los archivos estándar) se descomprimen en la memoria. Además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FSG, etc.), el módulo de análisis permite reconocer varios tipos de empaquetadores adicionales gracias a la emulación de códigos.

Opciones de análisis

Seleccione los métodos empleados al analizar el sistema en busca de infiltraciones. Están disponibles las opciones siguientes:

Heurística: la heurística es un algoritmo que analiza la actividad (maliciosa) de los programas. La principal ventaja de esta tecnología es la habilidad para identificar software malicioso que no existía o que el motor de detección anterior no conocía. Su desventaja es la probabilidad (muy pequeña) de falsas alarmas.

Heurística avanzada/ADN inteligentes: la heurística avanzada es un algoritmo heurístico único desarrollado por ESET optimizado para detectar gusanos informáticos y troyanos escritos en lenguajes de programación de alto nivel. El uso de la heurística avanzada mejora en gran medida la detección de amenazas por parte de los productos de ESET. Las firmas pueden detectar e identificar virus de manera fiable. Gracias al sistema de actualización automática, las nuevas firmas están disponibles en cuestión de horas cuando se descubre una amenaza. Su desventaja es que únicamente detectan los virus que conocen (o versiones ligeramente modificadas).

Desinfección

La configuración de desinfección determinan el comportamiento de ESET Endpoint Antivirus durante la desinfección de objetos.

Exclusiones

Una extensión es una parte del nombre de archivo delimitada por un punto. Una extensión define el tipo y el contenido de un archivo. En esta sección de la configuración de ThreatSense, es posible definir los tipos de archivos que se desean analizar.

Otros

Al configurar motor ThreatSense para un análisis del ordenador a petición, dispone también de las siguientes opciones en la sección **Otros**:

Analizar secuencias de datos alternativas (ADS): las secuencias de datos alternativos utilizadas por el sistema de archivos NTFS son asociaciones de carpetas y archivos que no se detectan con técnicas de análisis ordinarias. Muchas amenazas intentan evitar los sistemas de detección haciéndose pasar por flujos de datos alternativos.

Realizar análisis en segundo plano con baja prioridad: cada secuencia de análisis consume una cantidad determinada de recursos del sistema. Si se trabaja con programas cuyo consumo de recursos constituye una carga importante para el sistema, es posible activar el análisis en segundo plano con baja prioridad y reservar los recursos para las aplicaciones.

Registrar todos los objetos: el registro del análisis mostrará todos los archivos analizados en archivos comprimidos de autoextracción, incluso los no infectados (puede generar muchos datos de registro del análisis y aumentar el tamaño del archivo de registro del análisis).

Activar la optimización inteligente: si la opción Optimización inteligente está activada, se utiliza la configuración más óptima para garantizar el nivel de análisis más eficaz y, al mismo tiempo, mantener la máxima velocidad de análisis posible. Los diferentes módulos de protección analizan de forma inteligente, con métodos de análisis distintos y aplicados a tipos de archivo específicos. Si la optimización inteligente está desactivada, solamente se aplica la configuración definida por el usuario en el núcleo ThreatSense de los módulos donde se realiza el análisis.

Preservar el último acceso con su fecha y hora: seleccione esta opción para guardar la hora de acceso original de los archivos analizados, en lugar de actualizarlos (por ejemplo, para utilizar con sistemas de copia de seguridad de datos).

Límites

En la sección Límites se puede especificar el tamaño máximo de los objetos y los niveles de archivos anidados que se analizarán:

Configuración de los objetos

Tamaño máximo del objeto: define el tamaño máximo de los objetos que se analizarán. El módulo antivirus analizará solo los objetos que tengan un tamaño menor que el especificado. Esta opción solo deben cambiarla usuarios avanzados que tengan motivos específicos para excluir del análisis objetos más grandes. Valor predeterminado: ilimitado.

Tiempo máximo de análisis para el objeto (s): define el valor de tiempo máximo para el análisis de los archivos de un objeto contenedor (por ejemplo, un archivo comprimido RAR/ZIP o un mensaje de correo electrónico con varios archivos adjuntos). Este ajuste no se aplica a los archivos independientes. Si se ha introducido un valor definido por el usuario y ha transcurrido el tiempo, el análisis se detendrá lo antes posible, independientemente de si ha finalizado el análisis de cada archivo del objeto contenedor. En el caso de un archivo comprimido con archivos grandes, el análisis se detendrá en cuanto se extraiga un archivo del archivo comprimido (por ejemplo, si la variable definida por el usuario es de 3 segundos, pero la extracción de un archivo tarda 5 segundos). El resto de archivos del archivo comprimido no se analizarán una vez transcurrido el tiempo. Para limitar el tiempo de análisis, incluido el de los archivos comprimidos más grandes, utilice los ajustes **Tamaño máximo del objeto** y **Tamaño máx. de archivo en el archivo comprimido** (no se recomienda debido a posibles riesgos de seguridad).

Valor predeterminado: ilimitado.

Configuración del análisis de archivos comprimidos

Nivel de anidamiento de archivos: especifica el nivel máximo de análisis de archivos. Valor predeterminado: 10.

Tamaño máx. de archivo en el archivo comprimido: esta opción permite especificar el tamaño máximo de archivo de los archivos contenidos en archivos comprimidos (una vez extraídos) que se van a analizar. El valor máximo es 3 GB.

> No se recomienda cambiar los valores predeterminados; en circunstancias normales, no debería haber motivo para hacerlo.

Protección del acceso a la Web

La protección de acceso a la web le permite configurar opciones avanzadas del módulo Protección de internet. Las siguientes opciones están disponibles en Configuración avanzada > **Protecciones** > **Protección de acceso a la web** > **Protección de acceso a la web**:

Activar la protección de acceso a la web: cuando esta opción está desactivada, no se ejecutan Protección de acceso a la web ni Protección antiphishing.

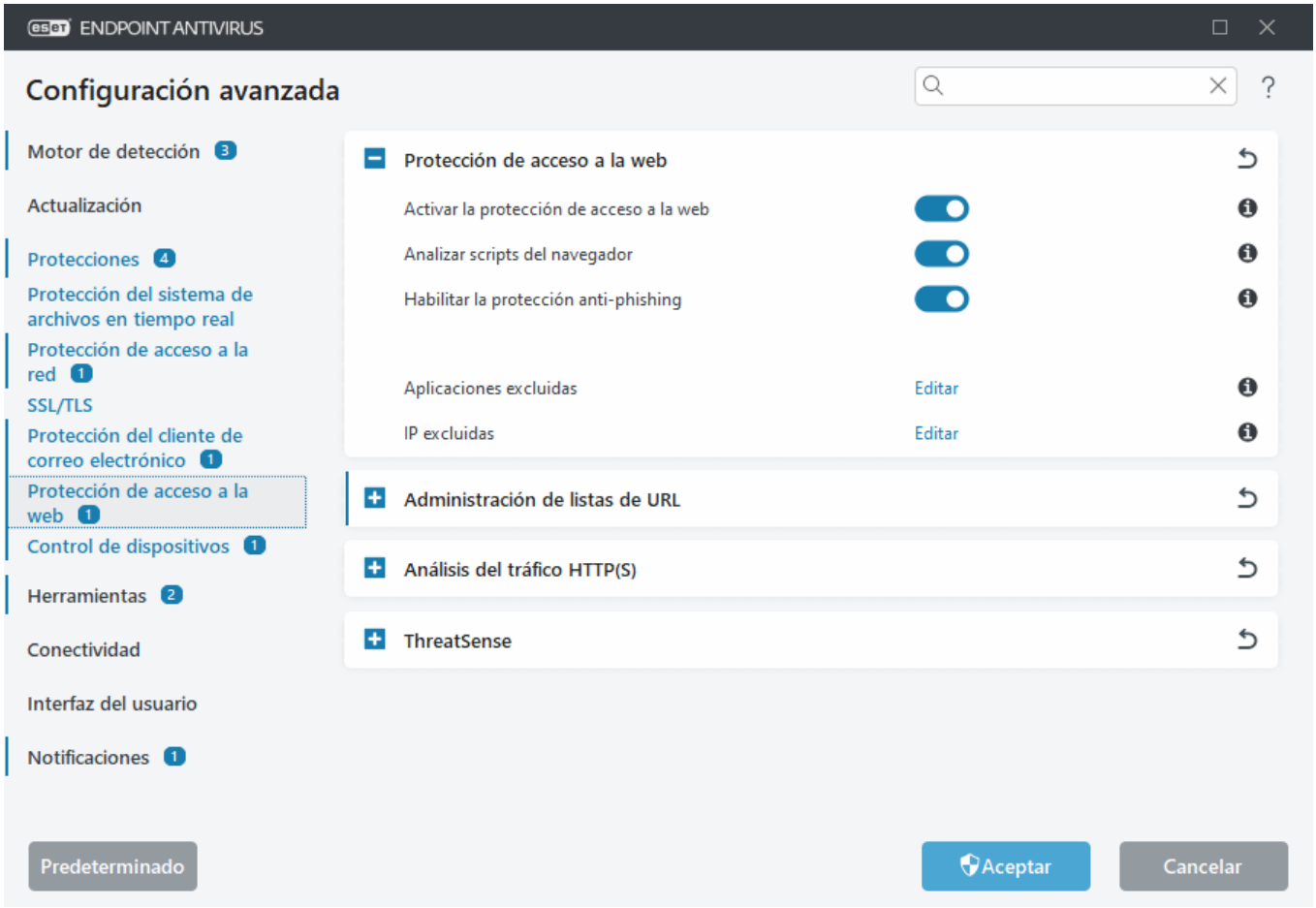
> Le recomendamos encarecidamente que deje activada la Protección de acceso a la web y no excluya ninguna aplicación o dirección IP de forma predeterminada.

Analizar scripts del navegador: cuando esta opción activada, el motor de detección comprueba todos los programas JavaScript ejecutados por los navegadores web.

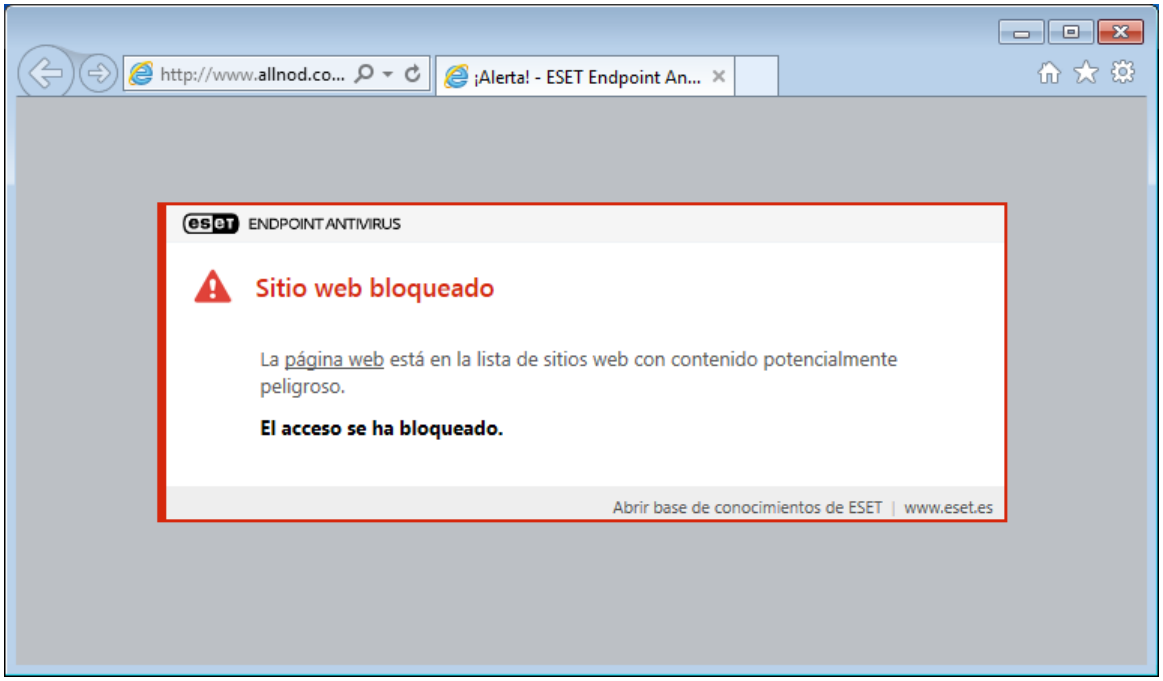
Activar protección anti-phishing: cuando esta opción activada, las páginas web de phishing se bloquean. Consulte Protección antiphishing para obtener más información.

Aplicaciones excluidas: permite excluir aplicaciones específicas del análisis de Protección de acceso a la web. Útil cuando la protección de acceso web causa problemas de compatibilidad.

IP excluidas: permite excluir direcciones remotas específicas del análisis de la protección de acceso a la Web. Útil cuando la protección de acceso web causa problemas de compatibilidad.



Protección de acceso a la web mostrará el siguiente mensaje en su navegador cuando el sitio web esté bloqueado:



Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:
- Unblock a safe website on an individual workstation in ESET Endpoint Antivirus

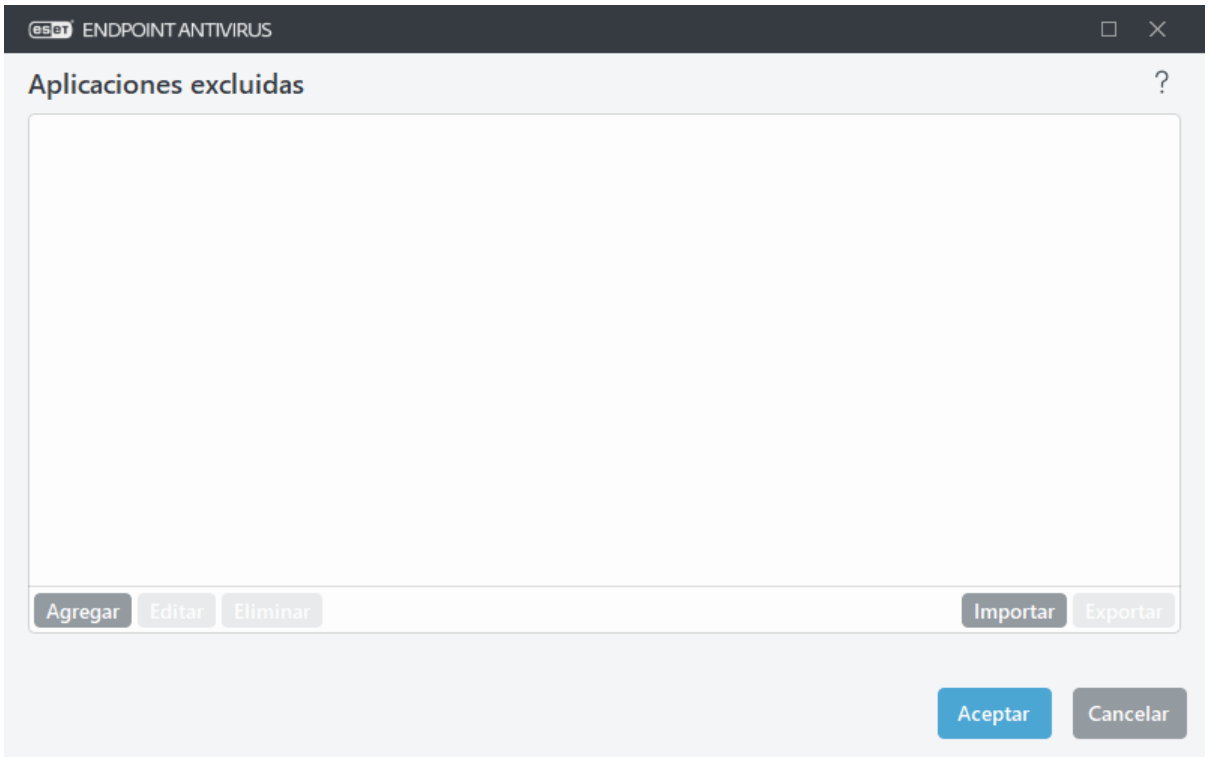
Aplicaciones excluidas

Para excluir el análisis de la comunicación para aplicaciones específicas, agréguelas a la lista. No se comprobará la presencia de amenazas en la comunicación HTTP(S)/POP3(S)/IMAP(S) de las aplicaciones seleccionadas. Se recomienda su uso únicamente en aplicaciones que no funcionen correctamente cuando se compruebe su comunicación.

Las aplicaciones y los servicios en ejecución estarán disponibles aquí de forma automática cuando haga clic en **Agregar**. Haga clic en **...** y navegue hasta una aplicación para agregar la exclusión manualmente.

Modificar: modifique las entradas seleccionadas de la lista.

Eliminado: elimina las entradas seleccionadas de la lista.



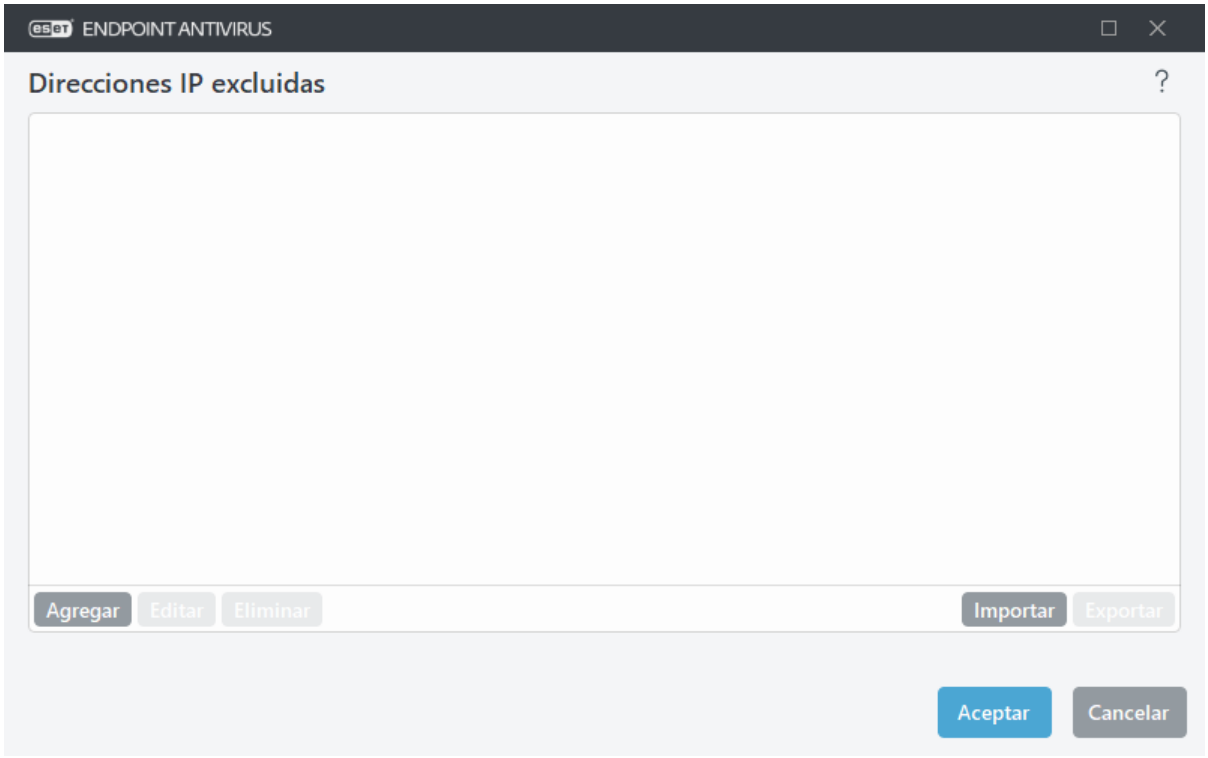
IP excluidas

Las entradas de la lista se excluirán del análisis. No se comprobará la presencia de amenazas en las comunicaciones HTTP(S)/POP3(S)/IMAP(S) entrantes y salientes de las direcciones seleccionadas. Esta opción se recomienda únicamente para direcciones que se sabe que son de confianza.

Agregar: haga clic para agregar una dirección IP, un intervalo de direcciones o una subred de un punto remoto al que se aplicará una regla.

Modificar: modifique las entradas seleccionadas de la lista.

Eliminado: elimina las entradas seleccionadas de la lista.



Ejemplos de direcciones IP

Agregar dirección IPv4:
Dirección única: agrega una dirección IP de un equipo individual (por ejemplo, *192.168.0.10*).
Rango de direcciones: especifique las direcciones IP inicial y final para delimitar el intervalo de direcciones de varios ordenadores (por ejemplo, *192.168.0.1-192.168.0.99*).
Subred: grupo de ordenadores definido por una dirección IP y una máscara. Por ejemplo, 255.255.255.0 es la máscara de red para la subred 192.168.1.0. Para excluir todo el tipo de subred en *192.168.1.0/24*.
Agregar dirección IPv6:
Dirección única: agrega la dirección IP de un ordenador individual (por ejemplo, *2001:718:1c01:16:214:22ff:fec9:ca5*).
Subred: grupo de ordenadores definido por una dirección IP y una máscara (por ejemplo, *2002:c0a8:6301:1::1/64*).

Administración de la lista de URL

La **administración de listas de URL** en Configuración avanzada > **Protecciones** > **Protección de acceso web** le permite especificar las direcciones HTTP para bloquear, permitir o excluir del análisis de contenido.

SSL/TLS debe estar habilitado si desea filtrar direcciones HTTPS además de HTTP. Si no lo hace, solo se agregarán los dominios de los sitios HTTPS que haya visitado, pero no la URL completa.

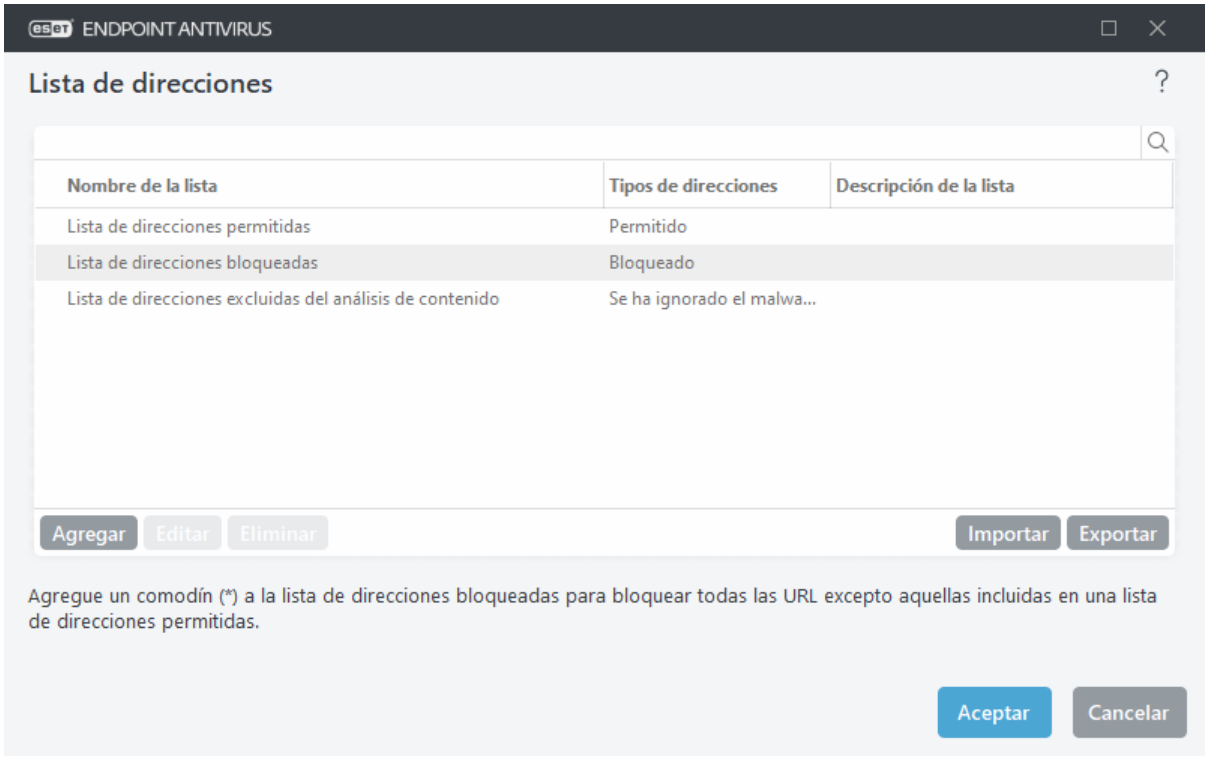
No podrá acceder a los sitios web de **Lista de direcciones bloqueadas** a menos que también se incluyan en **Lista de direcciones permitidas**. Cuando se acceda a sitios web que se encuentran en **Lista de direcciones excluidas del análisis de contenido**, dichos sitios web no se analizarán en busca de código malicioso.

Si desea bloquear todas las direcciones HTTP menos las incluidas en la **Lista de direcciones permitidas** activa, agregue el símbolo * a la **Lista de direcciones bloqueadas** activa.

No se pueden utilizar los símbolos especiales * (asterisco) y ? (signo de interrogación) en listas. El asterisco sustituye a cualquier cadena de caracteres y el signo de interrogación, a cualquier símbolo. Preste atención al

especificar direcciones excluidas, ya que la lista solo debe contener direcciones seguras y de confianza. Del mismo modo, es necesario asegurarse de que los símbolos * y ? se utilizan correctamente en esta lista. Consulte Agregar dirección HTTP/máscara de dominio para obtener información sobre cómo detectar un dominio completo con todos sus subdominios de forma segura. Para activar una lista, seleccione **Lista activa**. Si desea recibir una notificación cuando se introduzca una dirección de la lista actual, seleccione **Notificar al aplicar**.

> **Direcciones en las que confía ESET**
>
> Si la opción **No analizar el tráfico con dominios en los que ESET confía** está activada en SSL/TLS, los dominios de la lista blanca administrada por ESET no se verán afectados por la configuración de administración de la lista de URL.



Elementos de control

Agregar: crea una lista nueva que se suma a las predefinidas. Esta opción puede ser útil si se desea dividir varios grupos de direcciones de forma lógica. Por ejemplo, una lista de direcciones bloqueadas puede contener direcciones de una lista negra pública externa, mientras que otra contiene su propia lista negra. Esto facilita la actualización de la lista externa sin que la suya se vea afectada.

Modificar: modifica las listas existentes. Utilice esta opción para agregar o quitar direcciones.

Eliminar: elimina las listas existentes. Esta opción solo está disponible en listas creadas con **Agregar**, no en las listas predeterminadas.

Lista de direcciones

En esta sección podrá indicar las listas de direcciones HTTP(S) que desea bloquear, permitir o excluir del análisis.

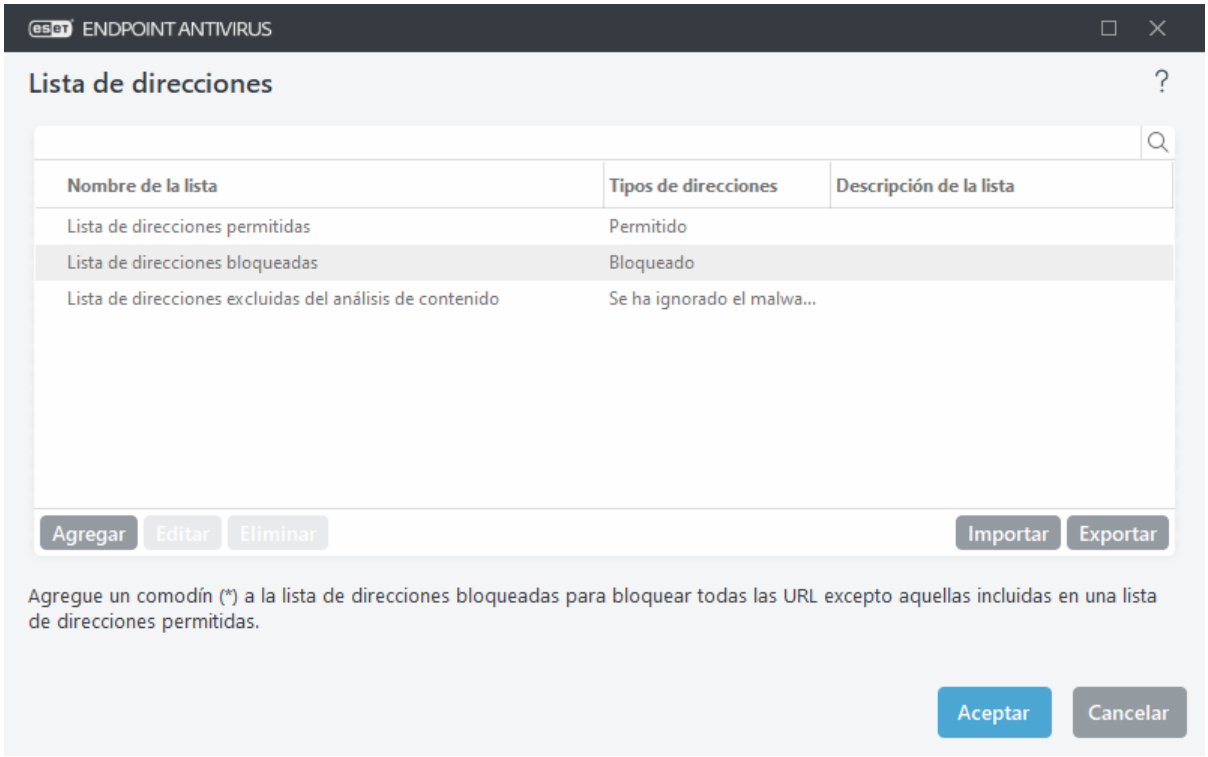
De forma predeterminada, están disponibles estas tres listas:

- **Lista de direcciones excluidas del análisis de contenido**: no se comprobará la existencia de código

malicioso en ninguna de las direcciones agregadas a esta lista.

- **Lista de direcciones permitidas**: si está activada la opción Permitir el acceso solo a las direcciones HTTP de la lista de direcciones permitidas y la lista de direcciones bloqueadas contiene un * (coincidir con todo), el usuario podrá acceder únicamente a las direcciones especificadas en esta lista. Las direcciones de esta lista estarán autorizadas incluso si se incluyen en la lista de direcciones bloqueadas.
- **Lista de direcciones bloqueadas**: el usuario no tendrá acceso a las direcciones incluidas en esta lista a menos que aparezcan también en la lista de direcciones permitidas.

Haga clic en **Agregar** para crear una lista nueva. Para eliminar las listas seleccionadas, haga clic en **Eliminar**.



Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:
- Unblock a safe website on an individual workstation in ESET Endpoint Antivirus

Si desea obtener más información, consulte Administración de direcciones URL.

Creación de nueva lista de direcciones

Este cuadro de diálogo permite configurar una nueva lista de máscaras o direcciones URL que se bloquearán, permitirán o excluirán de la comprobación.

Puede configurar las siguientes opciones:

Tipo de lista de direcciones: están disponibles tres tipos de listas:

- **Excluido de la comprobación**: no se comprobará la existencia de código malicioso en ninguna de las direcciones agregadas a esta lista.
- **Bloqueado**: se bloqueará el acceso a las direcciones especificadas en esta lista.
- **Permitido**: se permitirá el acceso a las direcciones especificadas en esta lista. Las direcciones de esta lista se permitirán aunque estén incluidas en la lista de direcciones bloqueadas.

Nombre de la lista: especifique el nombre de la lista. Este campo no está disponible cuando se edita una única lista predefinida.

Descripción de la lista: escriba una breve descripción de la lista (opcional). Este campo no está disponible cuando se edita una única lista predefinida.

Para activar una lista, seleccione **Lista activa** junto a ella. Si desea recibir una notificación cuando se utilice una lista específica al acceder a sitios web, seleccione **Notificar al aplicar**. Por ejemplo, recibirá una notificación si un sitio web se bloquea o se permite por estar incluido en la lista de direcciones bloqueadas o permitidas. La notificación contendrá el nombre de la lista.

Registro de severidad: seleccione el registro de severidad en el menú desplegable. El ESET PROTECT puede recopilar los registros con detalle de advertencia.

Los niveles de registro Información y Advertencia solo están disponibles para las reglas que contienen al menos dos componentes sin comodines dentro del dominio. Por ejemplo:
- *.domain.com/*
- *www.domain.com/*

Elementos de control

Agregar: agregue a la lista una dirección URL nueva (introduzca varios valores con un separador).

Modificar: modifica la dirección existente en la lista. Esta opción solo estará disponible para las direcciones creadas con **Agregar**.

Quitar: elimina las direcciones existentes de la lista. Esta opción solo estará disponible para las direcciones creadas con **Agregar**.

Importar: importe un archivo con direcciones URL separadas por un salto de línea (por ejemplo, un archivo *.txt con codificación UTF-8).

Para obtener más información, consulte el capítulo Cómo agregar una máscara URL.

Cómo agregar una máscara URL

Consulte las instrucciones de este cuadro de diálogo antes de escribir la dirección/máscara de dominio que desee.

ESET Endpoint Antivirus permite al usuario bloquear el acceso a determinados sitios web para evitar que el navegador de Internet muestre su contenido. También puede especificar las direcciones que no se deben comprobar. Si no se conoce el nombre completo del servidor remoto o si el usuario desea especificar un grupo completo de servidores remotos, se pueden utilizar máscaras para identificar dicho grupo. Las máscaras incluyen los símbolos "?" y "*":

- Utilice ? para sustituir un símbolo.
- Utilice * para sustituir una cadena de texto.

Por ejemplo, *.c?m sirve para todas las direcciones cuya última parte comienza con la letra c, termina con la letra m y contiene un símbolo desconocido entre ellas (.com, .cam, etc.).

Por ejemplo, la máscara *x? incluye todas las direcciones que tengan el carácter "x" en cualquier posición menos

al final. Para incluir todo el dominio, escríbalo con el formato **.domain.com/**. Especificar el prefijo del protocolo *http://*, *https://* en la máscara es opcional. Si se omite, la máscara funcionará con cualquier protocolo. Las secuencias que empiezan con "*." reciben un trato especial si se utilizan al principio de un nombre de dominio. En primer lugar, el comodín * no coincide con el carácter de barra ("/") en este caso. Con esto se pretende evitar que se burle la máscara, por ejemplo, la máscara **.domain.com* no coincidirá con *http://anydomain.com/anypath#.domain.com* (este sufijo se puede añadir a cualquier URL sin que la descarga se vea afectada). En segundo lugar, la secuencia "*." también se corresponde con una cadena vacía en este caso especial. El objetivo es permitir la detección de un dominio completo, incluidos todos sus subdominios, con una sola máscara. Por ejemplo, la máscara **.domain.com* también coincide con *http://domain.com*. No sería correcto utilizar **domain.com*, ya que esta cadena también detectaría *http://anotherdomain.com*.

Los niveles de registro Información y Advertencia solo están disponibles para las reglas que contienen al menos dos componentes sin comodines dentro del dominio. Por ejemplo:
- *.domain.com/*
- *www.domain.com/*

Exploración del tráfico HTTP(S)

De forma predeterminada, ESET Endpoint Antivirus está configurado para analizar el tráfico HTTP y HTTPS que utilizan los navegadores de Internet y otras aplicaciones. Debe deshabilitar el análisis de tráfico solo si tiene problemas con un software de terceros y desea saber si el problema lo causa ESET Endpoint Antivirus.

Activar análisis del tráfico HTTP: El tráfico HTTP se supervisa siempre en todos los puertos y para todas las aplicaciones.

Habilite el análisis de tráfico de HTTPS: el tráfico de HTTPS utiliza un canal cifrado para transferir información entre el servidor y el cliente. ESET Endpoint Antivirus comprueba la comunicación mediante los protocolos SSL (capa de sockets seguros) y TLS (seguridad de la capa de transporte). El programa solo analizará el tráfico de los puertos definidos en **Puertos utilizados por el protocolo HTTPS**, independientemente de la versión del sistema operativo (puede agregar puertos a los predefinidos 443 y 0-65535).

ThreatSense

ThreatSense consta de muchos métodos complejos de detección de amenazas. Esta tecnología es proactiva, lo que significa que también proporciona protección durante la fase inicial de expansión de una nueva amenaza. Utiliza una combinación de análisis de código, emulación de código, firmas genéricas y firmas de virus que funcionan de forma conjunta para mejorar en gran medida la seguridad del sistema. El motor de análisis es capaz de controlar varios flujos de datos de forma simultánea, de manera que maximiza la eficacia y la velocidad de detección. Además, la tecnología ThreatSense elimina eficazmente los programas peligrosos (rootkits).

Las opciones de configuración del motor de ThreatSense le permiten especificar varios parámetros de análisis:

- Los tipos de archivos y extensiones que se deben analizar
- La combinación de diferentes métodos de detección.
- Los niveles de desinfección, etc.

Para acceder a la ventana de configuración, haga clic en **ThreatSense** en la ventana Configuración avanzada de cualquier módulo que utilice la tecnología ThreatSense (consulte más abajo). Es posible que cada escenario de seguridad requiera una configuración diferente. Con esto en mente, ThreatSense se puede configurar individualmente para los siguientes módulos de protección:

- Protección del sistema de archivos en tiempo real
- Análisis de estado inactivo
- Análisis en el inicio
- Protección de documentos
- Protección del cliente de correo electrónico
- Protección del tráfico de Internet
- Análisis del ordenador

Los parámetros de ThreatSense están altamente optimizados para cada módulo y su modificación puede afectar al funcionamiento del sistema de forma significativa. Por ejemplo, la modificación de los parámetros para que siempre analicen empaquetadores de ejecución en tiempo real o la activación de la heurística avanzada en el módulo de protección del sistema de archivos en tiempo real podrían ralentizar el sistema (normalmente, con estos métodos solo se analizan los archivos recién creados). Se recomienda que no modifique los parámetros predeterminados de ThreatSense para ninguno de los módulos, a excepción de Análisis del ordenador.

Objetos a analizar

En esta sección se pueden definir los componentes y archivos del ordenador que se analizarán en busca de amenazas.

Memoria operativa: busca amenazas que ataquen a la memoria operativa del sistema.

Sectores de inicio/UEFI: analiza los sectores de inicio para detectar malware en el registro de inicio principal. Lea más sobre la UEFI en el glosario.

Archivos de correo: el programa admite las siguientes extensiones: DBX (Outlook Express) y EML.

Archivos comprimidos: el programa es compatible con las extensiones ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE y muchas más.

Archivos comprimidos autoextraíbles: los archivos comprimidos autoextraíbles (SFX) son archivos comprimidos que pueden extraerse por sí solos.

Empaquetadores en tiempo de ejecución: después de su ejecución, los empaquetadores en tiempo de ejecución (a diferencia de los archivos estándar) se descomprimen en la memoria. Además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FSG, etc.), el módulo de análisis permite reconocer varios tipos de empaquetadores adicionales gracias a la emulación de códigos.

Opciones de análisis

Seleccione los métodos empleados al analizar el sistema en busca de infiltraciones. Están disponibles las opciones siguientes:

Heurística: la heurística es un algoritmo que analiza la actividad (maliciosa) de los programas. La principal ventaja de esta tecnología es la habilidad para identificar software malicioso que no existía o que el motor de detección anterior no conocía. Su desventaja es la probabilidad (muy pequeña) de falsas alarmas.

Heurística avanzada/ADN inteligentes: la heurística avanzada es un algoritmo heurístico único desarrollado por ESET optimizado para detectar gusanos informáticos y troyanos escritos en lenguajes de programación de alto nivel. El uso de la heurística avanzada mejora en gran medida la detección de amenazas por parte de los productos de ESET. Las firmas pueden detectar e identificar virus de manera fiable. Gracias al sistema de actualización automática, las nuevas firmas están disponibles en cuestión de horas cuando se descubre una

amenaza. Su desventaja es que únicamente detectan los virus que conocen (o versiones ligeramente modificadas).

Desinfección

La configuración de desinfección determinan el comportamiento de ESET Endpoint Antivirus durante la desinfección de objetos.

Exclusiones

Una extensión es una parte del nombre de archivo delimitada por un punto. Una extensión define el tipo y el contenido de un archivo. En esta sección de la configuración de ThreatSense, es posible definir los tipos de archivos que se desean analizar.

Otros

Al configurar motor ThreatSense para un análisis del ordenador a petición, dispone también de las siguientes opciones en la sección **Otros**:

Analizar secuencias de datos alternativas (ADS): las secuencias de datos alternativos utilizadas por el sistema de archivos NTFS son asociaciones de carpetas y archivos que no se detectan con técnicas de análisis ordinarias. Muchas amenazas intentan evitar los sistemas de detección haciéndose pasar por flujos de datos alternativos.

Realizar análisis en segundo plano con baja prioridad: cada secuencia de análisis consume una cantidad determinada de recursos del sistema. Si se trabaja con programas cuyo consumo de recursos constituye una carga importante para el sistema, es posible activar el análisis en segundo plano con baja prioridad y reservar los recursos para las aplicaciones.

Registrar todos los objetos: el registro del análisis mostrará todos los archivos analizados en archivos comprimidos de autoextracción, incluso los no infectados (puede generar muchos datos de registro del análisis y aumentar el tamaño del archivo de registro del análisis).

Activar la optimización inteligente: si la opción Optimización inteligente está activada, se utiliza la configuración más óptima para garantizar el nivel de análisis más eficaz y, al mismo tiempo, mantener la máxima velocidad de análisis posible. Los diferentes módulos de protección analizan de forma inteligente, con métodos de análisis distintos y aplicados a tipos de archivo específicos. Si la optimización inteligente está desactivada, solamente se aplica la configuración definida por el usuario en el núcleo ThreatSense de los módulos donde se realiza el análisis.

Preservar el último acceso con su fecha y hora: seleccione esta opción para guardar la hora de acceso original de los archivos analizados, en lugar de actualizarlos (por ejemplo, para utilizar con sistemas de copia de seguridad de datos).

Límites

En la sección Límites se puede especificar el tamaño máximo de los objetos y los niveles de archivos anidados que se analizarán:

Configuración de los objetos

Tamaño máximo del objeto: define el tamaño máximo de los objetos que se analizarán. El módulo antivirus analizará solo los objetos que tengan un tamaño menor que el especificado. Esta opción solo deben cambiarla usuarios avanzados que tengan motivos específicos para excluir del análisis objetos más grandes. Valor predeterminado: ilimitado.

Tiempo máximo de análisis para el objeto (s): define el valor de tiempo máximo para el análisis de los archivos de un objeto contenedor (por ejemplo, un archivo comprimido RAR/ZIP o un mensaje de correo electrónico con varios archivos adjuntos). Este ajuste no se aplica a los archivos independientes. Si se ha introducido un valor definido por el usuario y ha transcurrido el tiempo, el análisis se detendrá lo antes posible, independientemente de si ha finalizado el análisis de cada archivo del objeto contenedor. En el caso de un archivo comprimido con archivos grandes, el análisis se detendrá en cuanto se extraiga un archivo del archivo comprimido (por ejemplo, si la variable definida por el usuario es de 3 segundos, pero la extracción de un archivo tarda 5 segundos). El resto de archivos del archivo comprimido no se analizarán una vez transcurrido el tiempo. Para limitar el tiempo de análisis, incluido el de los archivos comprimidos más grandes, utilice los ajustes **Tamaño máximo del objeto** y **Tamaño máx. de archivo en el archivo comprimido** (no se recomienda debido a posibles riesgos de seguridad). Valor predeterminado: ilimitado.

Configuración del análisis de archivos comprimidos

Nivel de anidamiento de archivos: especifica el nivel máximo de análisis de archivos. Valor predeterminado: 10.

Tamaño máx. de archivo en el archivo comprimido: esta opción permite especificar el tamaño máximo de archivo de los archivos contenidos en archivos comprimidos (una vez extraídos) que se van a analizar. El valor máximo es 3 GB.

> No se recomienda cambiar los valores predeterminados; en circunstancias normales, no debería haber motivo para hacerlo.

Control de dispositivos

ESET Endpoint Antivirus proporciona control automático del dispositivo (CD/DVD/USB/etc.). Este módulo le permite bloquear o ajustar los filtros y permisos ampliados, así como establecer los permisos de un usuario para acceder a un dispositivo dado y trabajar en él. Esto puede ser útil cuando el administrador del ordenador quiere impedir que los usuarios utilicen dispositivos con contenido no solicitado.

Dispositivos externos admitidos:

- Almacenamiento en disco (unidad de disco duro, disco USB extraíble)
- CD/DVD
- USB Impresora
- FireWire Almacenamiento
- Bluetooth Dispositivo
- Lector de tarjetas inteligentes
- Dispositivo de imagen
- Módem
- LPT/COM puerto
- Dispositivo portátil (dispositivos con batería, como reproductores multimedia, smartphones, dispositivos

plug-and-play, etc.)
- Todos los tipos de dispositivos

Las opciones de configuración del control del dispositivo se pueden modificar en Configuración avanzada > **Protecciones** > **Control del dispositivo**.

Haga clic en el botón **Habilitar control de dispositivo** para habilitar la función Control de dispositivos en ESET Endpoint Antivirus; debe reiniciar el equipo para que este cambio surta efecto. Una vez activado Control de dispositivos, puede definir las **Reglas** en la ventana Editor de reglas.

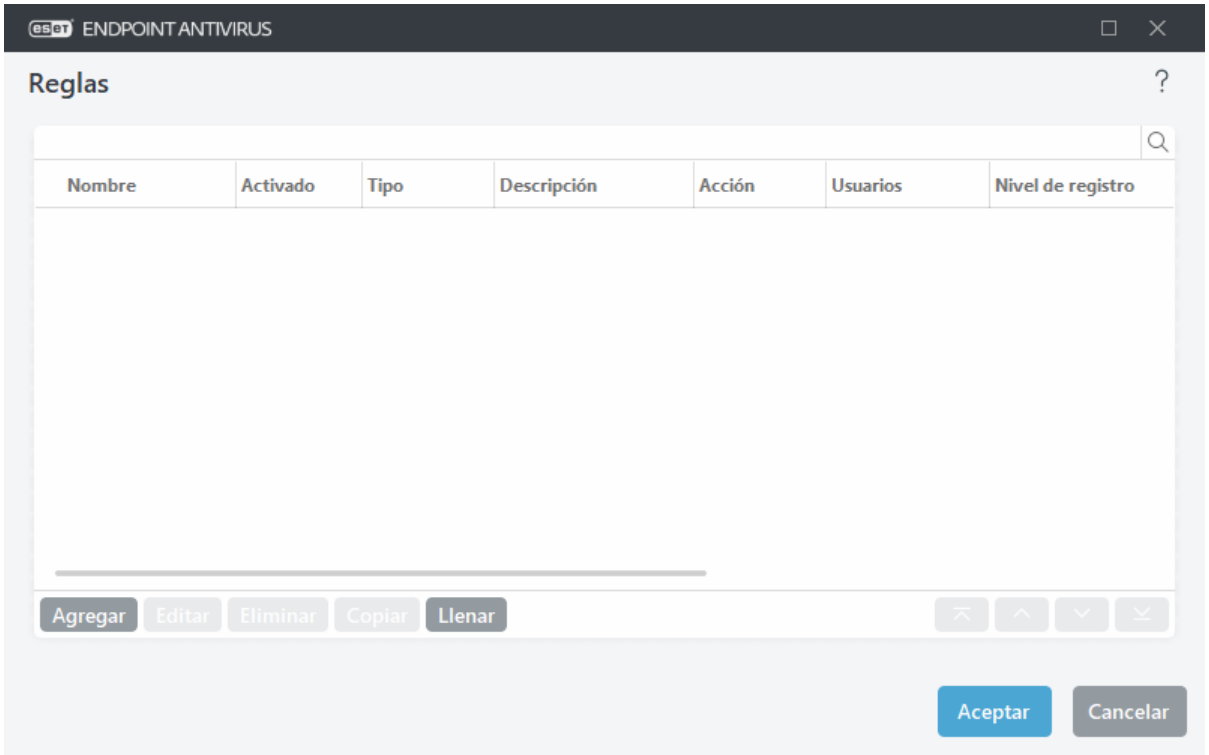
> Con tareas programadas puede importar un grupo de control de dispositivos con reglas desde un archivo xml. Para obtener más información y una guía paso a paso, consulte el artículo de la base de conocimiento de ESET.

Si se inserta un dispositivo que está bloqueado por una regla, se muestra una ventana de notificación y se prohíbe el acceso a dicho dispositivo.

Editor de reglas de control de dispositivos

La ventana **Editor de reglas de control de dispositivos** muestra las reglas existentes y permite controlar con precisión los dispositivos externos que los usuarios conectan al equipo. Consulte también Adición de reglas de control de dispositivos

> Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés: Agregar y modificar reglas de control de dispositivos con los productos ESET Endpoint

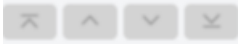


Determinados dispositivos se pueden permitir o bloquear según el usuario, el grupo de usuarios o según varios parámetros adicionales que se pueden especificar en la configuración de las reglas. La lista de reglas contiene varias descripciones de una regla, como el nombre, el tipo de dispositivo externo, la acción que debe realizarse tras conectar un dispositivo externo al ordenador y la gravedad del registro.

Haga clic en **Agregar** o en **Modificar** para administrar una regla. Desactive la casilla **Activado** que aparece junto a la regla para desactivarla hasta que la quiera usar en el futuro. Seleccione una o más reglas y haga clic en **Eliminar** para eliminar las reglas de forma permanente.

Copiar: crea una nueva regla con opciones predefinidas utilizadas para otra regla seleccionada.

Haga clic en **Llenar** para rellenar automáticamente los parámetros del medio extraíble conectado a su ordenador.

Las reglas se muestran en orden de prioridad; las que tienen más prioridad se muestran más arriba en la lista. Las reglas pueden moverse haciendo clic en  **Superior/Arriba/Abajo/Inferior** tanto por separado como en grupo.

El Registro de control de dispositivos anota todas las ocasiones en las que se activa el Control de dispositivos. Las entradas de registro se pueden ver desde la ventana principal del programa de ESET Endpoint Antivirus en **Herramientas** > **Archivos de registro**.

Dispositivos detectados

El botón **Llenar** contiene una visión general de todos los dispositivos conectados actualmente con información sobre los aspectos siguientes: tipo de dispositivo, proveedor del dispositivo, modelo y número de serie (si está disponible).

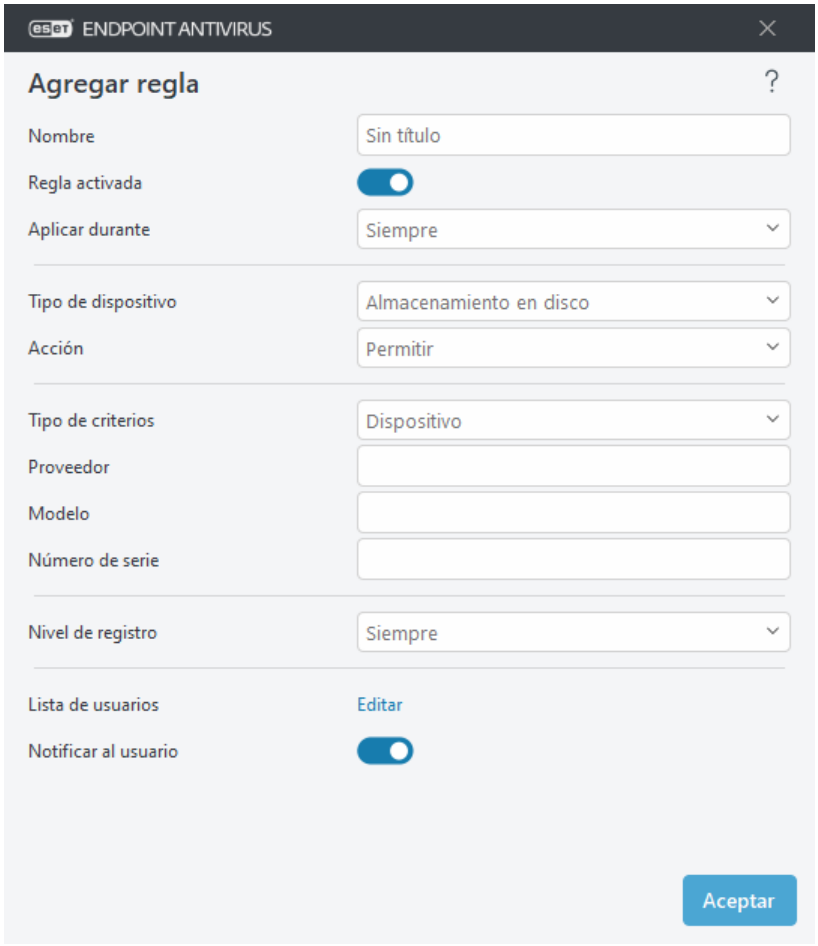
Seleccione un dispositivo en la lista de dispositivos detectados y haga clic en **Aceptar** para agregar una regla de control de dispositivos con información predefinida (se puede ajustar toda la configuración).

Los dispositivos que estén en el modo de bajo consumo (suspensión) están marcados con un icono de advertencia . Para activar el botón **Aceptar** y agregar una regla para este dispositivo:

- Reconecte el dispositivo.
- Utilice el dispositivo (por ejemplo, inicie la aplicación Cámara en Windows para activar una cámara web).

Adición de reglas de control de dispositivos

Una regla de control de dispositivos define la acción que se realizará al conectar al ordenador un dispositivo que cumple los criterios de la regla.



Introduzca una descripción de la regla en el campo **Nombre** para mejorar la identificación. Haga clic en el interruptor situado junto a **Regla activada** para activar o desactivar esta regla. Esto puede ser de utilidad cuando no se quiere eliminar una regla de forma permanente.

Aplicar durante: permite aplicar la regla creada durante el tiempo especificado. En el menú desplegable, seleccione el intervalo de tiempo creado. Consulte más información sobre los Intervalos de tiempo.

Tipo de dispositivo

Elija el tipo de dispositivo externo en el menú desplegable (Almacenamiento en disco, Dispositivo portátil, Bluetooth, FireWire…). La información sobre el tipo de dispositivo se recopila del sistema operativo y se puede ver en el administrador de dispositivos del sistema cada vez que se conecta un dispositivo al ordenador. Los dispositivos de almacenamiento abarcan discos externos o lectores de tarjetas de memoria convencionales conectados mediante USB o FireWire. Los lectores de tarjetas inteligentes abarcan todos los lectores que tienen incrustado un circuito integrado, como las tarjetas SIM o las tarjetas de autenticación. Ejemplos de dispositivos de imagen son escáneres o cámaras. Como estos dispositivos solo proporcionan información sobre sus acciones y no sobre los usuarios, solo pueden bloquearse a nivel global.

> la función de la lista de usuarios no está disponible para tipos de dispositivos modernos. La regla se aplicará a todos los usuarios, y se eliminará la lista de usuarios actual.

Acción

El acceso a dispositivos que no son de almacenamiento se puede permitir o bloquear. En cambio, las reglas para los dispositivos de almacenamiento permiten seleccionar una de las siguientes configuraciones de derechos:

- **Permitir**: se permitirá el acceso completo al dispositivo.
- **Bloquear**: se bloqueará el acceso al dispositivo.
- **Bloquear escritura**: solo se permitirá el acceso de lectura al dispositivo.
- **Advertir**: cada vez que se conecte un dispositivo se informará al usuario de si está permitido o bloqueado, y se efectuará una entrada de registro. Los dispositivos no se recuerdan, se seguirá mostrando una notificación en las siguientes conexiones del mismo dispositivo.

Tenga en cuenta que no todas las acciones (permisos) están disponibles para todos los tipos de dispositivos. Si se trata de un dispositivo de tipo almacenamiento, las cuatro acciones estarán disponibles. En el caso de los dispositivos que no son de almacenamiento solo hay tres disponibles (por ejemplo, **Bloquear escritura** no está disponible para Bluetooth, lo que significa que los dispositivos Bluetooth solo se pueden permitir, bloquear o emitirse una advertencia sobre ellos).

Tipo de criterios

Seleccione **Grupo de dispositivos** o **Dispositivo**.

Debajo se muestran otros parámetros que se pueden usar para ajustar las reglas según el dispositivo. Todos los parámetros distinguen entre mayúsculas y minúsculas y admiten comodines (*, ?):

- **Fabricante**: filtrado por nombre o identificador del fabricante.
- **Modelo**: el nombre del dispositivo.
- **Número de serie**: normalmente, los dispositivos externos tienen su propio número de serie. En el caso de los CD y DVD, el número de serie está en el medio, no en la unidad de CD.

> Si estos parámetros están sin definir, la regla ignorará estos cambios a la hora de establecer la coincidencia. Los parámetros de filtrado en todos los campos de texto distinguen entre mayúsculas y minúsculas y admiten comodines. El signo de interrogación (?) representa un carácter único, y el asterisco (*) una cadena variable de cero o más caracteres.

> Si desea ver información sobre un dispositivo, cree una regla para ese tipo de dispositivo, conecte el dispositivo al ordenador y, a continuación, consulte los detalles del dispositivo en el Registro de control de dispositivos.

Nivel de registro

- **Siempre**: registra todos los sucesos.
- **Diagnóstico**: registra la información necesaria para ajustar el programa.
- **Información**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alerta**: registra errores graves y mensajes de alerta y los envía a ERA Server.
- **Ninguno**: no se registra nada.

Las reglas se pueden limitar a determinados usuarios o grupos de usuarios agregándolos a la **Lista de usuarios**:

- **Agregar**: abre el cuadro de diálogo **Tipos de objeto: Usuarios o grupos**, que le permite seleccionar los usuarios que desee.
- **Quitar**: elimina del filtro al usuario seleccionado.

Limitaciones de la lista de usuarios

La lista de usuarios no se puede definir para reglas con tipos de dispositivo específicos:

- Impresora USB
- Dispositivo Bluetooth
- Lector de tarjetas inteligentes
- Dispositivo de imagen
- Módem
- Puerto LPT/COM

Notificar al usuario: si se inserta un dispositivo que está bloqueado por una regla, se muestra una ventana de notificación.

Grupos de dispositivos

La conexión de un dispositivo al ordenador puede presentar un riesgo para la seguridad.

La ventana Grupos de dispositivos se divide en dos partes. La parte derecha de la ventana contiene una lista de los dispositivos que pertenecen al grupo correspondiente, mientras que la parte izquierda contiene los grupos creados. Seleccione un grupo para mostrar los dispositivos en el panel de la derecha.

Cuando abre la ventana Grupos de dispositivos y selecciona uno de los grupos, puede agregar o quitar dispositivos de la lista. Otra forma de agregar dispositivos al grupo es importarlos desde un archivo. También puede hacer clic en el botón **Llenar** y se mostrarán en la ventana **Dispositivos detectados** todos aquellos dispositivos que estén conectados a su ordenador. Seleccione dispositivos de la lista para agregarlos al grupo haciendo clic en **Aceptar**.

Elementos de control

Agregar: puede agregar un grupo escribiendo su nombre o un dispositivo a un grupo existente en función del punto de la ventana en el que hiciera clic en el botón.

Modificar: le permite modificar el nombre del grupo seleccionado o los parámetros (proveedor, modelo, número de serie) del dispositivo.

Eliminar: elimina el grupo o el dispositivo seleccionados, según la parte de la ventana en la que hiciera clic.

Importar: importa una lista de dispositivos desde un archivo de texto. La importación de dispositivos desde un archivo de texto requiere el formato correcto:

- Cada dispositivo se inicia en una línea nueva.
- El **Proveedor**, el **Modelo** y el **Número de serie** deben estar presentes en cada dispositivo y separados con una coma.

A continuación se muestra un ejemplo del contenido del archivo de texto:

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Exportar: exporta una lista de dispositivos a un archivo.

El botón **Llenar** contiene una visión general de todos los dispositivos conectados actualmente con información sobre los aspectos siguientes: tipo de dispositivo, proveedor del dispositivo, modelo y número de serie (si está disponible).

Con tareas programadas puede importar un grupo de control de dispositivos con reglas desde un archivo xml. Para obtener más información y una guía paso a paso, consulte el artículo de la base de conocimiento de ESET.

Agregar dispositivo

Haga clic en Agregar la ventana de la derecha para agregar un dispositivo a un grupo existente. Debajo se muestran otros parámetros que se pueden usar para ajustar las reglas según el dispositivo. Todos los parámetros distinguen entre mayúsculas y minúsculas y admiten comodines (*, ?):

- **Proveedor**: filtrar por nombre o ID de proveedor.
- **Modelo**: el nombre del dispositivo.
- **Número de serie**: normalmente, los dispositivos externos tienen su propio número de serie. En el caso de los CD y DVD, el número de serie está en el medio, no en la unidad de CD.
- **Descripción**: descripción del dispositivo para una mejor organización.

Si estos parámetros están sin definir, la regla ignorará estos cambios a la hora de establecer la coincidencia. Los parámetros de filtrado en todos los campos de texto distinguen entre mayúsculas y minúsculas y admiten comodines. El signo de interrogación (?) representa un carácter único, y el asterisco (*) una cadena variable de cero o más caracteres.

Haga clic en **Aceptar** para guardar los cambios. Haga clic en **Cancelar** si desea cerrar la ventana **Grupos de dispositivos** sin guardar los cambios.

Tras crear un grupo de dispositivos, tendrá que agregar una nueva regla de control de dispositivos y elegir la acción que desea realizar.

Tenga en cuenta que no todas las acciones (permisos) están disponibles para todos los tipos de dispositivos. Si se trata de un dispositivo de tipo almacenamiento, las cuatro acciones estarán disponibles. En el caso de los dispositivos que no son de almacenamiento solo hay tres disponibles (por ejemplo, **Bloquear escritura** no está disponible para Bluetooth, lo que significa que los dispositivos Bluetooth solo se pueden permitir, bloquear o emitirse una advertencia sobre ellos).

ThreatSense

ThreatSense consta de muchos métodos complejos de detección de amenazas. Esta tecnología es proactiva, lo que significa que también proporciona protección durante la fase inicial de expansión de una nueva amenaza. Utiliza una combinación de análisis de código, emulación de código, firmas genéricas y firmas de virus que funcionan de forma conjunta para mejorar en gran medida la seguridad del sistema. El motor de análisis es capaz de controlar varios flujos de datos de forma simultánea, de manera que maximiza la eficacia y la velocidad de detección. Además, la tecnología ThreatSense elimina eficazmente los programas peligrosos (rootkits).

Las opciones de configuración del motor de ThreatSense le permiten especificar varios parámetros de análisis:

- Los tipos de archivos y extensiones que se deben analizar
- La combinación de diferentes métodos de detección.
- Los niveles de desinfección, etc.

Para acceder a la ventana de configuración, haga clic en **ThreatSense** en la ventana Configuración avanzada de cualquier módulo que utilice la tecnología ThreatSense (consulte más abajo). Es posible que cada escenario de

seguridad requiera una configuración diferente. Con esto en mente, ThreatSense se puede configurar individualmente para los siguientes módulos de protección:

- Protección del sistema de archivos en tiempo real
- Análisis de estado inactivo
- Análisis en el inicio
- Protección de documentos
- Protección del cliente de correo electrónico
- Protección del tráfico de Internet
- Análisis del ordenador

Los parámetros de ThreatSense están altamente optimizados para cada módulo y su modificación puede afectar al funcionamiento del sistema de forma significativa. Por ejemplo, la modificación de los parámetros para que siempre analicen empaquetadores de ejecución en tiempo real o la activación de la heurística avanzada en el módulo de protección del sistema de archivos en tiempo real podrían ralentizar el sistema (normalmente, con estos métodos solo se analizan los archivos recién creados). Se recomienda que no modifique los parámetros predeterminados de ThreatSense para ninguno de los módulos, a excepción de Análisis del ordenador.

Objetos a analizar

En esta sección se pueden definir los componentes y archivos del ordenador que se analizarán en busca de amenazas.

Memoria operativa: busca amenazas que ataquen a la memoria operativa del sistema.

Sectores de inicio/UEFI: analiza los sectores de inicio para detectar malware en el registro de inicio principal. Lea más sobre la UEFI en el glosario.

Archivos de correo: el programa admite las siguientes extensiones: DBX (Outlook Express) y EML.

Archivos comprimidos: el programa es compatible con las extensiones ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE y muchas más.

Archivos comprimidos autoextraíbles: los archivos comprimidos autoextraíbles (SFX) son archivos comprimidos que pueden extraerse por sí solos.

Empaquetadores en tiempo de ejecución: después de su ejecución, los empaquetadores en tiempo de ejecución (a diferencia de los archivos estándar) se descomprimen en la memoria. Además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FSG, etc.), el módulo de análisis permite reconocer varios tipos de empaquetadores adicionales gracias a la emulación de códigos.

Opciones de análisis

Seleccione los métodos empleados al analizar el sistema en busca de infiltraciones. Están disponibles las opciones siguientes:

Heurística: la heurística es un algoritmo que analiza la actividad (maliciosa) de los programas. La principal ventaja de esta tecnología es la habilidad para identificar software malicioso que no existía o que el motor de detección anterior no conocía. Su desventaja es la probabilidad (muy pequeña) de falsas alarmas.

Heurística avanzada/ADN inteligentes: la heurística avanzada es un algoritmo heurístico único desarrollado por ESET optimizado para detectar gusanos informáticos y troyanos escritos en lenguajes de programación de alto

nivel. El uso de la heurística avanzada mejora en gran medida la detección de amenazas por parte de los productos de ESET. Las firmas pueden detectar e identificar virus de manera fiable. Gracias al sistema de actualización automática, las nuevas firmas están disponibles en cuestión de horas cuando se descubre una amenaza. Su desventaja es que únicamente detectan los virus que conocen (o versiones ligeramente modificadas).

Desinfección

La configuración de desinfección determinan el comportamiento de ESET Endpoint Antivirus durante la desinfección de objetos.

Exclusiones

Una extensión es una parte del nombre de archivo delimitada por un punto. Una extensión define el tipo y el contenido de un archivo. En esta sección de la configuración de ThreatSense, es posible definir los tipos de archivos que se desean analizar.

Otros

Al configurar motor ThreatSense para un análisis del ordenador a petición, dispone también de las siguientes opciones en la sección **Otros**:

Analizar secuencias de datos alternativas (ADS): las secuencias de datos alternativos utilizadas por el sistema de archivos NTFS son asociaciones de carpetas y archivos que no se detectan con técnicas de análisis ordinarias. Muchas amenazas intentan evitar los sistemas de detección haciéndose pasar por flujos de datos alternativos.

Realizar análisis en segundo plano con baja prioridad: cada secuencia de análisis consume una cantidad determinada de recursos del sistema. Si se trabaja con programas cuyo consumo de recursos constituye una carga importante para el sistema, es posible activar el análisis en segundo plano con baja prioridad y reservar los recursos para las aplicaciones.

Registrar todos los objetos: el registro del análisis mostrará todos los archivos analizados en archivos comprimidos de autoextracción, incluso los no infectados (puede generar muchos datos de registro del análisis y aumentar el tamaño del archivo de registro del análisis).

Activar la optimización inteligente: si la opción Optimización inteligente está activada, se utiliza la configuración más óptima para garantizar el nivel de análisis más eficaz y, al mismo tiempo, mantener la máxima velocidad de análisis posible. Los diferentes módulos de protección analizan de forma inteligente, con métodos de análisis distintos y aplicados a tipos de archivo específicos. Si la optimización inteligente está desactivada, solamente se aplica la configuración definida por el usuario en el núcleo ThreatSense de los módulos donde se realiza el análisis.

Preservar el último acceso con su fecha y hora: seleccione esta opción para guardar la hora de acceso original de los archivos analizados, en lugar de actualizarlos (por ejemplo, para utilizar con sistemas de copia de seguridad de datos).

Límites

En la sección Límites se puede especificar el tamaño máximo de los objetos y los niveles de archivos anidados que se analizarán:

Configuración de los objetos

Tamaño máximo del objeto: define el tamaño máximo de los objetos que se analizarán. El módulo antivirus analizará solo los objetos que tengan un tamaño menor que el especificado. Esta opción solo deben cambiarla usuarios avanzados que tengan motivos específicos para excluir del análisis objetos más grandes. Valor predeterminado: ilimitado.

Tiempo máximo de análisis para el objeto (s): define el valor de tiempo máximo para el análisis de los archivos de un objeto contenedor (por ejemplo, un archivo comprimido RAR/ZIP o un mensaje de correo electrónico con varios archivos adjuntos). Este ajuste no se aplica a los archivos independientes. Si se ha introducido un valor definido por el usuario y ha transcurrido el tiempo, el análisis se detendrá lo antes posible, independientemente de si ha finalizado el análisis de cada archivo del objeto contenedor. En el caso de un archivo comprimido con archivos grandes, el análisis se detendrá en cuanto se extraiga un archivo del archivo comprimido (por ejemplo, si la variable definida por el usuario es de 3 segundos, pero la extracción de un archivo tarda 5 segundos). El resto de archivos del archivo comprimido no se analizarán una vez transcurrido el tiempo. Para limitar el tiempo de análisis, incluido el de los archivos comprimidos más grandes, utilice los ajustes **Tamaño máximo del objeto** y **Tamaño máx. de archivo en el archivo comprimido** (no se recomienda debido a posibles riesgos de seguridad). Valor predeterminado: ilimitado.

Configuración del análisis de archivos comprimidos

Nivel de anidamiento de archivos: especifica el nivel máximo de análisis de archivos. Valor predeterminado: 10.

Tamaño máx. de archivo en el archivo comprimido: esta opción permite especificar el tamaño máximo de archivo de los archivos contenidos en archivos comprimidos (una vez extraídos) que se van a analizar. El valor máximo es 3 GB.

> No se recomienda cambiar los valores predeterminados; en circunstancias normales, no debería haber motivo para hacerlo.

Niveles de desinfección

Para cambiar la configuración del nivel de desinfección de un módulo de protección, expanda **ThreatSense** (por ejemplo, **Protección del sistema de archivos en tiempo real**) y, a continuación, elija un **Nivel de desinfección** en el menú desplegable.

ThreatSense tiene los siguientes niveles de corrección (es decir, desinfección).

Corrección en ESET Endpoint Antivirus

Nivel de desinfección	Descripción
Reparar la detección siempre	Intentar corregir la detección durante la desinfección de objetos sin la intervención del usuario final. En algunos casos raros (por ejemplo, archivos del sistema), si no se puede corregir la detección, el objeto del que se informa se deja en su ubicación original. **Corregir siempre las detecciones** es el ajuste predeterminado recomendado en entornos administrados.

Nivel de desinfección	Descripción
Reparar la detección si es seguro, mantener de otro modo	Intentar corregir la detección durante la desinfección de objetos sin la intervención del usuario final. En algunos casos (por ejemplo, archivos del sistema o archivos comprimidos con archivos limpios e infectados), si la detección no se puede corregir, el objeto del que se informa se deja en su ubicación original.
Reparar la detección si es seguro, preguntar de otro modo	Intentar corregir la detección durante la desinfección de objetos. En algunos casos, si no se puede realizar ninguna acción, el usuario final recibe una alerta interactiva y debe seleccionar una acción de corrección (por ejemplo, eliminar o ignorar). Este ajuste se recomienda en la mayoría de los casos.
Preguntar siempre al usuario final	El usuario final recibe una ventana interactiva durante la desinfección de objetos y debe seleccionar una acción correctiva (por ejemplo, eliminar u omitir). Este nivel se ha diseñado para usuarios más avanzados que conocen los pasos necesarios en caso de detección.

Extensiones de archivo excluidas del análisis

Las extensiones de archivo excluidas forman parte de ThreatSense. Para configurar las extensiones de archivo excluidas, haga clic en **ThreatSense** en la ventana Configuración avanzada de cualquier módulo que utilice la tecnología ThreatSense.

Una extensión es una parte del nombre de archivo delimitada por un punto. Una extensión define el tipo y el contenido de un archivo. En esta sección de la configuración de ThreatSense, es posible definir los tipos de archivos que se desean analizar.

> No se confunda con Exclusiones de procesos, Exclusiones del HIPS ni Exclusiones de archivo/carpeta.

De forma predeterminada, se analizan todos los archivos. Se puede agregar cualquier extensión a la lista de archivos excluidos del análisis.

A veces es necesario excluir archivos del análisis si, por ejemplo, el análisis de determinados tipos de archivo impide la correcta ejecución del programa que utiliza determinadas extensiones. Por ejemplo, quizás sea aconsejable excluir las extensiones `.edb`, `.eml` y `.tmp` cuando se utilizan servidores Microsoft Exchange.

> Para agregar una nueva extensión a la lista, haga clic en **Agregar**. Escriba la extensión en el campo en blanco (por ejemplo, tmp) y haga clic en **Aceptar**. Cuando selecciona **Introduzca múltiples valores**, puede agregar varias extensiones de archivo delimitadas por líneas, comas o punto y coma (por ejemplo, elija **Punto y coma** en el menú desplegable como separador y escriba `edb;eml;tmp`).
> Puede utilizar un símbolo especial ? (signo de interrogación). El signo de interrogación representa cualquier símbolo (por ejemplo, `?db`).

> Para ver la extensión exacta (si la hubiera) de un archivo en un sistema operativo Windows, debe marcar la casilla de verificación **Extensiones de nombre de archivo** en **Explorador de Windows** > **Ver** (pestaña).

Parámetros adicionales de ThreatSense

Para modificar esta configuración, abra Configuración avanzada > **Protecciones** > **Protección del sistema de archivos en tiempo real** > **Parámetros adicionales ThreatSense**.

Parámetros adicionales de ThreatSense para archivos nuevos y modificados

La probabilidad de infección en los archivos recién creados o modificados es superior a la de los archivos existentes. Por eso el programa comprueba estos archivos con parámetros de análisis adicionales. ESET Endpoint Antivirus utiliza la heurística avanzada, que detecta amenazas nuevas antes de que se publique la actualización del motor de detección en combinación con métodos de análisis basados en firmas.

Además de en los archivos nuevos, el análisis se realiza también en los **archivos comprimidos de autoextracción** (.sfx) y **empaquetadores en tiempo real** (archivos ejecutables comprimidos internamente). De forma predeterminada, los archivos comprimidos se analizan hasta el 10.º nivel de anidamiento y se comprueban independientemente de su tamaño real. Para modificar la configuración de análisis de archivos comprimidos, anule la selección de la opción **Configuración predeterminada para el análisis de archivos comprimidos**.

Parámetros adicionales de ThreatSense para los archivos ejecutados

Heurística avanzada para los archivos ejecutados: de forma predeterminada, se utiliza la Heurística avanzada al ejecutar archivos. Si esta opción está activada, se recomienda encarecidamente dejar activadas las opciones Optimización inteligente y ESET LiveGrid® con el fin de mitigar su repercusión en el rendimiento del sistema.

Heurística avanzada al ejecutar archivos desde las unidades extraíbles: la heurística avanzada emula el código en un entorno virtual y evalúa su comportamiento antes de permitir la ejecución del código desde soportes extraíbles.

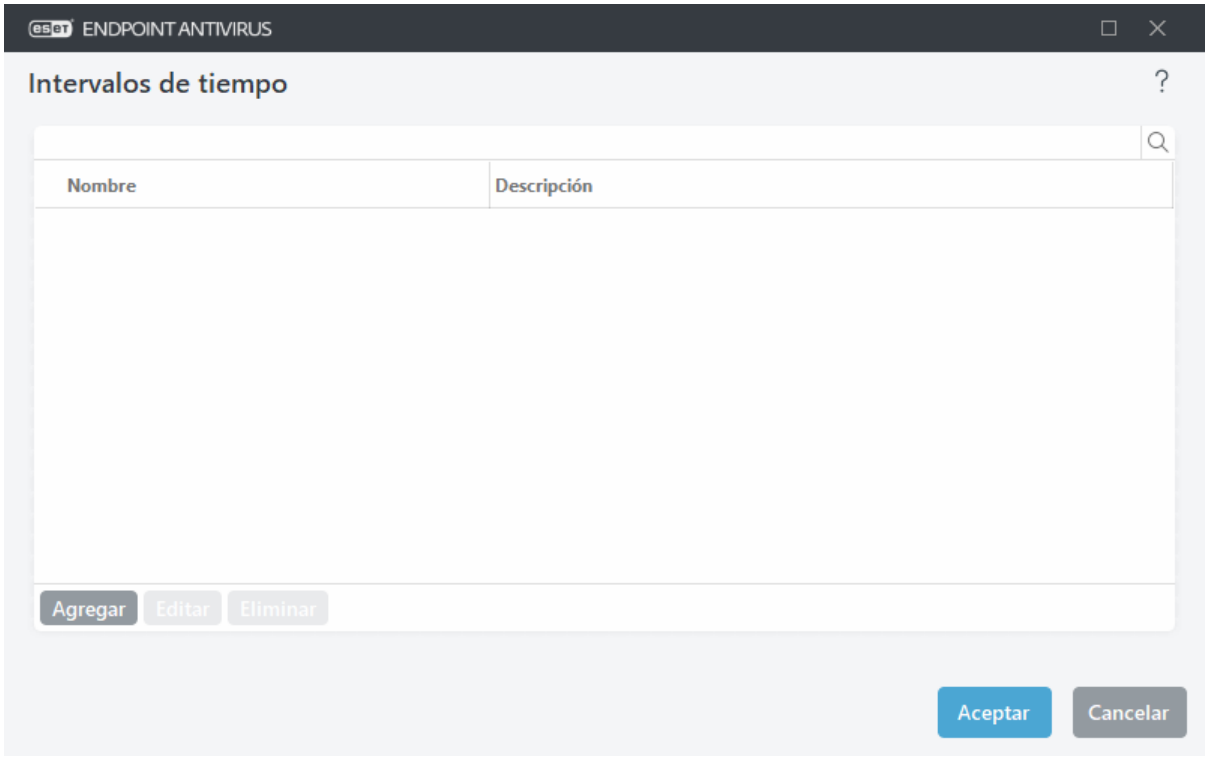
Herramientas

Puede configurar opciones avanzadas para funciones que ofrecen seguridad adicional y ayudan a simplificar la administración de ESET Endpoint Antivirus en Configuración avanzada > **Herramientas**.

- Intervalos de tiempo
- Microsoft Windows Update
- CMD de ESET
- Supervisión y administración remotas
- Intervalo de comprobación de la licencia
- Archivos de registro
- Modo de presentación
- Diagnóstico

Intervalos de tiempo

Puede crear intervalos de tiempo y asignarlos a reglas de **Control de dispositivos**. Encontrará el ajuste **Intervalos de tiempo** en Configuración avanzada > **Herramientas**. De esta forma, podrá definir intervalos de tiempo de uso frecuente (por ejemplo, tiempo de trabajo, fin de semana, etc.) y reutilizarlos con facilidad sin necesidad de volver a definirlos para cada regla. Los intervalos de tiempo se pueden aplicar a cualquier tipo de regla compatible con el análisis basado en el tiempo.



Para crear un intervalo de tiempo, realice los pasos siguientes:

1. Haga clic en **Modificar** > **Agregar**.
2. Escriba el nombre y **la descripción** del intervalo de tiempo, y haga clic en **Agregar**.
3. Especifique el día y las horas de inicio/fin del intervalo de tiempo, o seleccione **Todo el día**.
4. Haga clic en **Aceptar** para confirmar.

Puede definir un único intervalo de tiempo con uno o más periodos de tiempo basados en días o en horas. Cuando se cree el intervalo de tiempo, se mostrará en el menú desplegable **Aplicar durante** en la ventana del editor de reglas de Control de dispositivos.

Microsoft Windows Update

La función de actualización de Windows es un componente importante a la hora de proteger a los usuarios de software malicioso. Por eso es fundamental que instale las actualizaciones de Microsoft Windows en cuanto se publiquen. ESET Endpoint Antivirus le informa sobre las actualizaciones que le faltan, según el nivel que haya especificado. Están disponibles los siguientes niveles:

- **Sin actualizaciones**: no se ofrecerá ninguna actualización del sistema para la descarga.
- **Actualizaciones opcionales**: se ofrecerán para la descarga las actualizaciones marcadas como de baja prioridad y de niveles superiores.
- **Actualizaciones recomendadas**: se ofrecerán para la descarga las actualizaciones marcadas como habituales y de niveles superiores.
- **Actualizaciones importantes**: se ofrecerán para la descarga las actualizaciones marcadas como importantes y de niveles superiores.
- **Actualizaciones críticas**: solo se ofrecerá la descarga de actualizaciones críticas.

Haga clic en **Aceptar** para guardar los cambios. La ventana de actualizaciones del sistema se mostrará después de la verificación del estado con el servidor de actualización. Por tanto, es posible que la información de actualización del sistema no esté disponible inmediatamente después de guardar los cambios.

Cuadro de diálogo: Actualizaciones del sistema operativo

Si hay actualizaciones disponibles para su sistema operativo, la ventana de inicio de ESET Endpoint Antivirus mostrará la notificación correspondiente. Haga clic en **Más información** para abrir la ventana de actualizaciones del sistema.

En la ventana de actualizaciones del sistema se muestra la lista de actualizaciones disponibles que están listas para su descarga e instalación. El tipo de actualización se muestra junto a su nombre.

Haga doble clic en la fila de una de las actualizaciones para que se muestre la ventana Información de actualización con información adicional.

Haga clic en **Ejecutar actualización del sistema** para descargar e instalar todas las actualizaciones del sistema operativo incluidas en la lista.

Información de actualización

En la ventana de actualizaciones del sistema se muestra la lista de actualizaciones disponibles que están listas para su descarga e instalación. El nivel de prioridad de la actualización se muestra junto a su nombre.

Haga clic en **Ejecutar actualización del sistema** para iniciar la descarga e instalar las actualizaciones del sistema operativo.

Haga clic con el botón derecho del ratón en cualquier fila de actualización y, a continuación, haga clic en **Mostrar información** para abrir una ventana nueva con información adicional.

CMD de ESET

Se trata de una función que activa comandos de ecmd avanzados. Puede exportar e importar la configuración utilizando la línea de comandos (ecmd.exe). Hasta ahora, solo era posible exportar la configuración utilizando la interfaz gráfica de usuario. La configuración de ESET Endpoint Antivirus puede exportarse a un archivo *.xml*.

Si tiene activado ESET CMD, dispone de dos métodos de autorización:

- **Ninguno**: sin autorización. No le recomendamos este método, ya que permite importar configuraciones no firmadas, lo que supone un riesgo.
- **Configuración avanzada de contraseña**: se requiere contraseña para importar una configuración de un archivo *.xml*. Este archivo debe estar firmado (consulte cómo se firma un archivo de configuración *.xml* más adelante). Debe introducirse la contraseña especificada en Configuración de acceso para poder importar una nueva configuración. Si no ha activado la configuración de acceso, la contraseña no coincide o el archivo de configuración *.xml* no está firmado, la configuración no se importará.

Una vez que ESET CMD esté activado, podrá utilizar la línea de comandos para importar o exportar configuraciones de ESET Endpoint Antivirus. Podrá hacerlo manualmente o crear un script con fines de automatización.

Para poder utilizar comandos de ecmd avanzados, deberá ejecutarlos con privilegios de administrador, o abrir el símbolo del sistema de Windows (cmd) utilizando **Ejecutar como administrador**. De lo contrario, se mostrará el mensaje **Error executing command**. Asimismo, a la hora de exportar una configuración, deberá existir una carpeta de destino. El comando de exportación sigue funcionando cuando se desactiva el ajuste ESET CMD.

Los comandos de ecmd avanzados solo pueden ejecutarse localmente. La pausa de comandos de ecmd solo puede ejecutarse a través de la tarea de cliente **Ejecutar comando** utilizando ESET PROTECT.

Comando para exportar configuración:
`ecmd /getcfg c:\config\settings.xml`
Comando para importar configuración:
`ecmd /setcfg c:\config\settings.xml`

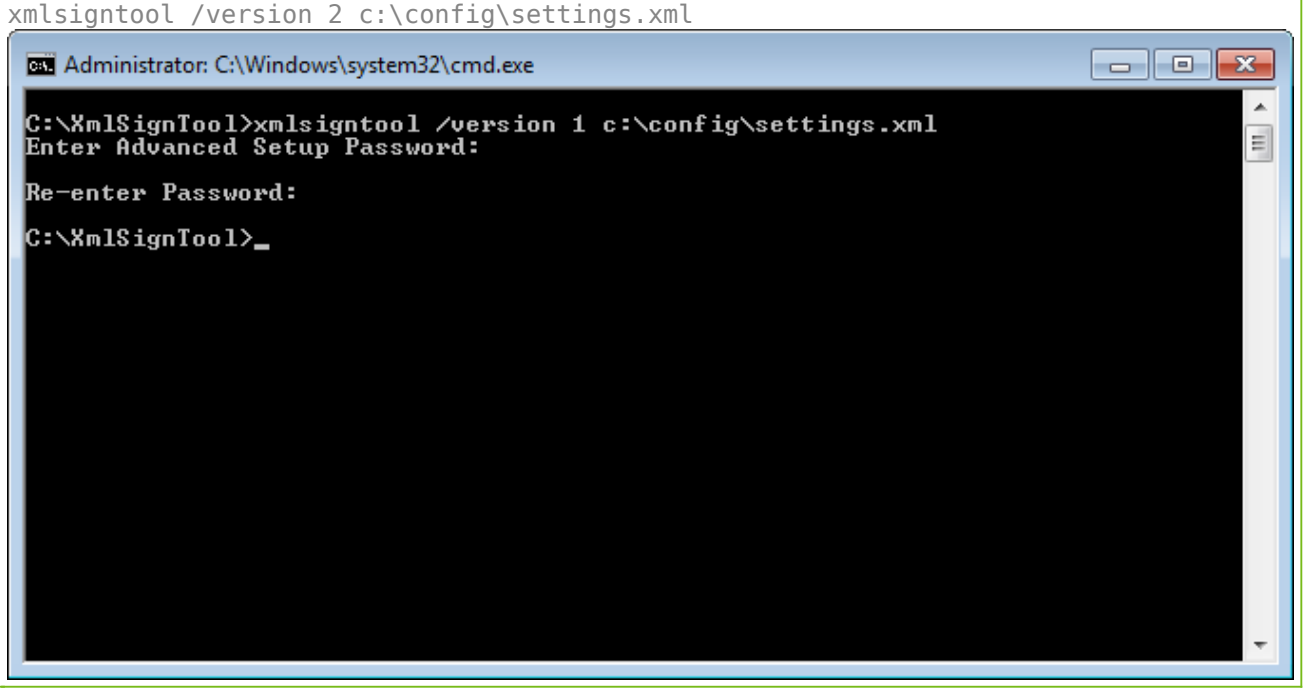
Cómo firmar un archivo de configuración *.xml*:

1. Descargue el archivo ejecutable XmlSignTool.
2. Abra el símbolo del sistema de Windows (cmd) utilizando **Ejecutar como administrador**.
3. Vaya a la ubicación en la que se ha guardado `xmlsigntool.exe`.
4. Ejecute un comando para firmar el archivo de configuración *.xml*; uso: `xmlsigntool /version 1|2 <xml_file_path>`.

El valor del parámetro `/version` depende de su versión de ESET Endpoint Antivirus. Use `/version 2` para la versión 7 y más recientes.

5. Introduzca y vuelva a introducir la contraseña de Configuración avanzada cuando se lo solicite XmlSignTool. Su archivo de configuración *.xml* ya estará firmado y podrá utilizarse para importar otra instancia de ESET Endpoint Antivirus con ESET CMD utilizando el método de autorización de contraseña.

Comando para firmar un archivo de configuración exportado:
`xmlsigntool /version 2 c:\config\settings.xml`



Si la contraseña de Configuración de acceso cambia y desea importar una configuración firmada anteriormente con una contraseña antigua, tendrá que volver a firmar el archivo de configuración *.xml* utilizando la contraseña actual. Esto le permitirá utilizar un archivo de configuración más antiguo sin necesidad de exportarlo a otro equipo que ejecute ESET Endpoint Antivirus antes de la importación.

No se recomienda activar el CMD de ESET sin autorización, ya que hacerlo permitirá importar configuraciones no firmadas. Configure la contraseña en Configuración avanzada > **Interfaz de usuario** > **Configuración de acceso** para evitar que los usuarios realicen modificaciones no autorizadas.

Lista de comandos de ecmd

Con la tarea de cliente Ejecutar comando mediante ESET PROTECT se pueden activar y desactivar temporalmente características de seguridad individuales. Los comandos no anulan los ajustes de las políticas, y los ajustes en pausa volverán a su estado original después de la ejecución del comando o después del reinicio del dispositivo. Para utilizar esta característica, especifique la línea de comandos que desee ejecutar en el campo del mismo nombre.

Revise la lista de comandos para cada característica de seguridad a continuación:

Característica de seguridad	Comando Pausa temporal	Comando Activar
Protección del sistema de archivos en tiempo real	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable
Protección de documentos	ecmd /setfeature document pause	ecmd /setfeature document enable
Control del dispositivo	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable
Modo de presentación	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable
Cortafuegos personal	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
Protección contra los ataques de red (IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
Protección contra botnets	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
Control de acceso web	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
Protección del tráfico de Internet	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
Protección del cliente de correo electrónico	ecmd /setfeature email pause	ecmd /setfeature email enable
Antispam del cliente de correo electrónico	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Protección Anti-Phishing	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

Supervisión y administración remotas

La supervisión y administración remotas (RMM) es el proceso de supervisar y controlar sistemas de software con un agente instalado localmente al que se puede acceder mediante un proveedor de servicios de administración.

ERMM: complemento de ESET para RMM

- La instalación predeterminada de ESET Endpoint Antivirus contiene el archivo `ermm.exe`, que se encuentra en la aplicación Endpoint del directorio:
  C:\Program Files\ESET\ESET Security\ermm.exe
- `ermm.exe` es una utilidad de línea de comandos diseñada para facilitar la administración de productos para equipos y comunicaciones con cualquier complemento de RMM.
- `ermm.exe` intercambia datos con el complemento de RMM, que se comunica con el agente de RMM

vinculado a un servidor de RMM. De manera predeterminada, la herramienta ESET RMM está desactivada.

Recursos adicionales

- Línea de comandos de ERMM
- Lista de comandos ERMM JSON

- Cómo activar supervisión y administración remotasESET Endpoint Antivirus

Complementos de ESET Direct Endpoint Management para soluciones RMM de terceros

RMM Server se ejecuta como servicio en un servidor de terceros. Si desea más información, consulte las siguientes guías del usuario en línea de ESET Direct Endpoint Management:

- Complemento de ESET Direct Endpoint Management para ConnectWise Automate
- Complemento de ESET Direct Endpoint Management para DattoRMM
- ESET Direct Endpoint Management para Solarwinds N-Central
- ESET Direct Endpoint Management para NinjaRMM

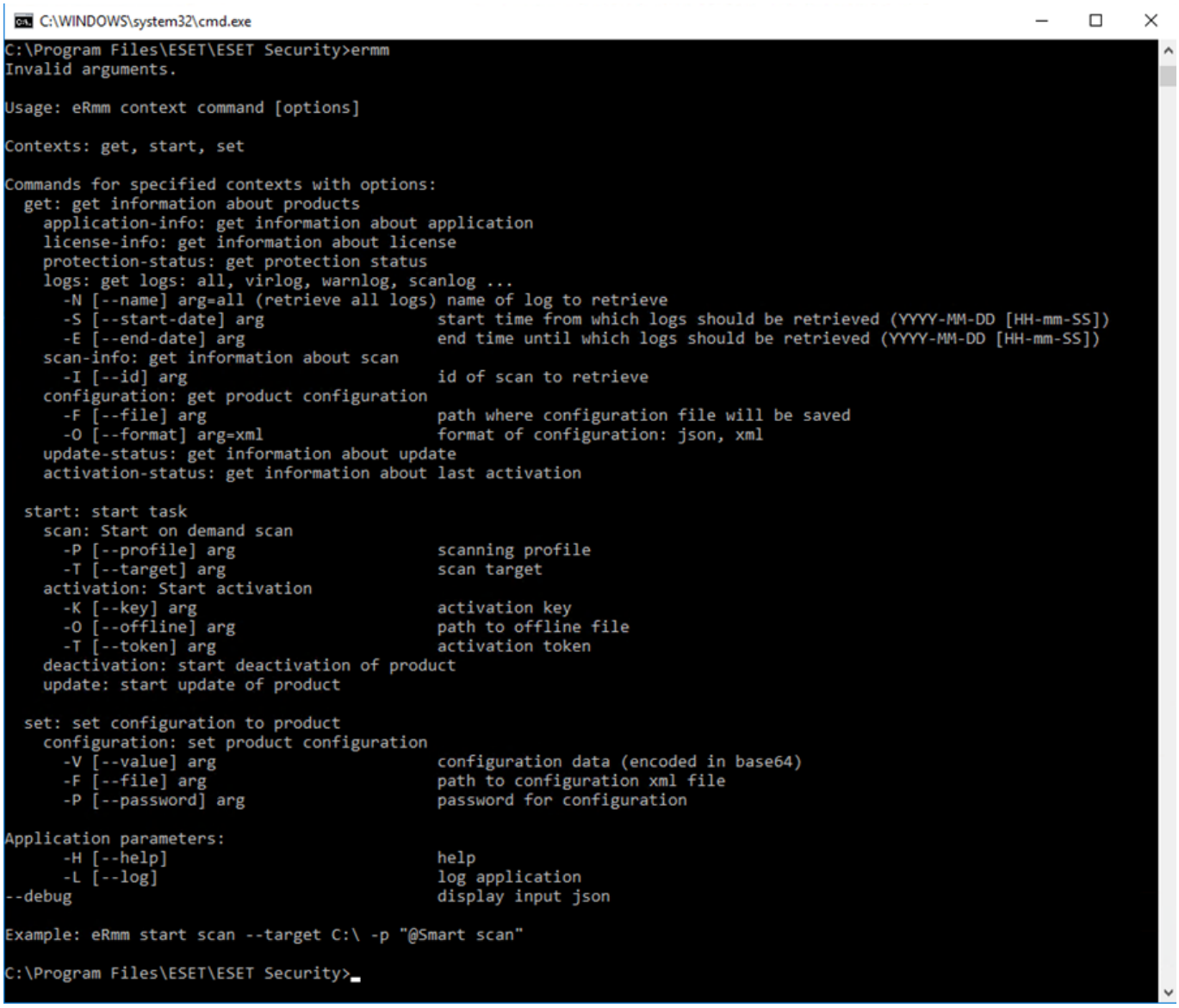
Línea de comandos de ERMM

La administración de supervisión remota se ejecuta mediante la interfaz de la línea de comandos. La instalación predeterminada de ESET Endpoint Antivirus contiene el archivo ermm.exe, que se encuentra en la aplicación Endpoint del directorio: *C:\Program Files\ESET\ESET Security*.

Ejecute el símbolo del sistema (cmd.exe) como administrador y vaya a la ruta mencionada (para abrir el símbolo del sistema, pulse el botón de Windows + R en el teclado, escriba cmd en la ventana Ejecutar y pulse Entrar).

La sintaxis del comando es: `ermm context command [options]`

Los parámetros del registro distinguen entre mayúsculas y minúsculas.



ermm.exe utiliza tres contextos básicos: Get, Start y Set. En la siguiente tabla puede encontrar ejemplos de sintaxis de los comandos. Haga clic en el vínculo de la columna Comando para ver más opciones, parámetros y ejemplos de uso. Tras la ejecución correcta del comando, se mostrará la parte de salida (resultado). Para ver una parte de entrada, agregue el parámetro `--debug` al final del comando.

Contexto	Comando	Descripción
get		**Obtener información sobre los productos**
	application-info	Obtener información sobre el producto
	license-info	Obtener información sobre la licencia
	protection-status	Obtener el estado de la protección
	logs	Obtener registros
	scan-info	Obtener información sobre un análisis en ejecución
	configuration	Obtener la configuración del producto
	update-status	Obtener información sobre la actualización
	activation-status	Obtener información sobre la última activación
start		**Iniciar tarea**
	scan	Iniciar análisis a petición

Contexto	Comando	Descripción
	activation	Iniciar activación del producto
	deactivation	Iniciar desactivación del producto
	update	Iniciar actualización del producto
set		**Definir las opciones del producto**
	configuration	Definir la configuración del producto

En el resultado de salida de cada comando, la primera información que se muestra es el ID del resultado. Para comprender mejor la información del resultado, consulte la tabla de ID que aparece a continuación.

ID de error	Error	Descripción
0	Success	
1	Command node not present	El nodo "Command" no está presente en el json de entrada
2	Command not supported	No se admite el comando
3	General error executing the command	Error durante la ejecución del comando
4	Task already running	La tarea solicitada ya se está ejecutando y no se ha iniciado
5	Invalid parameter for command	La entrada del usuario no es correcta
6	Command not executed because it's disabled	RMM no está activado en la configuración avanzada o no se ha iniciado como administrador

Lista de comandos ERMM JSON

- get protection-status
- get application-info
- get license-info
- get logs
- get activation-status
- get scan-info
- get configuration
- get update-status
- start scan
- start activation
- start deactivation
- start update
- set configuration

get protection-status

Get the list of application statuses and the global application status

Línea de comandos

```
ermm.exe get protection-status
```

Parámetros

None

Ejemplo

call

```
{
"command":"get_protection_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"statuses":[{
"id":"EkrnNotActivated",
"status":2,
"priority":768,
"description":"Product not activated"
}],
"status":2,
"description":"Security alert"
},
"error":null
}
```

get application-info

Get information about the installed application

Línea de comandos

```
ermm.exe get application-info
```

Parámetros

None

Ejemplo

call

```
{
"command":"get_application_info",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"description":"ESET Endpoint Antivirus",
"version":"6.6.2018.0",
"product":"eea",
"lang_id":1033,
"modules":[{
"id":"SCANNER32",
"description":"Detection engine",
"version":"15117",
"date":"2017-03-20"
},{
"id":"PEGASUS32",
"description":"Rapid Response module",
"version":"9734",
"date":"2017-03-20"
},{
"id":"LOADER32",
"description":"Update module",
"version":"1009",
"date":"2016-12-05"
},{
"id":"PERSEUS32",
"description":"Antivirus and antispyware scanner module",
"version":"1513",
"date":"2017-03-06"
},{
"id":"ADVHEUR32",
"description":"Advanced heuristics module",
"version":"1176",
"date":"2017-01-16"
},{
"id":"ARCHIVER32",
"description":"Archive support module",
"version":"1261",
"date":"2017-02-22"
},{
"id":"CLEANER32",
"description":"Cleaner module",
"version":"1132",
"date":"2017-03-15"
},{
"id":"SYSTEMSTATUS32",
"description":"ESET SysInspector module",
"version":"1266",
"date":"2016-12-22"
},{
"id":"TRANSLATOR32",
"description":"Translation support module",
"version":"1588B",
"date":"2017-03-01"
},{
"id":"HIPS32",
"description":"HIPS support module",
"version":"1267",
"date":"2017-02-16"
},{
"id":"PROTOSCAN32",
"description":"Internet protection module",
"version":"1300",
"date":"2017-03-03"
},{
"id":"DBLITE32",
"description":"Database module",
"version":"1088",
"date":"2017-01-05"
},{
"id":"CONFENG32",
"description":"Configuration module (33)",
"version":"1496B",
"date":"2017-03-17"
},{
"id":"IRIS32",
"description":"LiveGrid communication module",
"version":"1022",
"date":"2016-04-01"
},{
"id":"SAURON32",
"description":"Rootkit detection and cleaning module",
"version":"1006",
"date":"2016-07-15"
},{
"id":"SSL32",
"description":"Cryptographic protocol support module",
"version":"1009",
"date":"2016-12-02"
}
},
"error":null
}
}
```

get license-info

Get information about the license of the product

Línea de comandos

```
ermm.exe get license-info
```

Parámetros

None

Ejemplo

call

```
{
"command":"get_license_info",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"type":"NFR",
"expiration_date":"2020-12-31",
"expiration_state":"ok",
"public_id":"3XX-7ED-7XF",
"seat_id":"6f726793-ae95-4e04-8ac3-e6a20bc620bf",
"seat_name":"M"
},
"error":null
}
```

get logs

Get logs of the product

Línea de comandos

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-
date "2017-04-04 12-00-00"
```

Parámetros

Name	Value
name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

Ejemplo

call

```
{
"command":"get_logs",
"id":1,
"version":"1",
"params":{
"name":"warnlog",
"start_date":"2017-04-04 06-00-00",
"end_date":"2017-04-04 12-00-00"
}
}
```

result

```
{
"id":1,
"result":{
"warnlog":{
"display_name":"Events",
"logs":[{
"Time":"2017-04-04 06-05-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15198 (20170404).",
"UserData":""
},{
"Time":"2017-04-04 11-12-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15199 (20170404).",
"UserData":""
}]
}
},
"error":null
}
```

get activation-status

Get information about the last activation. Result of status can be { success, running, failure }

Línea de comandos

```
ermm.exe get activation-status
```

Parámetros

None

Ejemplo

call

```
{
"command":"get_activation_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"status":"success"
},
"error":null
}
```

get scan-info

Obtenga información sobre un análisis que está ejecución.

Línea de comandos

```
ermm.exe get scan-info
```

Parámetros

Ninguno

Ejemplo

llamada

```
{
"command":"get_scan_info",
"id":1,
"version":"1"
}
```

resultado

```
{
"id":1,
"result":{
"scan-info":{
"scans":[{
"scan_id":65536,
"timestamp":272,
"state":"finished",
"pause_scheduled_allowed":false,
"pause_time_remain":0,
"start_time":"2017-06-20T12:20:33Z",
"elapsed_tickcount":328,
"exit_code":0,
"progress_filename":"Operating memory",
"progress_arch_filename":"",
"total_object_count":268,
"infected_object_count":0,
"cleaned_object_count":0,
"log_timestamp":268,
"log_count":0,
"log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
"username":"test-PC\\test",
"process_id":3616,
"thread_id":3992,
"task_type":2
}],
"pause_scheduled_active":false
}
},
"error":null
}
```


get configuration

Get the product configuration. Result of status may be { success, error }

Línea de comandos

```
ermm.exe get configuration --file C:\tmp\conf.xml --format xml
```

Parámetros

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

Ejemplo

call

```
{
"command":"get_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml"
}
}
```

result

```
{
"id":1,
"result":{
"configuration":"PD94bWwgdmVyc2lvbj0iMS4w=="
},
"error":null
}
```

get update-status

Get information about the update. Result of status may be { success, error }

Línea de comandos

```
ermm.exe get update-status
```

Parámetros

None

Ejemplo

call

```
{
"command":"get_update_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"last_update_time":"2017-06-20 13-21-37",
"last_update_result":"error",
"last_successful_update_time":"2017-06-20 11-21-45"
},
"error":null
}
```

start scan

Start scan with the product

Línea de comandos

```
ermm.exe start scan --profile "profile name" --target "path"
```

Parámetros

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

Ejemplo

call

```
{
"command":"start_scan",
"id":1,
"version":"1",
"params":{
"profile":"Smart scan",
"target":"c:\\"
}
}
```

result

```
{
"id":1,
"result":{
"task_id":458752
},
"error":null
}
```

start activation

Start activation of product

Línea de comandos

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

Parámetros

Name	Value
key	Activation key

offline	Path to offline file

Ejemplo

call

```
{
"command":"start_activation"
"id":1,
"version":"1",
"params":{
"key":"XXXX-XXXX-XXXX-XXXX-XXXX"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start deactivation

Start deactivation of the product

Línea de comandos

```
ermm.exe start deactivation
```

Parámetros

None

Ejemplo

call

```
{
"command":"start_deactivation",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start update

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

Línea de comandos

```
ermm.exe start update
```

Parámetros

None

Ejemplo

call

```
{
"command":"start_update",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":{
"id":4,
"text":"Task already running."
}
}
```

set configuration

Set configuration to the product. Result of status may be { success, error }

Línea de comandos

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

Parámetros

Name	Value
file	the path where the configuration file will be saved
password	password for configuration
value	configuration data from the argument (encoded in base64)

Ejemplo

call

```
{
"command":"set_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml",
"password": "pass"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

Intervalo de comprobación de la licencia

ESET Endpoint Antivirus necesita conectarse a los servidores de licencias de ESET de manera automática. Puede limitar el número de conexiones al servidor de licencias de ESET en Configuración avanzada > **Herramientas** > **Licencia**. De forma predeterminada, la **Verificación de intervalo** se establece en **Automática** y la conexión se establece varias veces cada hora. Si el tráfico de red aumenta, cambie el ajuste de **Verificación de intervalo** a **Limitado** para reducir la sobrecarga. Si se selecciona **Limitado**, ESET Endpoint Antivirus contacta con el servidor de licencias una vez al día o cuando el ordenador se reinicia.

Si el ajuste **Intervalo de comprobación** está ajustado en **Limitado**, todos los cambios relacionados con la licencia efectuados mediante ESET HUB/ESET MSP Administrator pueden tardar hasta un día en aplicarse a la configuración de ESET Endpoint Antivirus.

Archivos de registro

Se puede acceder a la configuración de registro de ESET Endpoint Antivirus en Configuración avanzada > **Herramientas** > **Archivos de registro**. La sección de registros se utiliza para definir cómo se gestionarán los registros. El programa elimina automáticamente los registros antiguos para ahorrar espacio en el disco duro. Puede especificar las siguientes opciones para los archivos de registro:

Nivel mínimo de detalle al registrar: especifica el nivel de contenido mínimo de los sucesos que se van a registrar:

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Advertencias**: registra errores graves y mensajes de alerta.
- **Errores**: se registran los errores graves y errores del tipo "Error al descargar el archivo".
- **Críticos**: registra únicamente los errores graves (errores al iniciar la protección antivirus, etc.).

Al seleccionar el nivel de detalle de **diagnóstico** se registrarán todas las conexiones bloqueadas.

Las entradas de registro anteriores al número de días especificado en el campo **Eliminar automáticamente los registros con una antigüedad de más de (días)** se eliminarán de manera automática.

Optimizar archivos de registro automáticamente: si se selecciona esta opción, los archivos de registro se desfragmentarán automáticamente si el porcentaje de fragmentación es superior al valor especificado en **Si la cantidad de registros eliminados supera el (%)**.

Haga clic en **Optimizar** para empezar la desfragmentación de los archivos de registro. Todas las entradas de registro vacías se eliminan durante este proceso para aumentar el rendimiento y la velocidad de procesamiento del registro. Esta mejora es especialmente notable cuando los registros contienen muchas entradas.

Active **Habilitar formato del texto** para activar el almacenamiento de registros en otro formato de archivo, independiente de Archivos de registro:

- **Directorio de destino**: seleccione el directorio donde se almacenarán los archivos de registro (solo se aplica a los formatos de texto y CSV). Puede copiar la ruta o seleccionar otro directorio haciendo clic en **Borrar**. Cada sección de registros tiene su propio archivo con un nombre de archivo predefinido (por ejemplo, *virlog.txt* para la sección **Amenazas detectadas** de Archivos de registro, si se utiliza el formato de archivo de texto plano para almacenar registros).
- **Tipo**: si selecciona el formato de archivo **Texto**, los registros se almacenarán en un archivo de texto y los datos se separarán mediante tabuladores. El comportamiento es el mismo para el formato de archivo **CSV** con datos separados por comas. Si selecciona **Suceso**, los registros se almacenarán en el registro de eventos de Windows (que se puede ver en el Visor de eventos del Panel de control), en vez de en un archivo.
- **Eliminar todos los archivos de registro**: borra todos los registros almacenados que se seleccionen en el menú desplegable **Tipo**. Se mostrará una notificación sobre la correcta eliminación de los archivos de registro.

Activar control de cambios de configuración en el registro de auditoría: le informa sobre cada cambio de configuración. Consulte Registros de auditoría si desea más información.

ESET podría solicitarle los registros de su ordenador para agilizar la solución de problemas. ESET Log Collector facilita la recopilación de los datos necesarios. Para obtener más información sobre ESET Log Collector, consulte el artículo de la base de conocimiento de ESET.

Modo de presentación

El modo de presentación es una función para usuarios que exigen un uso del software sin interrupciones y sin ventanas de notificación o alerta, así como un menor uso de la CPU. Este modo también se puede utilizar para que las presentaciones no se vean interrumpidas por la actividad del módulo antivirus. Al activar esta característica se desactivan todas las ventanas emergentes y la actividad del planificador de tareas se detiene por completo. La protección del sistema sigue ejecutándose en segundo plano, pero no requiere la intervención del usuario.

Puede activar o desactivar el Modo de presentación en la ventana principal del programa, dentro de **Configuración** > **Ordenador**. Para ello, haga clic en  o en  junto a **Modo de presentación**. Activar el modo de presentación constituye un riesgo de seguridad potencial, por lo que el icono de estado de la protección disponible en la barra de tareas se volverá naranja y mostrará un signo de alerta. Esta alerta también

se puede ver en la ventana principal del programa donde verá el mensaje **Modo de presentación activo** en naranja.

Active la opción **Activar el modo de presentación automáticamente al ejecutar aplicaciones en pantalla completa** en Configuración avanzada > **Herramientas** > **Modo de presentación** para que el Modo de presentación se active cuando inicie una aplicación a pantalla completa y se detenga cuando cierre dicha aplicación.

Active **Desactivar el modo de presentación automáticamente después de** para definir la cantidad de tiempo que tardará en desactivarse el modo de presentación automáticamente.

Diagnóstico

El diagnóstico proporciona volcados de memoria de los procesos de ESET (por ejemplo, ekrn). Cuando una aplicación se bloquea, se genera un volcado de memoria. Puede ayudar a los desarrolladores a depurar y arreglar ESET Endpoint Antivirus problemas diversos.

Haga clic en el menú desplegable situado junto a **Tipo de volcado** y seleccione una de las tres opciones disponibles:

- Seleccione **Desactivar** para desactivar esta característica.
- **Mini** (predeterminado): registra la información mínima necesaria para identificar el motivo del bloqueo inesperado de la aplicación. Este tipo de archivo de volcado puede resultar útil cuando el espacio es limitado, pero dada la poca información que contiene, es posible que el análisis de este archivo no detecte los errores que no estén relacionados directamente con el subproceso que se estaba ejecutando cuando se produjo el problema.
- **Completo**: registra todo el contenido de la memoria del sistema cuando la aplicación se detiene de forma inesperada. Los volcados de memoria completos pueden contener datos de procesos que se estaban ejecutando cuando se generó el volcado.

Directorio de destino: directorio en el que se genera el volcado durante el bloqueo.

Abrir la carpeta de diagnóstico: haga clic en **Abrir** para abrir este directorio en una ventana nueva del *Explorador de Windows*.

Crear volcado de diagnóstico: haga clic en **Crear** para crear archivos de volcado de diagnóstico en el **Directorio de destino**.

Registro avanzado

Activar registro avanzado del análisis del ordenador: registrar todos los sucesos que tienen lugar durante el análisis de archivos y carpetas del análisis del ordenador o de la protección del sistema de archivos en tiempo real.

Activar registro avanzado de Control de dispositivos: registrar todos los sucesos que tienen lugar en Control de dispositivos. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con Control de dispositivos.

Habilitar el registro avanzado de Direct Cloud – Registrar toda la comunicación del producto entre el producto y los servidores de Direct Cloud.

Activar registro avanzado de la Protección de documentos: registre todos los sucesos que se produzcan en la

Protección de documentos para permitir el diagnóstico y la resolución de problemas.

Activar registro avanzado de la protección del cliente de correo electrónico: registra todos los sucesos que tienen lugar en la Protección del cliente de correo electrónico y el complemento del cliente de correo electrónico para permitir diagnosticar y resolver problemas.

Activar registro avanzado del núcleo: registra todos los eventos que tienen lugar en el servicio de núcleo de ESET (ekrn) para poder diagnosticar y resolver problemas.

Activar registro avanzado de licencias: registra toda la comunicación del producto con los servidores de activación y licencias de ESET.

Activar seguimiento de memoria: registre todos los eventos que ayudarán a los desarrolladores a diagnosticar fugas de memoria.

Activar registro avanzado de la protección de la red: registrar los datos de red que pasan a través del cortafuegos en formato PCAP. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con el cortafuegos.

Activar registro avanzado del analizador de tráfico de red: registre todos los datos que pasan a través del analizador de tráfico de red en el formato PCAP para ayudar a los desarrolladores a diagnosticar y solucionar problemas relacionados con el analizador de tráfico de red

Activar registro avanzado del sistema operativo: se recopilará información adicional sobre el sistema operativo, tal como los procesos en ejecución, la actividad de la CPU, las operaciones del disco, etc. Estos datos pueden ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con el producto de ESET que se ejecuta en su sistema operativo.

Activar registro avanzado de mensajes push – Registre todos los sucesos que se produzcan durante los mensajes push para permitir el diagnóstico y la resolución de problemas.

Activar el registro avanzado de la Protección del sistema de archivos en tiempo real: registrar todos los sucesos que se produzcan en la Protección del sistema de archivos en tiempo real para permitir el diagnóstico y la solución de problemas.

Activar registro avanzado del motor de actualización: registrar todos los eventos que se producen durante el proceso de actualización. Esto puede ayudar a los desarrolladores a diagnosticar y corregir los problemas relacionados con el motor de actualización.

Activar el registro avanzado de la Administración de parches y vulnerabilidades: registra todos los eventos de Administración de parches y vulnerabilidades. Este ajuste solo se muestra si la función Administración de parches y vulnerabilidades está activada en el entorno (activada en ESET PROTECT Cloud).

Los archivos de registro se encuentran en *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Soporte técnico

Cuando se pondrá en contacto con el servicio de soporte técnico de ESET desde ESET Endpoint Antivirus, puede enviar datos de configuración del sistema. Seleccione **Enviar siempre** en el menú desplegable **Enviar datos de configuración del sistema** para enviar los datos automáticamente, o seleccione **Preguntar antes de enviar** antes de que se envíen los datos.

Conectividad

En las redes locales de gran tamaño, un servidor proxy puede mediar en la comunicación entre su ordenador e Internet. Si está utilizando un servidor proxy, debe definir la siguiente configuración. De lo contrario, ESET Endpoint Antivirus y sus módulos no se pueden actualizar automáticamente. En ESET Endpoint Antivirus, la configuración del servidor proxy está disponible en dos secciones diferentes de Configuración avanzada.

En primer lugar, se puede configurar en Configuración avanzada > **Conectividad** > **Servidor Proxy**. Al especificar el servidor Proxy en este nivel, se define la configuración global del servidor Proxy para ESET Endpoint Antivirus. Todos los módulos que requieran conexión a Internet utilizarán estos parámetros.

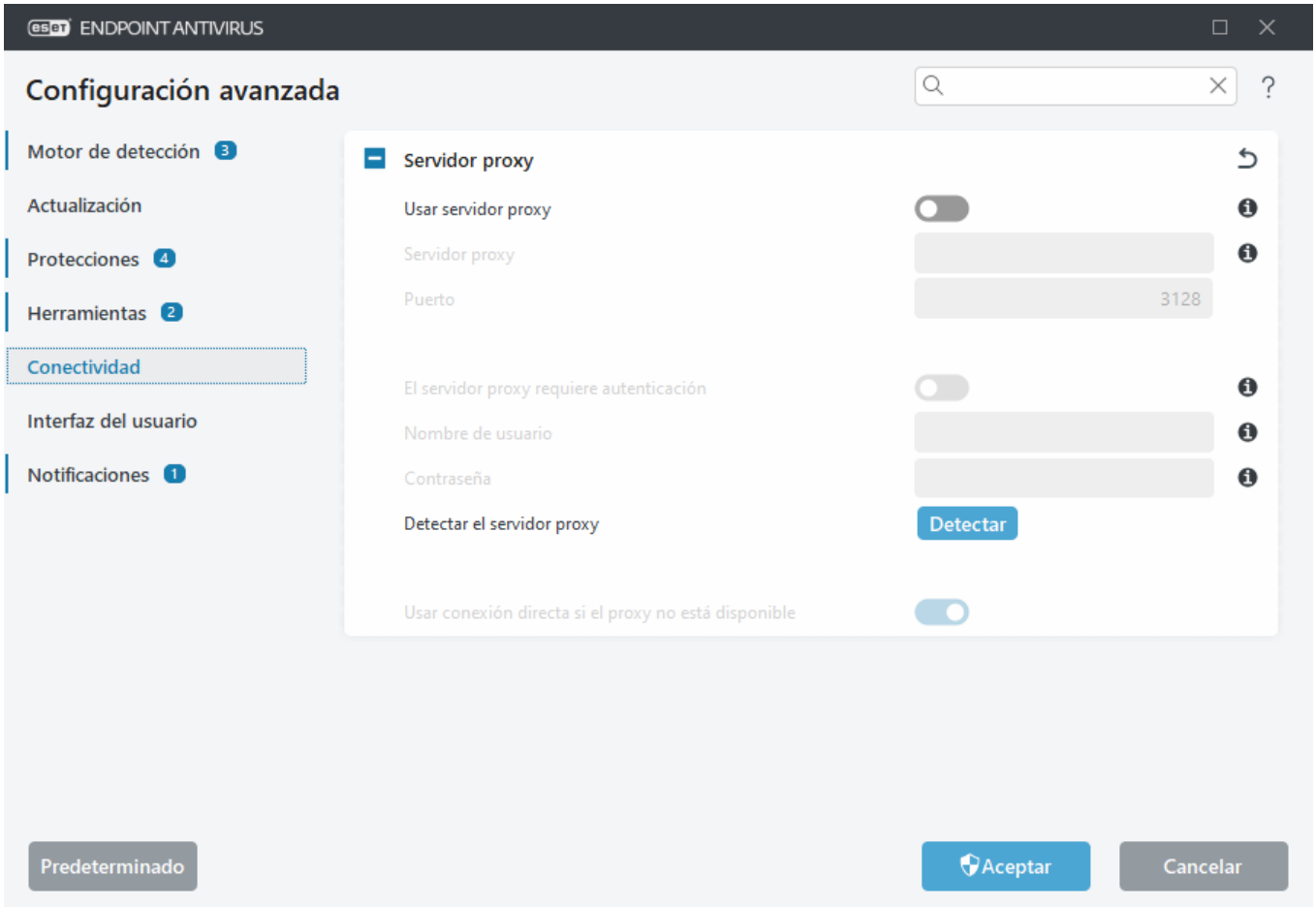
Para especificar la configuración global del servidor proxy, habilite **Usar servidor proxy** y escriba la **dirección del servidor proxy** junto con el número de **puerto** del servidor proxy.

Si la comunicación con el servidor proxy requiere autenticación, seleccione **El servidor proxy requiere autenticación** e introduzca un **nombre de usuario** y una **contraseña** válidos en los campos correspondientes. Haga clic en **Detectar el servidor proxy** para detectar y cumplimentar la configuración del servidor proxy de forma automática. Para buscar la configuración del proxy en su sistema operativo, pulse las teclas de método abreviado **Windows + I** y haga clic en **Redes e Internet** > **Proxy**. ESET Endpoint Antivirus copiará los parámetros especificados en las Opciones de Internet de Internet Explorer o Google Chrome.

> Debe especificar el nombre de usuario y la contraseña manualmente en la configuración del **Servidor proxy**.

Usar conexión directa si el proxy no está disponible: si ESET Endpoint Antivirus está configurado para conectarse mediante proxy y es imposible conectar con el proxy, ESET Endpoint Antivirus omitirá el proxy y se conectará directamente con los servidores de ESET.

La configuración del servidor proxy también se puede definir en Configuración avanzada > **Actualización** > **Perfiles** > **Actualizaciones** > **Opciones de conexión**; para ello, seleccione **Conexión a través de un servidor proxy** en el menú desplegable **Modo proxy**. Esta configuración se aplica solo para actualizaciones y se recomienda para equipos portátiles que reciben actualizaciones de módulos desde ubicaciones remotas. Para obtener más información, consulte Configuración avanzada de actualizaciones.



Interfaz del usuario

Para configurar el comportamiento de la interfaz gráfica de usuario (GUI) del programa, abra Configuración avanzada > **Interfaz de usuario**.

Puede ajustar el aspecto visual del programa y los efectos utilizados en la pantalla Configuración avanzada de elementos de la interfaz del usuario.

Si desea disponer del máximo nivel de seguridad del software de seguridad, proteja la configuración mediante una contraseña para impedir la desinstalación o los cambios no autorizados con la herramienta Configuración de acceso.

> Consulte el apartado Notificaciones para configurar el comportamiento de las notificaciones del sistema, las alertas de detección y los estados de la aplicación.

El Modo de presentación es útil para usuarios que deseen trabajar con una aplicación sin la interrupción de ventanas emergentes, tareas programadas y cualquier componente que cargue el procesador y la memoria RAM.

Consulte también Cómo minimizar la interfaz de usuario de ESET Endpoint Antivirus (útil para entornos administrados).

Elementos de la interfaz del usuario

Las opciones de configuración de la interfaz de usuario de ESET Endpoint Antivirus le permiten ajustar el entorno de trabajo según sus necesidades. Estas opciones de configuración están disponibles en la sección **Configuración avanzada** (F5) > **Interfaz de usuario** > **Elementos de la interfaz de usuario**.

En la sección **Elementos de la interfaz del usuario** puede ajustar el entorno de trabajo. Utilice el menú desplegable **Modo de inicio** para seleccionar uno de los siguientes modos de inicio de la interfaz gráfica de usuario (GUI):

Completo: se muestra la GUI completa.

Mínimo: la GUI se está ejecutando, pero el usuario solo ve las notificaciones.

Manual: la GUI no se abre automáticamente al iniciar sesión; cualquier usuario puede abrirla de forma manual.

Silencioso: no se muestran notificaciones ni alertas. Solo el administrador puede abrir la GUI. Este modo puede resultar útil en entornos administrados o cuando necesita ahorrar recursos del sistema.

> Cuando se seleccione el modo de inicio de GUI Mínimo y se reinicie el ordenador las notificaciones se mostrarán, pero la interfaz gráfica no. Para volver al modo de interfaz gráfica de usuario completa, ejecute la interfaz gráfica desde el menú Inicio en **Todos los programas** > **ESET** > ESET Endpoint Antivirus como administrador, o hágalo desde ESET PROTECT utilizando una política.

Modo de color: seleccione el esquema de colores de la interfaz gráfica de usuario de ESET Endpoint Antivirus en el menú desplegable:

- **Igual que el color del sistema**: el esquema de colores de ESET Endpoint Antivirus se definirá según la configuración del sistema operativo.
- **Oscuro**: ESET Endpoint Antivirus tendrá un esquema de colores oscuros (modo oscuro).
- **Claro**: ESET Endpoint Antivirus tendrá un esquema de colores estándar y claro.

> También puede seleccionar el esquema de colores de la interfaz gráfica de usuario de ESET Endpoint Antivirus en la esquina superior derecha de la ventana principal del programa.

Si desea desactivar la pantalla inicial de ESET Endpoint Antivirus, anule la selección de **Mostrar pantalla inicial con la carga del sistema**.

Si desea que ESET Endpoint Antivirus reproduzca un sonido cuando se produzcan sucesos importantes durante un análisis, por ejemplo al detectar una amenaza o al finalizar el análisis, seleccione **Usar señal acústica**.

Integrar en el menú contextual: integra los elementos de control de ESET Endpoint Antivirus en el menú contextual.

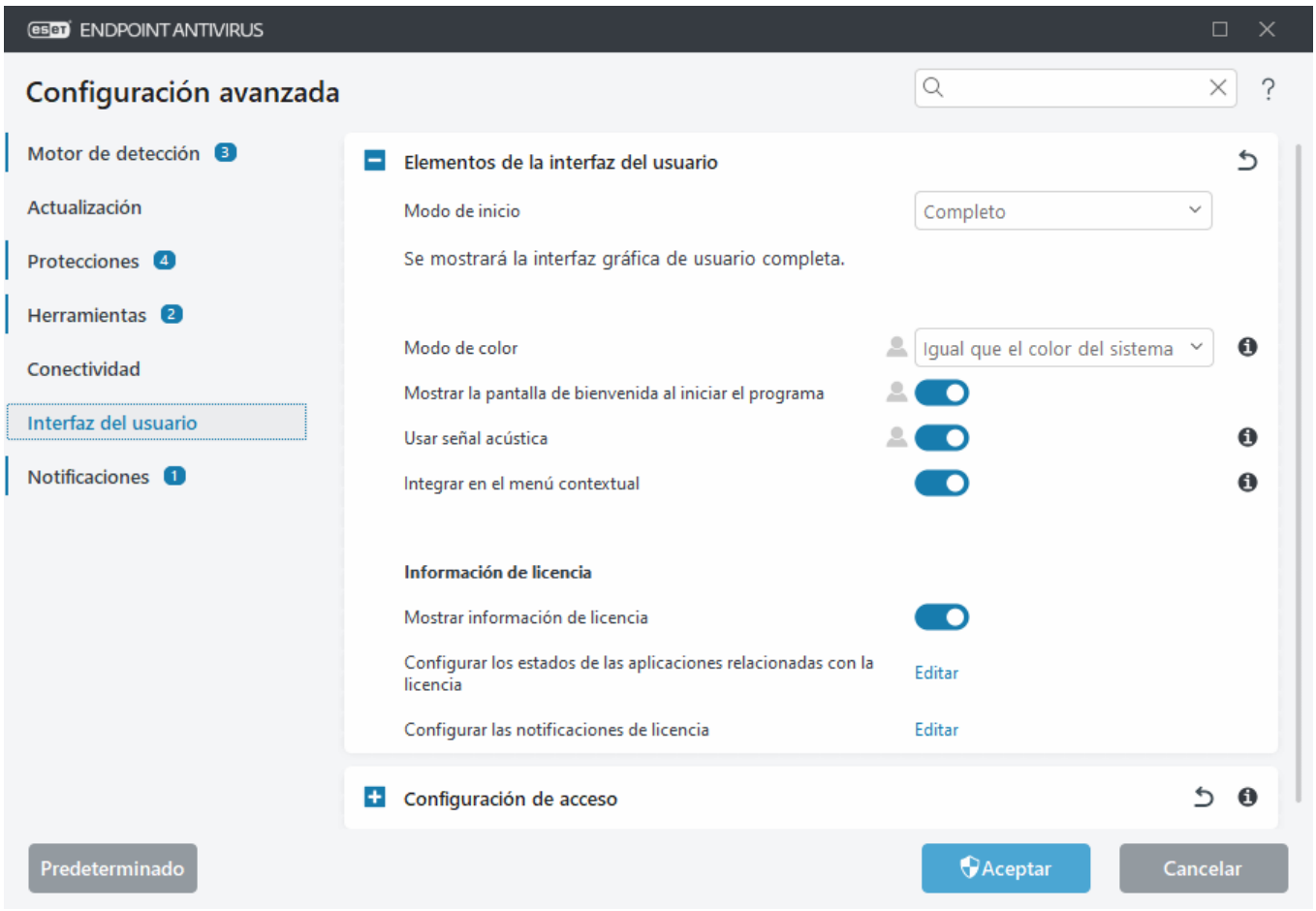
Información de licencia

Mostrar información de licencia: cuando esta opción esté desactivada, no se mostrará la fecha de caducidad de la licencia en **Estado de protección** ni en la pantalla **Ayuda y soporte**.

Configurar los estados de las aplicaciones relacionadas con la licencia: abre la lista de estados de las aplicaciones relacionadas con la licencia.

Configurar las notificaciones de licencia: abre la lista de notificaciones relacionadas con la licencia.

> En las instancias de ESET Endpoint Antivirus activadas con licencia MSP, los ajustes de información de la licencia se aplican pero no son accesibles.



Configuración de acceso

La configuración de ESET Endpoint Antivirus es una parte crucial de la política de seguridad. Las modificaciones no autorizadas pueden poner en peligro la estabilidad y la protección del sistema. Para evitar modificaciones no autorizadas, los parámetros de configuración y la desinstalación de ESET Endpoint Antivirus se pueden proteger mediante contraseña. La configuración de acceso se puede configurar en Configuración avanzada > **Interfaz de usuario** > **Configuración de acceso**.

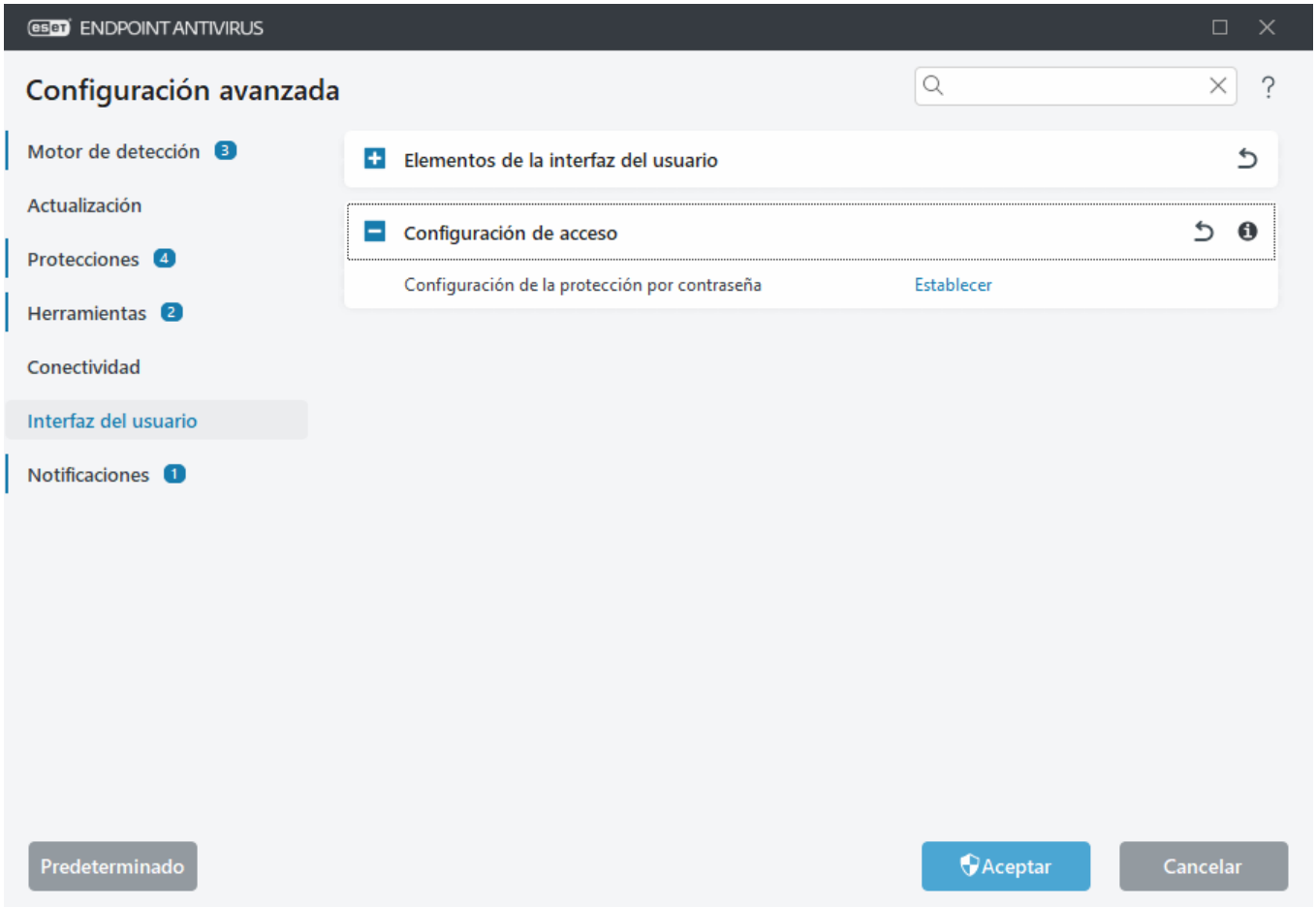
Para establecer una contraseña para proteger los parámetros de configuración y la desinstalación de ESET Endpoint Antivirus, haga clic en el botón **Establecer** junto a **Configuración de protección de contraseña**.

Para cambiar la contraseña, haga clic en **Cambiar contraseña** junto a **Configuración de protección de contraseña**.

Para quitar la contraseña, haga clic en **Quitar** junto a **Configuración de protección de contraseña**.

Entornos administrados

El administrador puede crear una política para proteger la configuración de ESET Endpoint Antivirus con una contraseña en los ordenadores cliente conectados. Para crear una política nueva, consulte Configuración protegida con contraseña.



Contraseña de Configuración avanzada

Para proteger la configuración avanzada de ESET Endpoint Antivirus y evitar modificaciones no autorizadas, escriba la nueva contraseña en los campos **Nueva contraseña** y **Confirmar contraseña**. Haga clic en **Aceptar**.

Entornos administrados

El administrador puede crear una política para proteger la configuración de ESET Endpoint Antivirus con una contraseña en los ordenadores cliente conectados. Para crear una política nueva, consulte Configuración protegida con contraseña.

No administrado

Si desea cambiar una contraseña:

1. Escriba la contraseña anterior en el campo **Contraseña anterior**.
2. Escriba la nueva contraseña en los campos **Nueva contraseña** y **Confirmar contraseña**.
3. Haga clic en **Aceptar**.

Esta contraseña será necesaria para realizar modificaciones futuras en ESET Endpoint Antivirus.

Si ha olvidado su contraseña, consulte Desbloquear contraseña de configuración en los productos de ESET Endpoint.

Para recuperar la clave de licencia de ESET, la fecha de caducidad o cualquier otra información sobre la licencia de

ESET Endpoint Antivirus, consulte He perdido el nombre de usuario y la clave de licencia/contraseña.

Contraseña

Para evitar modificaciones no autorizadas, los parámetros de configuración de ESET Endpoint Antivirus se pueden proteger mediante contraseña.

Modo seguro

Si la interfaz gráfica de ESET Endpoint Antivirus se ejecuta en modo seguro, aparecerá un cuadro de diálogo indicando que la aplicación se debe ejecutar en modo seguro. Dado que en este modo el funcionamiento de todos los programas es limitado, no es posible abrir la interfaz gráfica de ESET Endpoint Antivirus como en el modo estándar.

La ventana que se muestra le permitirá ejecutar un análisis del ordenador. Si desea buscar código malicioso en su ordenador, seleccione la opción **Sí**.

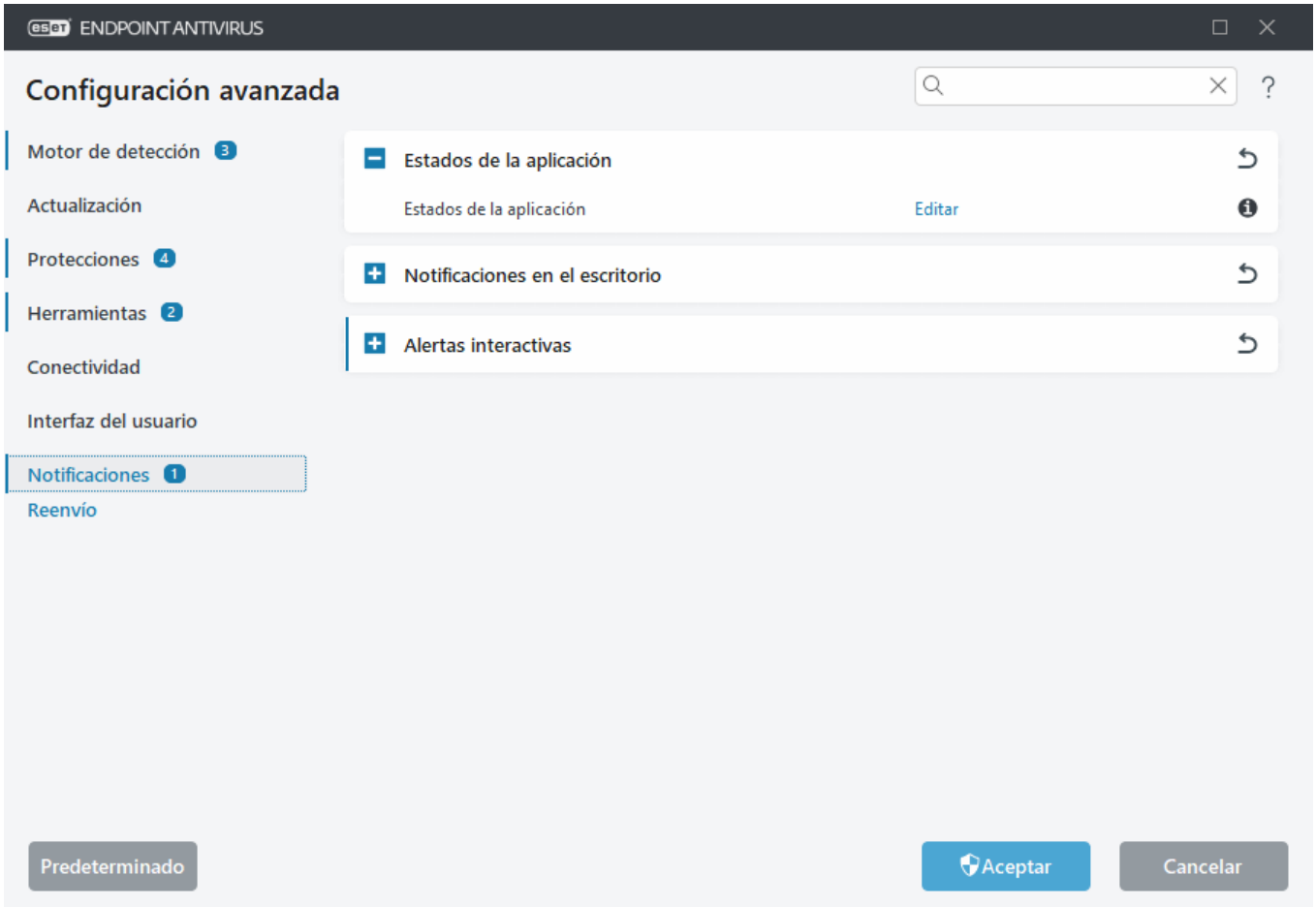
De esta forma, el análisis se realizará en una ventana distinta con los mismos parámetros que el perfil de análisis del ordenador predeterminado tras la instalación de ESET Endpoint Antivirus.

Seleccione la opción **No** para cerrar el cuadro de diálogo; ESET Endpoint Antivirus no realizará ninguna acción.

Notificaciones

Para administrar las notificaciones de ESET Endpoint Antivirus, abra Configuración avanzada > **Notificaciones**. Puede definir los tipos de notificaciones siguientes:

- Estados de la aplicación: notificaciones que se muestran en la sección de inicio de la ventana principal del programa.
- Notificaciones en el escritorio: pequeñas ventanas de notificación junto a la barra de tareas del sistema.
- Alertas interactivas: ventanas de alerta y cuadros de mensajes que requieren la intervención del usuario.
- Reenvío (Notificaciones por correo electrónico): las notificaciones por correo electrónico se envían a la dirección de correo electrónico especificada.
- Personalización de las notificaciones: agregue un mensaje personalizado a, por ejemplo, una notificación en el escritorio.



Estados de la aplicación

Estados de la aplicación: haga clic en **Editar** para seleccionar los estados de la aplicación que se muestran en la sección de inicio de la ventana principal del programa.

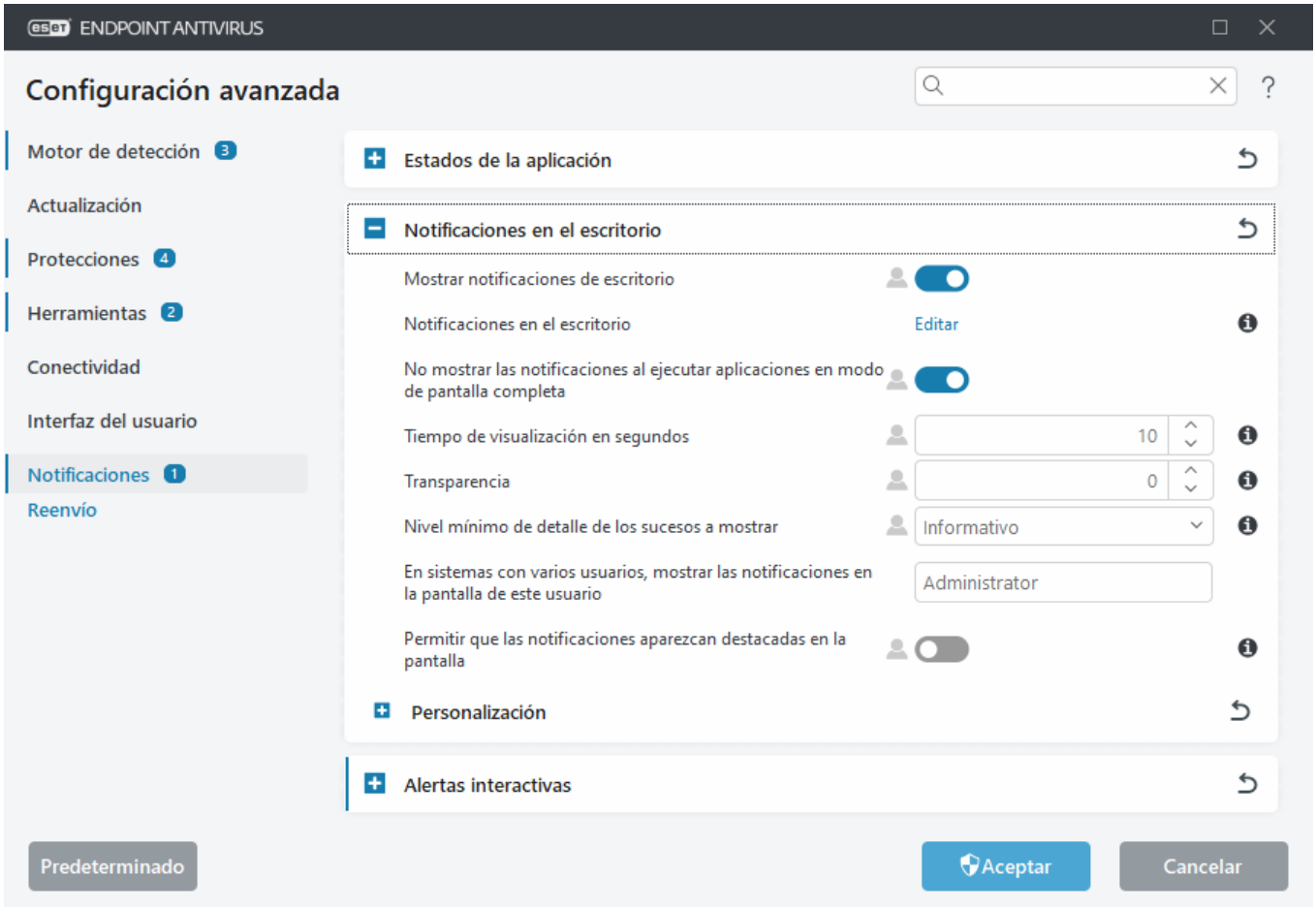
Estados de la aplicación

Para configurar los estados de la aplicación que deben mostrarse (por ejemplo, al pausar la Protección antivirus y antiespía o activar el Modo de presentación), abra Configuración avanzada > **Notificaciones** y haga clic en **Editar** junto a **Estados de la aplicación**.

El estado de la aplicación también se mostrará si su producto no está activado o la licencia ha caducado. Este ajuste puede modificarse a través de Políticas de ESET PROTECT.

Notificaciones en el escritorio

La notificación en el escritorio se representa mediante una pequeña ventana de notificación junto a la barra de tareas del sistema. De forma predeterminada, está configurada para mostrarse durante 10 segundos. Esta es la manera principal en la que ESET Endpoint Antivirus se comunica con el usuario para informarle de actualizaciones correctas de los componentes de los programas, la conexión de nuevos dispositivos, la finalización de tareas de análisis de virus o la detección de nuevas amenazas.



Mostrar notificaciones en el escritorio: se recomienda mantener esta opción activada, para que el producto pueda informarle cuando se produce un suceso nuevo.

Notificaciones en el escritorio: haga clic en **Editar** para activar o desactivar las notificaciones en el escritorio.

No mostrar las notificaciones al ejecutar aplicaciones en modo de pantalla completa: suprime todas las notificaciones que no son interactivas al ejecutar aplicaciones en modo de pantalla completa.

Tiempo de espera en segundos: definir la duración de la visibilidad de la notificación. El valor debe estar entre 3 y 30 segundos.

Transparencia: definir el porcentaje de transparencia de la notificación. El intervalo admitido es de 0 (sin transparencia) a 80 (transparencia muy alta).

Nivel mínimo de detalle de los suceso a mostrar: definir el nivel de gravedad de la notificación inicial mostrado. Seleccione una de las siguientes opciones en el menú desplegable:

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: registra los mensajes informativos, como los sucesos de red no convencionales, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Advertencias**: registra errores graves y mensajes de alerta (por ejemplo, un fallo de actualización).
- **Errores**: se registran los errores (protección de documentos no iniciada) y los errores graves.
- **Críticos**: registra únicamente los errores graves (errores al iniciar la protección antivirus o de infección del sistema).

En sistemas con varios usuarios, mostrar las notificaciones en la pantalla de este usuario: permite que la cuenta seleccionada reciban notificaciones en el escritorio. Por ejemplo, si no utiliza la cuenta de administrador, escriba

el nombre completo de la cuenta para que se muestren las notificaciones en el escritorio relacionadas. Solo una cuenta de usuario puede recibir las notificaciones en el escritorio.

Permitir que las notificaciones aparezcan destacadas en la pantalla: las notificaciones aparecerán destacadas en la pantalla y se podrá acceder a ellas con Alt+Tab.

Personalización de las notificaciones

Esta ventana permite personalizar los mensajes utilizados en notificaciones.

Mensaje de notificación predeterminado: un mensaje predeterminado que se mostrará en el pie de página de las notificaciones.

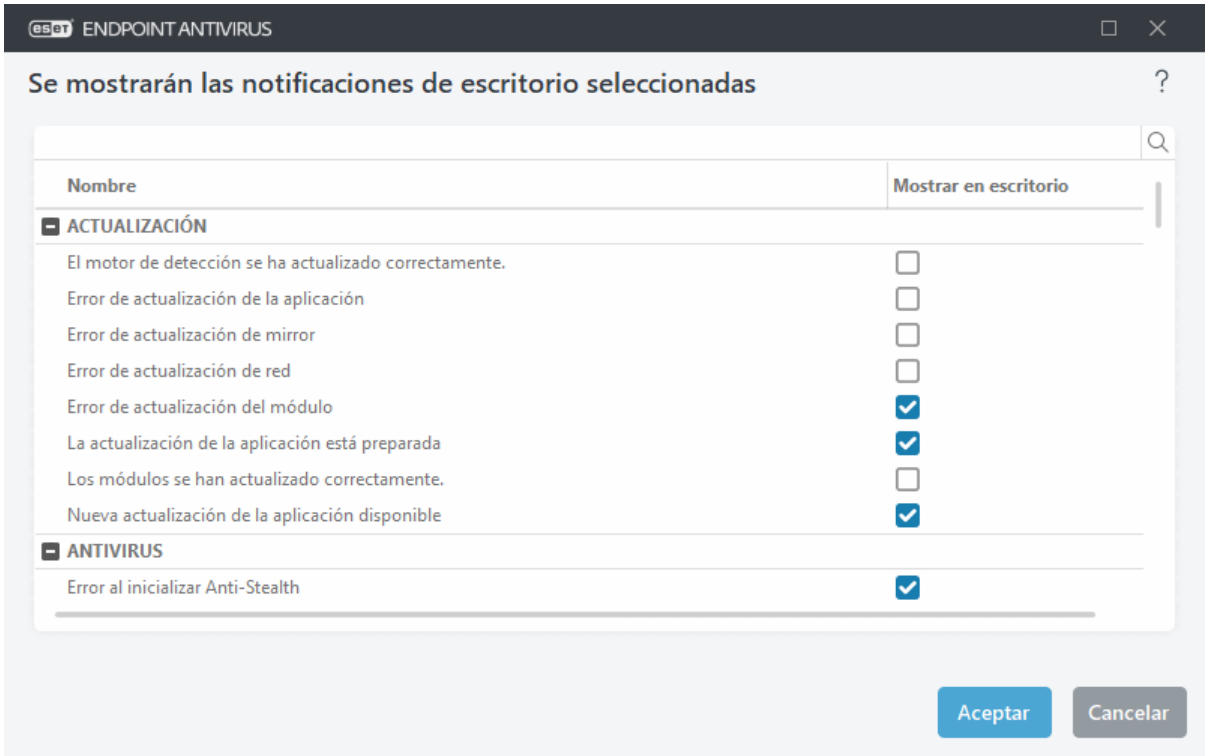
Detecciones

Active **No cerrar las notificaciones de malware automáticamente** para mantener las notificaciones de malware en pantalla hasta que se cierren manualmente.

Desactive **Usar mensaje predeterminado** e introduzca su propio mensaje en el campo **Mensaje de notificación de detección** para utilizar mensajes de notificación personalizados.

Cuadro de diálogo: Notificaciones en el escritorio

Para ajustar la visibilidad de las notificaciones en el escritorio (mostradas en la parte inferior derecha de la pantalla), abra Configuración avanzada > **Notificaciones** > **Notificaciones en el escritorio**. Haga clic en **Editar** junto a **Notificaciones en el escritorio** y marque la casilla **Mostrar en escritorio** adecuada.



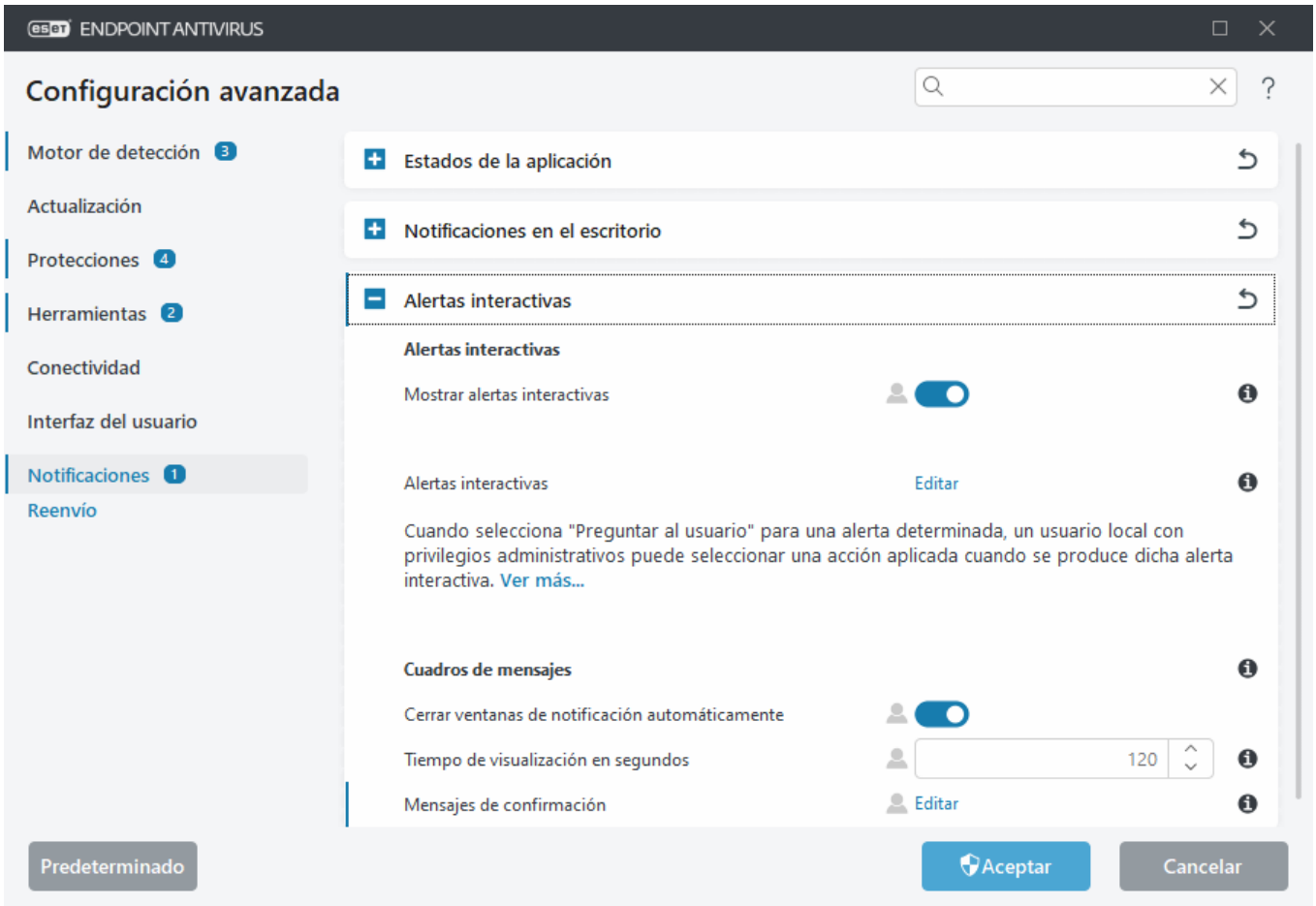
Si desea configurar notificaciones de **Archivo analizado** y **Archivo no analizado** durante el uso de ESET LiveGuard, debe configurarse Protección proactiva en **Bloquear ejecución hasta que se reciban los resultados del análisis**.

Alertas interactivas

¿Busca información sobre alertas y notificaciones habituales?

- Amenaza detectada
- La dirección se ha bloqueado.
- El producto no está activado
- Actualización disponible
- La información de actualización no es consistente
- Solución de problemas para el mensaje "Error de actualización de los módulos"
- "Archivo dañado" o "No se pudo cambiar el nombre del archivo"
- El certificado del sitio web se ha revocado
- Amenaza de red bloqueada
- Archivo bloqueado debido al análisis

La sección **Alertas interactivas** de Configuración avanzada > **Notificaciones** le permite configurar cómo gestiona ESET Endpoint Antivirus los cuadros de mensajes y las alertas interactivas de las detecciones cuando un usuario debe tomar una decisión (por ejemplo, sitios web que pueden ser de phishing).



Alertas interactivas

Si desactiva la opción **Mostrar alertas interactivas**, se ocultarán todas las ventanas de alerta y los cuadros de diálogo del navegador. Solo resulta útil para una serie de situaciones muy específicas.

- A los usuarios no administrados les recomendamos dejar el ajuste predeterminado de esta opción (activada).
- Los usuarios administrados deben dejar activado este ajuste y seleccionar una acción predefinida para los usuarios de Lista de alertas interactivas.

Alertas interactivas: haga clic en **Modificar** para seleccionar qué Alertas interactivas se mostrarán.

Cuadros de mensajes

Para cerrar los cuadros de mensajes automáticamente después de un de tiempo determinado, seleccione la opción **Cerrar cuadros de mensajes automáticamente**. Si no se cierran de forma manual, las ventanas de alerta se cerrarán automáticamente cuando haya transcurrido el periodo de tiempo especificado.

Tiempo de espera en segundos: define la duración de la visibilidad de la alerta. El valor debe estar entre 10 y 999 segundos.

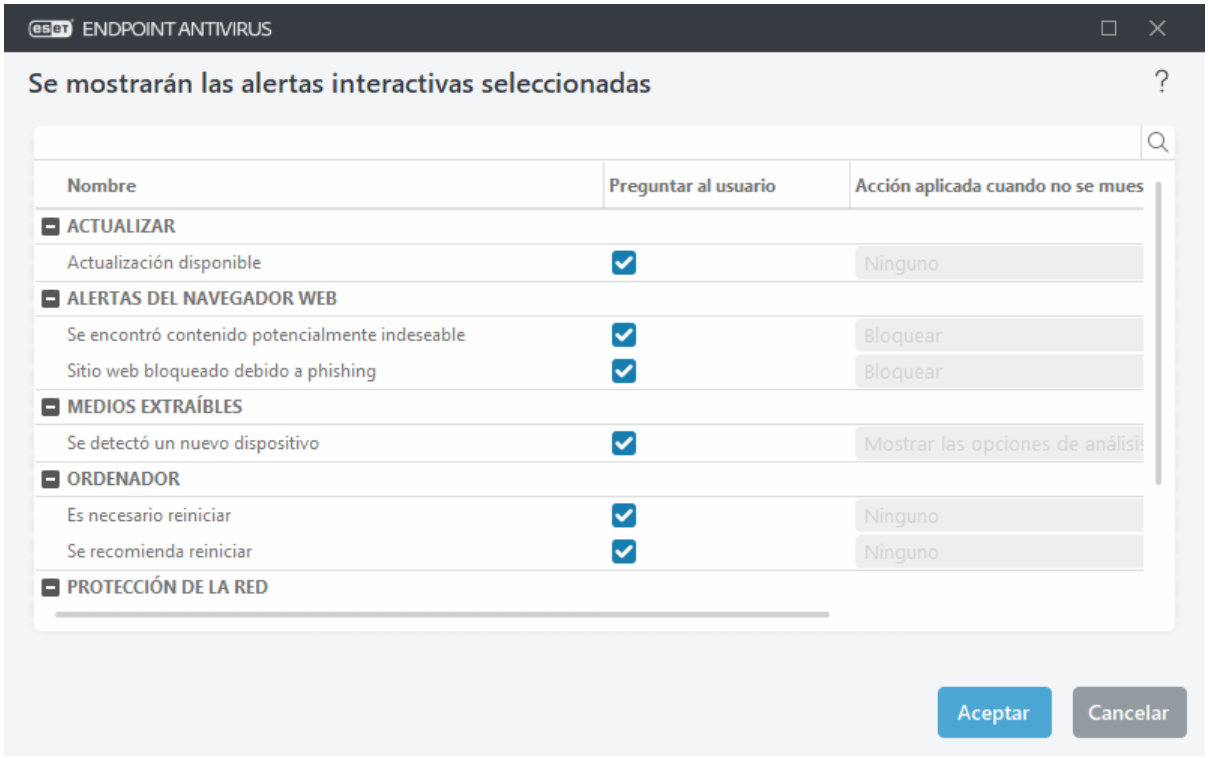
Mensajes de confirmación: haga clic en **Editar** para ver una lista de mensajes de confirmación que se pueden seleccionar para que se muestren o no.

Lista de alertas interactivas

Esta sección resume varias ventanas de alertas interactivas que ESET Endpoint Antivirus mostrará antes de que se realice ninguna acción.

Para ajustar el comportamiento de las alertas interactivas configurables, abra Configuración avanzada > **Notificaciones** > **Alertas interactivas** y haga clic en **Modificar** junto a **Alertas interactivas**.

> Útil en entornos administrados en los que el administrador puede cancelar la selección de **Preguntar al usuario** en todas partes y seleccionar una acción predefinida aplicada cuando se muestran ventanas de alertas interactivas.



Consulte otras secciones de ayuda que hacen referencia a una ventana específica de alerta interactiva:

Unidades extraíbles

- Se detectó un nuevo dispositivo

Protección de la red

- Acceso a la red bloqueado se muestra cuando se activa la tarea del cliente **Aislar ordenador de la red** de esta estación de trabajo desde ESET PROTECT.
- Comunicación de red bloqueada
- Amenaza de red bloqueada

Alertas del navegador web

- Se encontró contenido potencialmente indeseable
- Sitio web bloqueado debido a phishing

Equipo

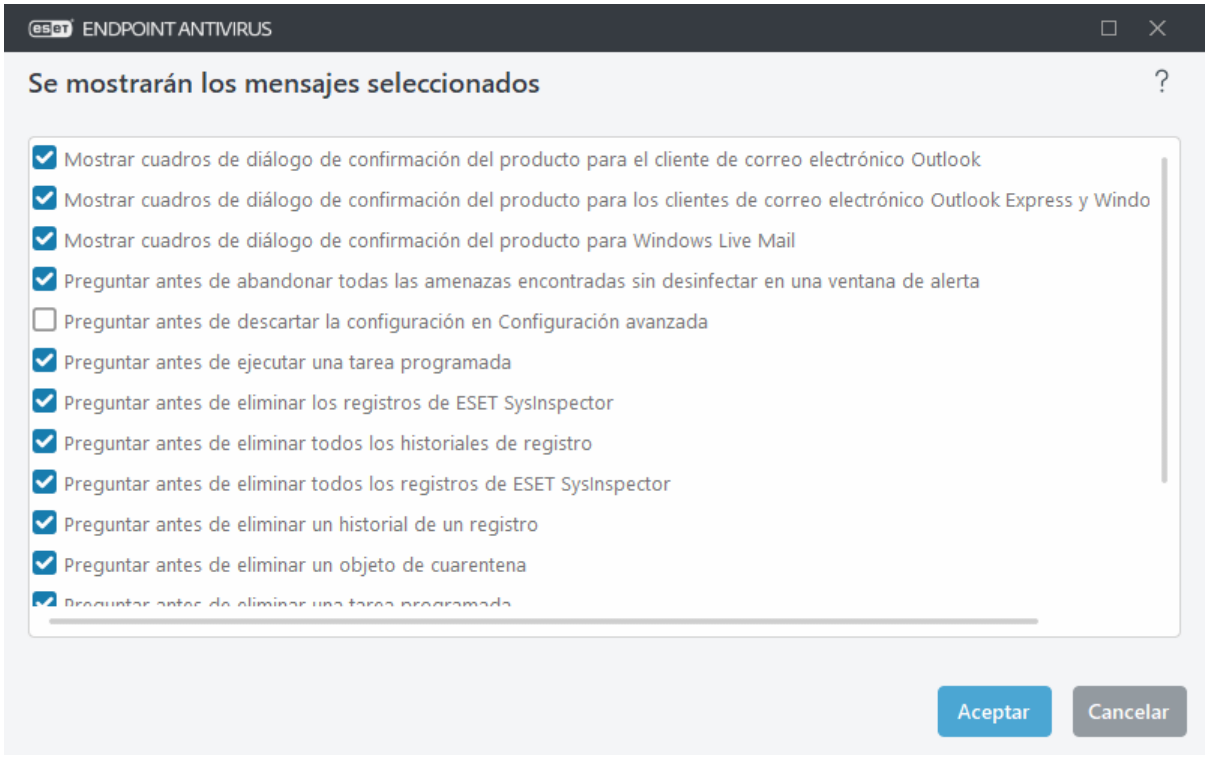
La presencia de estas alertas cambiará el color de la interfaz de usuario:

- Reiniciar el ordenador (obligatorio)
- Reiniciar el ordenador (recomendado)

> Las alertas interactivas no contienen ventanas interactivas de Motor de detección, HIPS o Cortafuegos, pues su comportamiento se puede configurar individualmente en la característica específica.

Mensajes de confirmación

Para ajustar los mensajes de confirmación, vaya Configuración avanzada > **Notificaciones** > **Alertas interactivas** y haga clic en **Editar** junto a **Mensajes de confirmación**.



En este cuadro de diálogo se muestran los mensajes de confirmación que mostrará ESET Endpoint Antivirus antes de que se realice cualquier acción. Seleccione o anule la selección de la casilla de verificación disponible junto a cada mensaje de confirmación para permitirlo o desactivarlo.

Obtenga más información sobre la función específica relacionada con los mensajes de confirmación:

- Preguntar antes de eliminar registros de ESET SysInspector
- Preguntar antes de eliminar todos los registros de ESET SysInspector
- Preguntar antes de eliminar un objeto de cuarentena
- Preguntar antes de descartar la configuración en Configuración avanzada
- Preguntar antes de abandonar todas las amenazas encontradas sin desinfectar en una ventana de alerta
- Preguntar antes de eliminar un historial de un registro
- Preguntar antes de eliminar una tarea programada
- Preguntar antes de eliminar todos los historiales de registro
- Preguntar antes de restablecer las estadísticas
- Preguntar antes de restaurar un objeto de cuarentena
- Preguntar antes de restaurar objetos de cuarentena y excluirlos del análisis
- Preguntar antes de ejecutar una tarea programada
- Mostrar cuadros de diálogo de confirmación del producto para los clientes de correo electrónico Outlook Express y Windows Mail
- Mostrar cuadros de diálogo de confirmación del producto para Windows Live Mail
- Mostrar cuadros de diálogo de confirmación del producto para el cliente de correo electrónico Outlook

Error de conflicto de configuración avanzada

Este error se puede producir si algún componente (p. ej., HIPS) y el usuario crean las reglas en modo de aprendizaje o interactivo al mismo tiempo.

Se recomienda cambiar el modo de filtrado al **modo automático** predeterminado si quiere crear sus propias reglas. Más información acerca de HIPS y los modos de filtrado de HIPS.

Es necesario reiniciar

Se debe reiniciar el ordenador después de actualizar ESET Endpoint Antivirus a una versión nueva o aplicar parches a las aplicaciones mediante la Administración de parches y vulnerabilidades. Las versiones nuevas de ESET Endpoint Antivirus implementan mejoras o solucionan problemas que no se pueden resolver con las actualizaciones automáticas de los módulos de programa.

Haga clic en **Reiniciar ahora** para reiniciar el ordenador. Si tiene pensado reiniciar el ordenador más tarde, haga clic en **Recordármelo más tarde**. Posteriormente, puede reiniciar el ordenador manualmente desde la sección **Estado de la protección** de la ventana principal del programa.

Para desactivar las alertas "Es necesario reiniciar" o "Se recomienda reiniciar", siga los pasos que se indican a continuación:

1. Abra **Configuración avanzada** (F5) > **Notificaciones** > **Alertas interactivas**.
2. Haga clic en **Modificar** junto a **Alertas interactivas**. En la sección **Ordenador**, desmarque las casillas de verificación situadas junto a **Reiniciar el ordenador (obligatorio)** y **Reiniciar el ordenador (recomendado)**.
3. Haga clic en **Aceptar** para guardar sus cambios en las dos ventanas abiertas.
4. Las alertas ya no aparecerán en la máquina del punto de conexión.
5. (opcional) Para desactivar el estado de la aplicación en la ventana del programa principal de ESET Endpoint Antivirus, en la ventana Estados de la aplicación, desmarque las casillas de verificación situadas junto a **Es necesario reiniciar el ordenador** y **Es recomendable reiniciar el ordenador**.

Se recomienda reiniciar

Después de actualizar ESET Endpoint Antivirus a una nueva versión es necesario reiniciar el ordenador. Las versiones nuevas de ESET Endpoint Antivirus implementan mejoras o solucionan problemas que no se pueden resolver con las actualizaciones automáticas de los módulos de programa.

Haga clic en **Reiniciar ahora** para reiniciar el ordenador. Si tiene pensado reiniciar el ordenador más tarde, haga clic en **Recordármelo más tarde**. Posteriormente, puede reiniciar el ordenador manualmente desde la sección **Estado de la protección** de la ventana principal del programa.

Para desactivar las alertas "Es necesario reiniciar" o "Se recomienda reiniciar", siga los pasos que se indican a continuación:

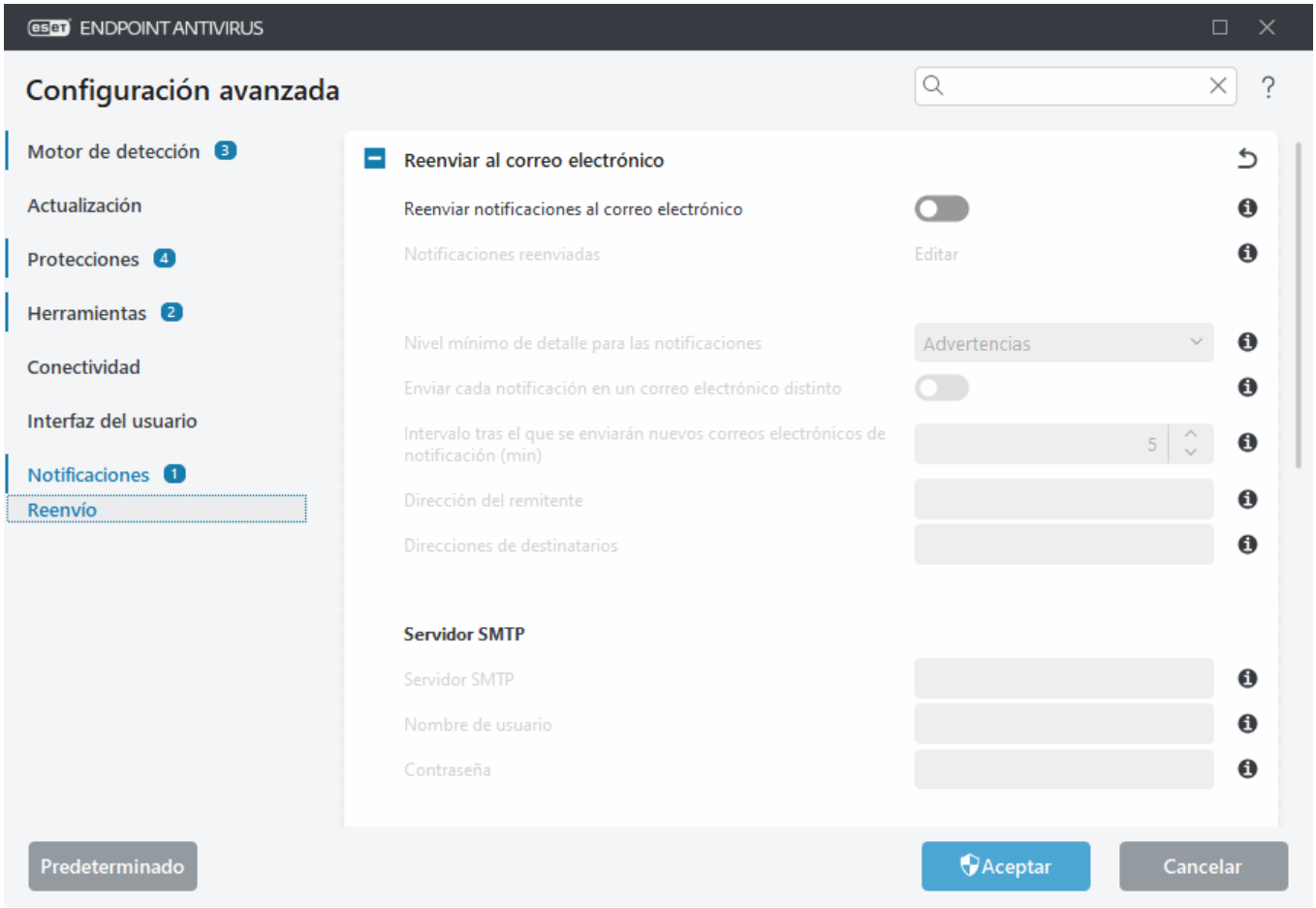
1. Abra **Configuración avanzada** (F5) > **Notificaciones** > **Alertas interactivas**.
2. Haga clic en **Modificar** junto a **Alertas interactivas**. En la sección **Ordenador**, desmarque las casillas de verificación situadas junto a **Reiniciar el ordenador (obligatorio)** y **Reiniciar el ordenador (recomendado)**.
3. Haga clic en **Aceptar** para guardar sus cambios en las dos ventanas abiertas.

4. Las alertas ya no aparecerán en la máquina del punto de conexión.
5. (opcional) Para desactivar el estado de la aplicación en la ventana del programa principal de ESET Endpoint Antivirus, en la ventana Estados de la aplicación, desmarque las casillas de verificación situadas junto a **Es necesario reiniciar el ordenador** y **Es recomendable reiniciar el ordenador**.

Reenvío

ESET Endpoint Antivirus puede enviar correos electrónicos de forma automática si se produce un suceso con el nivel de detalle seleccionado. En la sección Configuración avanzada > **Notificaciones** > **Reenvío** > **Reenviar al correo electrónico**, active **Reenviar notificaciones al correo electrónico** para permitir las notificaciones por correo electrónico.

Notificaciones reenviadas: seleccione qué notificaciones de escritorio se reenviarán al correo electrónico.



En el menú desplegable **Nivel mínimo de detalle para las notificaciones** puede seleccionar el nivel de gravedad inicial de las notificaciones que desea enviar.

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: registra los mensajes informativos, como los sucesos de red no convencionales, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Advertencias**: registra errores graves y mensajes de alerta (por ejemplo, un fallo de actualización).
- **Errores**: se registran los errores (protección de documentos no iniciada) y los errores graves.
- **Crítico**: registra solo errores críticos (por ejemplo, Error al activar la protección antivirus o Amenaza detectada).

Enviar cada notificación en un correo electrónico distinto: si esta opción está activada, el destinatario recibirá un correo electrónico nuevo para cada notificación. Esto podría suponer la recepción de varios correos electrónicos en un breve periodo de tiempo.

Intervalo tras el que se enviarán nuevos correos electrónicos de notificación (min): intervalo en minutos tras el cual se enviarán nuevas notificaciones al correo electrónico. Si define este valor en 0, las notificaciones se enviarán de forma inmediata.

Dirección del remitente: defina la dirección de correo del emisor que se mostrará en el encabezado de los mensajes de correo electrónico de notificación.

Direcciones de destinatarios: defina las direcciones de correo de los destinatarios que se muestran en el encabezado de los mensajes de correo electrónico de notificación. Es posible incluir varios valores. Utilice el punto y coma como separador.

Servidor SMTP

Servidor SMTP: el servidor SMTP que se utiliza para enviar notificaciones (por ejemplo, *smtp.provider.com:587*, el puerto predefinido es 25).

Los servidores SMTP con cifrado TLS son compatibles con ESET Endpoint Antivirus.

Nombre de usuario y contraseña: si el servidor SMTP requiere autenticación, estos campos deben cumplimentarse con un nombre de usuario y una contraseña válidos que faciliten el acceso al servidor SMTP.

Dirección del remitente: este campo especifica la dirección de correo del emisor, que se mostrará en el encabezado de los mensajes de notificación.

Direcciones de destinatarios: este campo especifica la dirección de correo de los destinatarios que se mostrarán en el encabezado de los mensajes de notificación. Utilice un punto y coma ";" para separar varias direcciones de correo electrónico.

Habilitar TLS: active el envío de mensajes de notificación y alerta que admite el cifrado TLS.

Formato de mensajes

Las comunicaciones entre el programa y un usuario o administrador de sistemas remotos se realizan a través de mensajes de correo electrónico o mensajes de red local (mediante el servicio de mensajería de Windows). El formato predeterminado de los mensajes de alerta y las notificaciones será el óptimo para la mayoría de situaciones. En algunas circunstancias, tendrá que cambiar el formato de los mensajes de sucesos.

Para notificar la ocurrencia de sucesos: formato de los mensajes de suceso que se muestran en los ordenadores remotos.

Formato de mensajes de alerta de amenazas: los mensajes de notificación y alerta de amenazas tienen un formato predefinido. Le aconsejamos que no modifique este formato. No obstante, en algunas circunstancias (por ejemplo, si tiene un sistema automatizado de procesamiento de correo electrónico), es posible que deba modificar el formato de los mensajes.

Conjunto de caracteres: convierte un mensaje de correo electrónico a la codificación de caracteres ANSI según la configuración regional de Windows (por ejemplo, windows-1250, Unicode (UTF-8), ACSII 7-bit o japonés

(ISO-2022-JP)). El resultado es que "á" se cambiará por "a" y un símbolo desconocido, por "?".

Usar codificación Quoted-printable: el origen del mensaje de correo electrónico se codificará a formato Quoted-printable (QP), que utiliza caracteres ASCII y solo pude transmitir correctamente caracteres nacionales especiales por correo electrónico en formato de 8 bits (áéíóú).

Las palabras clave (cadenas separadas por signos %) se sustituyen en el mensaje por la información real especificada. Están disponibles las siguientes palabras clave:

- **%TimeStamp%**: fecha y hora del suceso.
- **%Scanner%**: módulo correspondiente.
- **%ComputerName%**: nombre del ordenador en el que se produjo la alerta.
- **%ProgramName%**: programa que generó la alerta.
- **%InfectedObject%**: nombre del archivo, mensaje, etc., infectado.
- **%VirusName%**: identificación de la infección.
- **%Action%**: acción adoptada respecto a la amenaza.
- **%ErrorDescription%**: descripción de un suceso que no está relacionado con un virus.

Las palabras clave **%InfectedObject%** y **%VirusName%** solo se utilizan en los mensajes de alerta de amenaza y **%ErrorDescription%**, en los mensajes de sucesos.

Restaurar todos los valores de todas las configuraciones

Haga clic en **Predeterminado** en Configuración avanzada para restablecer todos los ajustes del programa para todos los módulos. Esto restablecerá los ajustes al estado que habrían tenido tras una nueva instalación.

Consulte también Importar y exportar configuración.

Restaurar todas las opciones de esta sección

Haga clic en la flecha curva para restaurar los ajustes predeterminados definidos por ESET de todas las opciones de esta sección.

Tenga en cuenta que, al hacer clic en **Restaurar predeterminados**, se perderán todos los cambios realizados.

Restaurar el contenido de las tablas: si está activada, se perderán las reglas, tareas o perfiles que se hayan añadido de forma manual o automática.

Consulte también Importar y exportar configuración.

Error al guardar la configuración

Este mensaje de error indica que la configuración no se guardó correctamente debido a un error.

Esto suele significar que el usuario que intentó modificar los parámetros del programa:

- no tiene suficientes derechos de acceso o no tiene los privilegios necesarios en el sistema operativo para

modificar archivos de configuración y el registro del sistema.
> Para realizar las modificaciones deseadas, el administrador del sistema debe iniciar sesión.

- ha activado recientemente Modo de aprendizaje en HIPS o Cortafuegos e intentado realizar cambios en Configuración avanzada.
  > Para guardar la configuración y evitar el conflicto de configuración, cierre Configuración avanzada sin guardar e intente realizar los cambios deseados de nuevo.

La segunda causa más común es que el programa ya no funcione correctamente, que esté dañado y, por lo tanto, se deba volver a instalar.

Análisis de línea de comandos

El módulo antivirus de ESET Endpoint Antivirus se puede iniciar manualmente a través de la línea de comandos, con el comando "ecls" o con un archivo por lotes ("bat").

Uso del análisis de línea de comandos de ESET:

```
ecls [OPTIONS..] FILES..
```

Los siguientes parámetros y modificadores se pueden utilizar al ejecutar el análisis a petición desde la línea de comandos:

Opciones

/base-dir=CARPETA	cargar módulos desde una CARPETA
/quar-dir=CARPETA	CARPETA de cuarentena
/exclude=MÁSCARA	excluir del análisis los archivos que cumplan MÁSCARA
/subdir	analizar subcarpetas (predeterminado)
/no-subdir	no analizar subcarpetas
/max-subdir-level=NIVEL	máximo nivel de anidamiento para subcarpetas a analizar
/symlink	seguir enlaces simbólicos (predeterminado)
/no-symlink	omitir enlaces simbólicos
/ads	analizar ADS (predeterminado)
/no-ads	no analizar ADS
/log-file=ARCHIVO	registrar salida en ARCHIVO
/log-rewrite	sobrescribir el archivo de salida (predeterminado – agregar)
/log-console	enviar registro a la consola (predeterminado)
/no-log-console	no enviar registro a la consola
/log-all	registrar también los archivos sin infectar
/no-log-all	no registrar archivos sin infectar (predeterminado)
/aind	mostrar indicador de actividad
/auto	analizar y desinfectar automáticamente todos los discos locales

Opciones de análisis

/files	analizar archivos (predeterminado)
/no-files	no analizar archivos
/memory	analizar memoria
/boots	analizar sectores de inicio
/no-boots	no analizar sectores de inicio (predeterminado)
/arch	analizar archivos comprimidos (predeterminado)
/no-arch	no analizar archivos
/max-obj-size=TAMAÑO	analizar solo archivos menores de TAMAÑO megabytes (predeterminado 0 = ilimitado)
/max-arch-level=NIVEL	máxima profundidad de anidamiento para archivos comprimidos (archivos anidados) a analizar
/scan-timeout=LÍMITE	analizar archivos comprimidos durante LÍMITE segundos como máximo
/max-arch-size=TAMAÑO	analizar los archivos dentro de un archivo comprimido solo si su tamaño es inferior a TAMAÑO (predeterminado 0 = ilimitado)
/max-sfx-size=TAMAÑO	analizar solo los archivos en un archivo comprimido de autoextracción si su tamaño es inferior a TAMAÑO megabytes (predeterminado 0 = ilimitado)
/mail	analizar archivos de correo (predeterminado)
/no-mail	no analizar archivos de correo
/mailbox	analizar buzones de correo (predeterminado)
/no-mailbox	no analizar buzones de correo
/sfx	analizar archivos comprimidos de autoextracción (predeterminado)
/no-sfx	no analizar archivos comprimidos de autoextracción
/rtp	analizar empaquetadores en tiempo real (predeterminado)
/no-rtp	no analizar empaquetadores en tiempo real
/unsafe	analizar en busca de aplicaciones potencialmente peligrosas
/no-unsafe	no analizar en busca de aplicaciones potencialmente peligrosas
/unwanted	analizar en busca de aplicaciones potencialmente indeseables
/no-unwanted	no analizar en busca de aplicaciones potencialmente indeseables (predeterminado)
/suspicious	analizar en busca de aplicaciones sospechosas (predeterminado)
/no-suspicious	no analizar en busca de aplicaciones sospechosas
/pattern	usar firmas (predeterminado)
/no-pattern	no usar firmas
/heur	activar heurística (predeterminado)
/no-heur	desactivar heurística
/adv-heur	activar heurística avanzada (predeterminado)
/no-adv-heur	desactivar heurística avanzada
/ext-exclude=EXTENSIONES	excluir EXTENSIONES de archivo del análisis, separándolas por el signo ":" (dos puntos)

/clean-mode=MODO	utilizar el MODO desinfección para objetos infectados Están disponibles las opciones siguientes: • `none` (predeterminado): no se realiza la desinfección automática. • `standard`: ecls.exe intenta desinfectar o eliminar automáticamente los archivos infectados. • `strict` (estricto): ecls.exe intenta desinfectar o eliminar automáticamente los archivos infectados sin la intervención del usuario (no verá una notificación antes de que se eliminen los archivos). • `rigorous` (riguroso): ecls.exe elimina los archivos sin intentar desinfectarlos, sea cual sea el archivo. • `delete` (eliminar): ecls.exe elimina los archivos sin intentar desinfectarlos, pero no elimina archivos delicados como los archivos del sistema de Windows.
/quarantine	copiar archivos infectados (si se han desinfectado) a la carpeta Cuarentena (complementa la acción realizada durante la desinfección)
/no-quarantine	no copiar archivos infectados a cuarentena

Opciones generales

/help	mostrar ayuda y salir
/version	mostrar información sobre la versión y salir
/preserve-time	conservar hora del último acceso

Códigos de salida

0	no se ha detectado ninguna amenaza
1	amenaza detectada y eliminada
10	no se han podido analizar todos los archivos (pueden ser amenazas)
50	amenaza detectada
100	error

Los códigos de salida superiores a 100 significan que no se ha analizado el archivo y que, por lo tanto, puede estar infectado.

Preguntas habituales

Este capítulo abarca algunas de las preguntas más frecuentes y los problemas encontrados. Haga clic en el título del tema para obtener información sobre cómo solucionar el problema:

- Cómo actualizar ESET Endpoint Antivirus
- Cómo activar ESET Endpoint Antivirus
- ESET Endpoint Antivirus ha detectado una amenaza
- Cómo eliminar un virus de mi PC
- Cómo crear una tarea nueva en Tareas programadas
- Cómo programar un análisis del ordenador semanal
- Cómo administrar notificaciones y alertas interactivas
- Cómo conectar mi producto a ESET PROTECT
  - Cómo utilizar el modo de anulación

- Procedimiento para aplicar una política recomendada para ESET Endpoint Antivirus
- Cómo configurar un Mirror
- Cómo actualizar a Windows 10 con ESET Endpoint Antivirus
- Cómo activar supervisión y administración remotas
- Cómo bloquear la descarga de tipos de archivo específicos de Internet
- Cómo minimizar la interfaz de usuario de ESET Endpoint Antivirus

Si no encuentra su problema en las páginas de ayuda anteriores, realice una búsqueda por palabra clave o por frase para describir el problema en las páginas de Ayuda de ESET Endpoint Antivirus.

Si no encuentra la solución a su problema o consulta en las páginas de Ayuda, consulte la base de conocimiento de ESET, donde encontrará respuesta a las preguntas y los problemas más habituales.

- ¿Cómo se desinstala ESET Endpoint Antivirus?
- Prácticas recomendadas para protegerse contra malware de tipo filecoder (ransomware)
- Preguntas frecuentes sobre ESET Endpoint Security y ESET Endpoint Antivirus
- ¿Qué direcciones y puertos del cortafuegos de terceros debo abrir para garantizar la compatibilidad con todas las funciones de mi producto de ESET?

Si es necesario, puede ponerse en contacto con nuestro centro de soporte técnico en línea para comunicarle sus consultas o problemas. El vínculo al formulario de contacto a través de Internet está disponible en el panel **Ayuda y soporte** de la ventana principal del programa.

Preguntas frecuentes sobre actualizaciones automáticas

Para ver información adicional sobre las actualizaciones del producto en ESET Endpoint Antivirus, lea el siguiente artículo de la base de conocimiento de ESET:
- ¿Cuáles son los diferentes tipos de versiones y actualizaciones de los productos de ESET?

¿Los ordenadores se actualizarán automáticamente? ¿La actualización se descarga antes o después del reinicio?

La descarga tiene lugar antes del reinicio y los archivos actualizados también se preparan en esta fase. Tras el reinicio, los archivos actualizados siguen preparados únicamente para su uso, y la versión instalada ofrece protección ininterrumpida. Los cambios se aplican tras el siguiente inicio del producto ESET Endpoint Antivirus.

Tengo aproximadamente 3.000 ordenadores. ¿Descargarán todos los ordenadores las actualizaciones al mismo tiempo? ¿Puedo utilizar un proxy para las actualizaciones automáticas con tantos ordenadores?

ESET ofrece la herramienta Mirror y soluciones proxy para redes de gran tamaño, de manera que las actualizaciones se descargan solo una vez de Internet y, a continuación, se distribuyen localmente. Las actualizaciones son más pequeñas, suelen tener entre 5 y 10 MB, y ESET las limitará durante las primeras semanas de disponibilidad. Por lo tanto, no todos los clientes iniciarán la descarga al mismo tiempo cuando se conecten directamente a los servidores de ESET.

¿Puedo decidir cuántos ordenadores o qué ordenadores se actualizarán automáticamente? No quiero descargar en más de diez ordenadores por hora, o solo quiero actualizar diez ordenadores por ahora, y otro ordenador después de un par de días.

Los entornos administrados tienen una política de actualización automática en la que puede especificar la versión más reciente que desee. También se admiten comodines (por ejemplo, 9.0.2032.*). Si desea más información, consulte el capítulo Actualizaciones automáticas en la ayuda en línea de ESET PROTECT o ESET PROTECT Cloud. Por desgracia, en este momento no hay otras opciones disponibles para limitar las actualizaciones automáticas. Puede asignar varias políticas a varios grupos.

¿Las actualizaciones automáticas solo se configuran mediante políticas? ¿Puedo desactivar la política si no quiero que se actualice un producto de ESET?

Si existe una revisión de seguridad y estabilidad para el producto ESET Endpoint, el producto se actualizará incluso cuando las actualizaciones automáticas estén desactivadas, de acuerdo con los términos establecidos en el EULA aplicable. ESET utiliza revisiones de seguridad y estabilidad para resolver problemas críticos y garantizar la máxima seguridad y estabilidad para su producto de ESET.

Puede asignar una política de actualización automática a cualquier grupo de equipos, sea cual sea su configuración de actualización automática. En entornos no administrados, el usuario puede configurar las actualizaciones automáticas de forma local en la pantalla Configuración avanzada de un producto de ESET del equipo.

¿Qué sucede si configuro una política para utilizar la versión más antigua disponible? Aun así, ¿ESET actualizará mis productos?

Las revisiones y las revisiones críticas (actualizaciones de seguridad y estabilidad) son categorías de actualización ligeramente diferentes. Las revisiones normales se asignan a las actualizaciones automáticas con una prioridad estándar cuando se aceptan los ajustes del usuario. A las revisiones críticas se les aplica prioridad máxima, independientemente de los ajustes del usuario.

¿Cómo funcionarán las actualizaciones en situaciones sin conexión? ¿Cuándo utilizan los usuarios el repositorio sin conexión?

El repositorio sin conexión también contiene archivos .dup y .fup. La sección del repositorio debe descargarse con la herramienta Mirror, no con la actualización de los módulos. Para obtener más información, consulte el tema Repositorio sin conexión en la ayuda en línea de ESET PROTECT.

¿Cómo saben los productos de ESET que es necesaria la actualización? ¿Por el repositorio? ¿Se envía algún dato a los servidores? Si ESET tiene

previsto realizar una actualización un mes después del lanzamiento de una versión, ¿pueden los servidores de ESET gestionar un lanzamiento internacional?

Los productos de ESET descargan actualizaciones automáticas del repositorio. Los servidores están preparados para eso, ya que las actualizaciones críticas tienen solo unos cuantos kilobytes. ESET no limitará las actualizaciones críticas en los servidores del repositorio. Sin embargo, existe la opción de limitar las actualizaciones de los servidores si las actualizaciones automáticas son grandes. En la siguiente tabla se ofrecen ejemplos de los tamaños de revisiones en el caso de una actualización automática diferencial:

Versión anterior	Nueva versión	Tamaño
9.0.2032.2	9.0.2032.6	420 KB
8.1.2037.2	9.0.2032.2	6.5 MB
8.0.2028.0	9.0.2032.2	11.5 MB

Si una actualización automática diferencial falla, el producto de ESET puede iniciar una actualización completa. Sigue siendo una actualización automática con una garantía de funcionalidad, pero, en lugar de un archivo .dup, se descargará un .fup, que es un archivo mayor. Para la versión 9.0.2032.2 tiene 27 MB. Sin embargo, un caso de este tipo es raro.

¿Se lanzará la actualización de ESET Endpoint Antivirus con regulación? En ese caso, ¿durante cuánto tiempo se limitará la actualización tras el lanzamiento?

ESET limita las actualizaciones durante las primeras semanas tras el lanzamiento de una nueva versión con el fin de reducir la carga en nuestros servidores y distribuir la nueva versión de forma uniforme.

Las actualizaciones automáticas serán uno de los principales métodos de actualización. ¿Cómo funcionan exactamente?

El objetivo de ESET es que el mayor número posible de clientes utilice las actualizaciones automáticas. Es difícil mantener muchas versiones anteriores. La función de actualizaciones automáticas es sencilla. Hay archivos .dup que se descargan durante la primera comprobación de la actualización de los módulos. Durante el procedimiento de actualización, el producto es totalmente funcional y protege el ordenador. La nueva versión se activa tras el reinicio. En ESET PROTECT (en el servidor), puede utilizar una política para especificar la versión más alta a la que desea actualizarse o utilizar comodines. Si desea más información, consulte el capítulo Actualizaciones automáticas en la ayuda en línea de ESET PROTECT o ESET PROTECT Cloud.

¿Es cierto que las actualizaciones automáticas funcionan en 1/10? Ya utilizo ESET Endpoint Security 8.0.2028.1. ¿A qué versión se actualizará si se ejecutan las actualizaciones automáticas?

La actualización de productos con actualizaciones automáticas puede retrasarse debido a la limitación de los servidores del repositorio. Si una actualización de componentes de los programas se publica con limitación, es posible que las comprobaciones de actualizaciones automáticas no la reciban inmediatamente. Si la actualización

se considera segura y estable, la limitación puede reducirse o eliminarse por completo para que todos los clientes restantes reciban la actualización.

El procedimiento de limitación puede durar un tiempo diferente en cada actualización. Varía en función del número de clientes que soliciten la actualización, del tráfico de nuestros servidores y otros factores. Este procedimiento está en constante evolución, y se producen cambios continuamente.

¿Cuándo comenzarán las actualizaciones si inicio un ordenador a las 8:45 a. m. y lo apago a las 5:00 p. m.?

Las actualizaciones automáticas se iniciarán con la siguiente actualización de los módulos programada correctamente, como máximo una vez cada 24 horas.

¿Cuándo se ejecutará la actualización de nuevo si el ordenador se apaga mientras se ejecutan las actualizaciones automáticas?

La actualización se ejecutará en la siguiente ventana de actualización programada. El procedimiento de actualización automática (antes uPCU) cuenta con un sólido mecanismo a prueba de fallos. Tras descargar la actualización y reiniciar el ordenador, los archivos actualizados siguen preparados para su uso, y la versión instalada ofrece protección ininterrumpida. Los cambios se aplican tras el siguiente inicio del producto ESET Endpoint.

¿Cómo puedo ejecutar las actualizaciones automáticas inmediatamente sin esperar a una conexión regular cada 24 horas? ¿Existe alguna otra forma de poder hacer clic en Buscar actualizaciones?

Puede iniciar el procedimiento de actualización automática de forma manual cuando abre la ventana principal del programa y hace clic en **Actualizar** > **Buscar actualizaciones**. Todas las demás formas de iniciar las actualizaciones de los módulos reflejan la política de las tareas programadas de actualización automática de 24 horas. No se puede iniciar de forma remota una descarga de actualizaciones automáticas en este momento. Agregaremos esta función más adelante.

Cómo actualizar ESET Endpoint Antivirus

ESET Endpoint Antivirus Se puede actualizar de forma manual o automática. Para activar la actualización, haga clic en **Actualización** en la ventana principal del programa y, a continuación, haga clic en **Buscar actualizaciones**.

La configuración de instalación predeterminada crea una tarea de actualización automática que se lleva a cabo cada hora. Para cambiar el intervalo, vaya a **Herramientas** > Tareas programadas.

Cómo eliminar un virus de mi PC

Si su ordenador muestra señales de una infección por código malicioso, por ejemplo, es más lento o se bloquea a menudo, se recomienda que haga lo siguiente:

1. En la ventana principal del programa, haga clic en **Análisis del ordenador**.

2. Haga clic en **Análisis estándar** para iniciar la exploración del sistema.
3. Una vez finalizado el análisis, revise el registro con el número de archivos analizados, infectados y desinfectados.
4. Si solo desea analizar determinadas partes del disco, haga clic en **Análisis personalizado** y especifique los objetos que desee analizar en busca de virus.

Si desea información adicional, visite nuestro artículo de la base de conocimientos de ESET, que se actualiza periódicamente.

Cómo crear una tarea nueva en el Planificador de tareas

Para crear una tarea nueva en **Herramientas** > **Planificador de tareas**, haga clic en **Agregar tarea** o haga clic con el botón derecho y seleccione **Agregar** en el menú contextual. Están disponibles cinco tipos de tareas programadas:

- **Ejecutar aplicación externa**: programa la ejecución de una aplicación externa.
- **Mantenimiento de registros**: los archivos de registro también contienen restos de los registros eliminados. Esta tarea optimiza periódicamente los registros incluidos en los archivos para aumentar su eficacia.
- **Verificación de archivos en el inicio del sistema**: comprueba los archivos que se pueden ejecutar al encender o iniciar el sistema.
- **Crear un informe del estado del sistema**: crea una instantánea del ordenador de ESET SysInspector recopila información detallada sobre los componentes del sistema (por ejemplo controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.
- **Análisis del ordenador a petición**: analiza los archivos y las carpetas del ordenador.
- **Actualización**: programa una tarea de actualización mediante la actualización de los módulos.

La **actualización** es una de las tareas programadas más frecuentes, por lo que a continuación explicaremos cómo se agrega una nueva tarea de actualización:

En el menú desplegable **Tarea programada**, seleccione **Actualización**. Introduzca el nombre de la tarea en el campo **Nombre de la tarea** y haga clic en **Siguiente**. Seleccione la frecuencia de la tarea. Están disponibles las opciones siguientes: **Una vez**, **Reiteradamente**, **Diariamente**, **Semanalmente** y **Cuando se cumpla la condición.** **Seleccione No ejecutar la tarea si está funcionando con batería** para minimizar los recursos del sistema mientras un ordenador portátil esté funcionando con batería. La tarea se ejecutará en la fecha y hora especificadas en el campo **Ejecución de la tarea**. A continuación, defina la acción que debe llevarse a cabo si la tarea no se puede realizar o completar a la hora programada. Están disponibles las opciones siguientes:

- **En la siguiente hora programada**
- **Lo antes posible**
- **Inmediatamente, si la hora desde la última ejecución excede un valor especificado** (el intervalo se puede definir con el cuadro **Tiempo desde la última ejecución**)

En el paso siguiente, se muestra una ventana de resumen que contiene información acerca de la tarea programada actualmente. Haga clic en **Finalizar** cuando haya terminado de hacer cambios.

Aparecerá un cuadro de diálogo que permite al usuario elegir los perfiles que desea utilizar para la tarea programada. Aquí puede definir los perfiles principal y alternativo. El perfil alternativo se utiliza cuando la tarea no se puede completar con el perfil principal. Haga clic en **Finalizar** para confirmar la operación; la nueva tarea se agregará a la lista de tareas programadas actualmente.

Cómo programar un análisis del ordenador semanal

Para programar una tarea periódica, abra la ventana principal del programa > **Herramientas** > **Tareas programadas**. A continuación, se proporcionan las instrucciones básicas para programar una tarea que analice las unidades locales cada semana. Consulte el artículo de nuestra Base de conocimiento para ver instrucciones más detalladas.

Para programar una tarea:

1. Haga clic en **Agregar tarea** en la pantalla principal del Planificador.
2. Seleccione **Análisis de estado inactivo** en el menú desplegable.
3. Escriba un nombre para la tarea y seleccione **Semanalmente para la frecuencia de la tarea**.
4. Establezca el día y la hora de ejecución de la tarea.
5. Seleccione **Ejecutar la tarea lo antes posible** para realizar la tarea más tarde si no se ejecuta a la hora programada por cualquier motivo (por ejemplo, si el ordenador estaba apagado).
6. Revise el resumen de la tarea programada y haga clic en **Finalizar**.
7. En el menú desplegable **Objetos**, seleccione **Discos locales**.
8. Haga clic en **Finalizar** para aplicar la tarea.

Cómo conectar ESET Endpoint Antivirus a ESET PROTECT

Cuando haya instalado ESET Endpoint Antivirus en su ordenador y desee conectarse a través de ESET PROTECT, asegúrese de haber instalado también el agente ESET Management en su estación de trabajo de cliente. Es una parte esencial de todas las soluciones de cliente que se comunican con ESET PROTECT Server.

- Instalar o implementar ESET Management Agent en estaciones de trabajo cliente

Consulte también:

- Documentación para equipos administrados de forma remota
- Cómo utilizar el modo de anulación
- Cómo aplicar una política recomendada para ESET Endpoint Antivirus

Cómo utilizar el modo de anulación

Los usuarios con productos ESET Endpoint (versión 6.5 y superiores) para Windows instalados en sus máquinas podrán utilizar la función de anulación. El modo de anulación permite a los usuarios de nivel de ordenador cliente cambiar la configuración del producto ESET instalado, incluso si hay una política aplicada a dicha configuración. El modo de anulación puede activarse para determinados usuarios de AD o protegerse mediante contraseña. La función no puede activarse durante más de cuatro horas directamente.

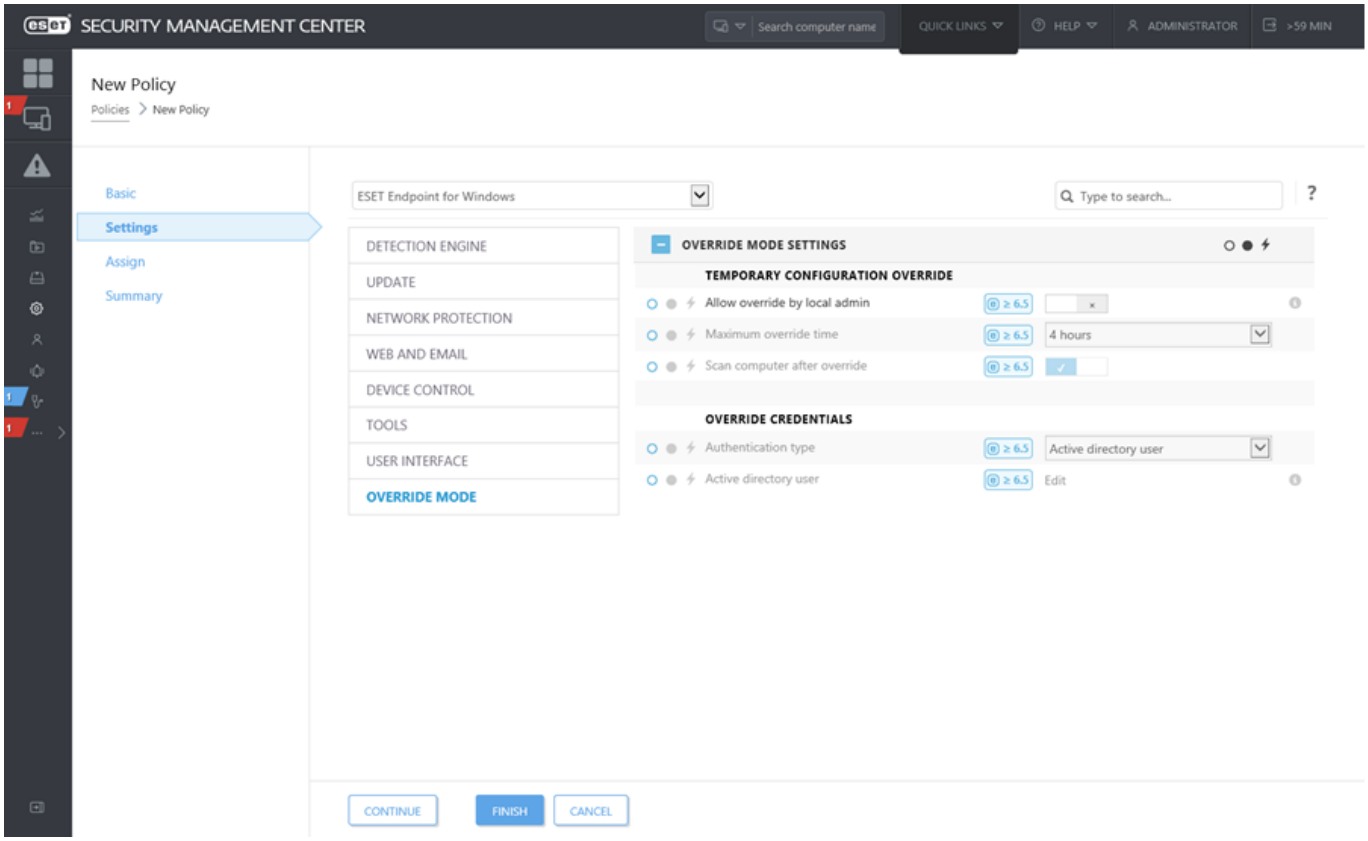
No puede detener el modo de anulación desde ESET PROTECT Web Console cuando se activa. El modo de anulación se deshabilitará automáticamente cuando venza el periodo de anulación. También puede desactivarse en el equipo cliente.

El usuario que utiliza el modo de anulación también necesita tener derechos de administrador de Windows. De lo contrario, el usuario no podrá guardar los cambios realizados en la configuración de ESET Endpoint Antivirus.

La autenticación de grupo de Active Directory es compatible.

Para configurar el **Modo de anulación**:

1. Vaya a **Políticas** > **Nueva política**.
2. En la sección **Básico**, escriba un **Nombre** y una **Descripción** para esta política.
3. En la sección **Configuración**, seleccione **ESET Endpoint para Windows**.
4. Haga clic en **Modo de anulación** y configure reglas para el modo de anulación.
5. En la sección **Asignar**, seleccione el ordenador o el grupo de ordenadores a los que se aplicará esta política.
6. Revise la configuración en la sección **Resumen** y haga clic en **Finalizar** para aplicar la política.



Si *John* tiene un problema porque la configuración de Endpoint está bloqueando algunas funciones importantes o el acceso web en su máquina, el Administrador podrá permitir que *John* anule su política de Endpoint existente y ajuste la configuración manualmente en su máquina. Después, ESET PROTECT podrá solicitar la nueva configuración, por lo que el Administrador podrá crear una nueva política a raíz de la misma.
Para hacerlo, siga estos pasos:
1. Vaya a **Políticas** > **Nueva política**.
2. Complete los campos **Nombre** y **Descripción**. En la sección **Configuración**, seleccione **ESET Endpoint para Windows**.
3. Haga clic en **Modo de anulación**, active el modo de anulación durante una hora y seleccione *John* como usuario de AD.
4. Asigne la política al *Ordenador de John* y haga clic en **Finalizar** para guardar la política.
5. *John* deberá activar el **Modo de anulación** en su ESET Endpoint y cambiar la configuración manualmente en su máquina.
6. En ESET PROTECT Web Console, vaya a **Ordenadores**, seleccione *Ordenador de John* y haga clic en **Mostrar detalles**.
7. En la sección **Configuración**, haga clic en **Solicitar configuración** para programar una tarea de cliente para obtener la configuración del cliente lo antes posible.
8. Poco después aparecerá la nueva configuración. Haga clic en el producto cuya configuración desea guardar y, a continuación, haga clic en **Abrir configuración**.
9. Puede revisar la configuración y, a continuación, hacer clic en **Convertir en política**.
10. Complete los campos **Nombre** y **Descripción**.
11. En la sección **Configuración**, puede modificar la configuración en caso necesario.
12. En la sección **Asignar**, puede asignar esta política al *Ordenador de John* (o a otros).
13. Haga clic en **Finalizar** para guardar la configuración.
14. No olvide eliminar la política de anulación cuando ya no la necesite.

Cómo aplicar una política recomendada para ESET Endpoint Antivirus

La práctica recomendada tras conectar ESET Endpoint Antivirus a ESET PROTECT es aplicar una política recomendada o aplicar una personalizada.

Hay varias políticas integradas para ESET Endpoint Antivirus:

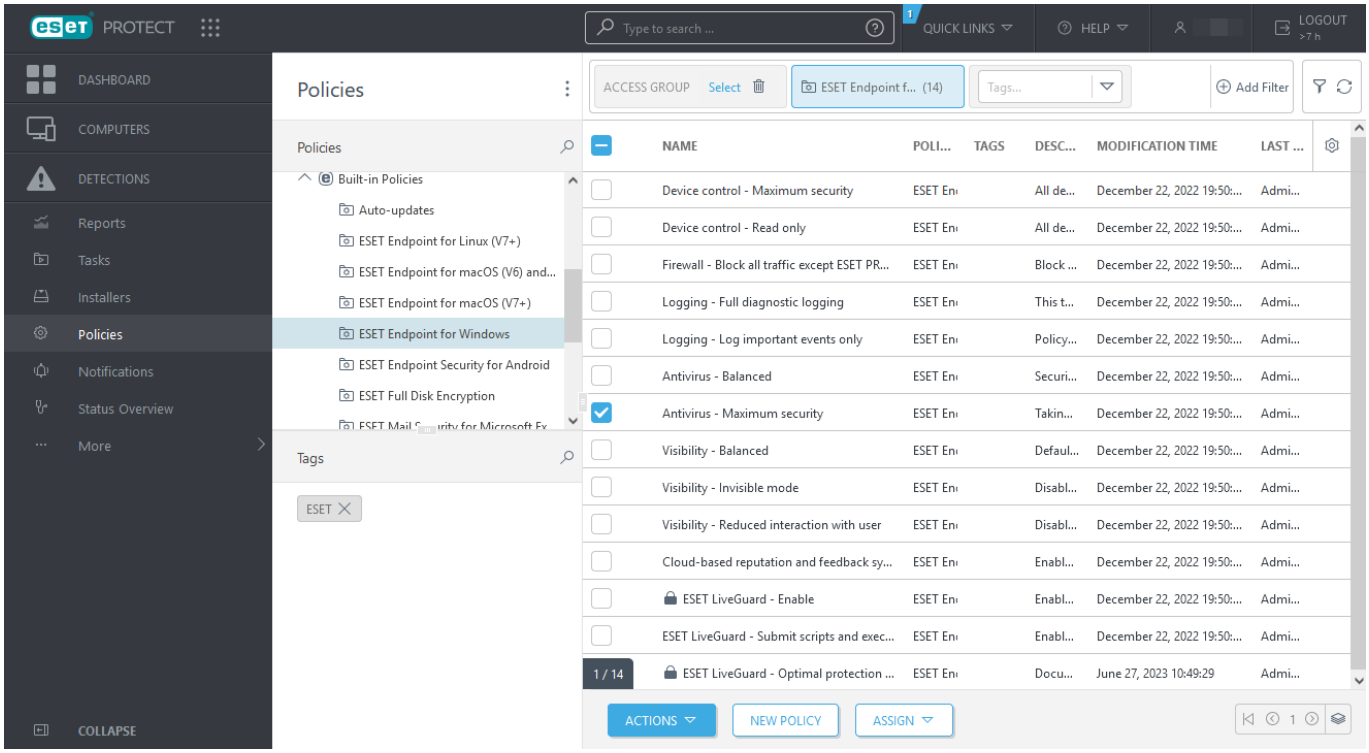
Política	Descripción
Antivirus: equilibrada	Configuración de seguridad recomendada para la mayoría de las configuraciones.
Antivirus: seguridad máxima	Uso de aprendizaje automático, análisis profundo de inspección de comportamiento y filtrado de SSL. La detección de aplicaciones potencialmente peligrosas, no deseadas y sospechosas se ve afectada.
Sistema de reputación y respuesta basado en la nube	Activa el sistema de reputación y respuesta en la nube ESET LiveGrid® para mejorar la detección de las amenazas más recientes y compartir potenciales amenazas maliciosas o desconocidas para un análisis más detallado.
Control de dispositivos: seguridad máxima	Se bloquean todos los dispositivos. Cuando se desee conectar un dispositivo, el administrador deberá permitirlo.
Control de dispositivos: solo lectura	Todos los dispositivos son de solo lectura. No se permite escritura.

Política	Descripción
Cortafuegos: bloquear todo el tráfico, excepto la conexión de ESET PROTECT y ESET Inspect	Bloquear todo el tráfico, salvo la conexión a ESET PROTECT y ESET Inspect Server (solo ESET Endpoint Security).
Registro: registro de diagnóstico completo	Esta plantilla garantizará que el administrador tendrá todos los registros disponibles cuando los necesite. Todo se registrará desde un nivel de detalle mínimo, incluidos ThreatSense e HIPS y el cortafuegos. Los registros se eliminan automáticamente transcurridos 90 días.
Registro: registrar solo los eventos importantes	Esta política garantiza que se registrarán las alertas, los errores y los sucesos graves. Los registros se eliminan automáticamente transcurridos 90 días.
Visibilidad: equilibrada	Configuración predeterminada de visibilidad. Los estados y las notificaciones están habilitados.
Visibilidad: modo invisible	Se desactivan las notificaciones, las alertas, la interfaz gráfica de usuario y la integración en el menú contextual. No se ejecutará el archivo egui.exe. Idóneo para administración exclusiva desde ESET PROTECT Cloud.
Visibilidad: interacción con el usuario reducida	Se desactivan los estados, las notificaciones, se muestra la interfaz gráfica de usuario.

Para establecer la política llamada **Antivirus: seguridad máxima**, que aplica más de 50 ajustes recomendados para ESET Endpoint Antivirus cuando está instalado en sus estaciones de trabajo, siga estos pasos:

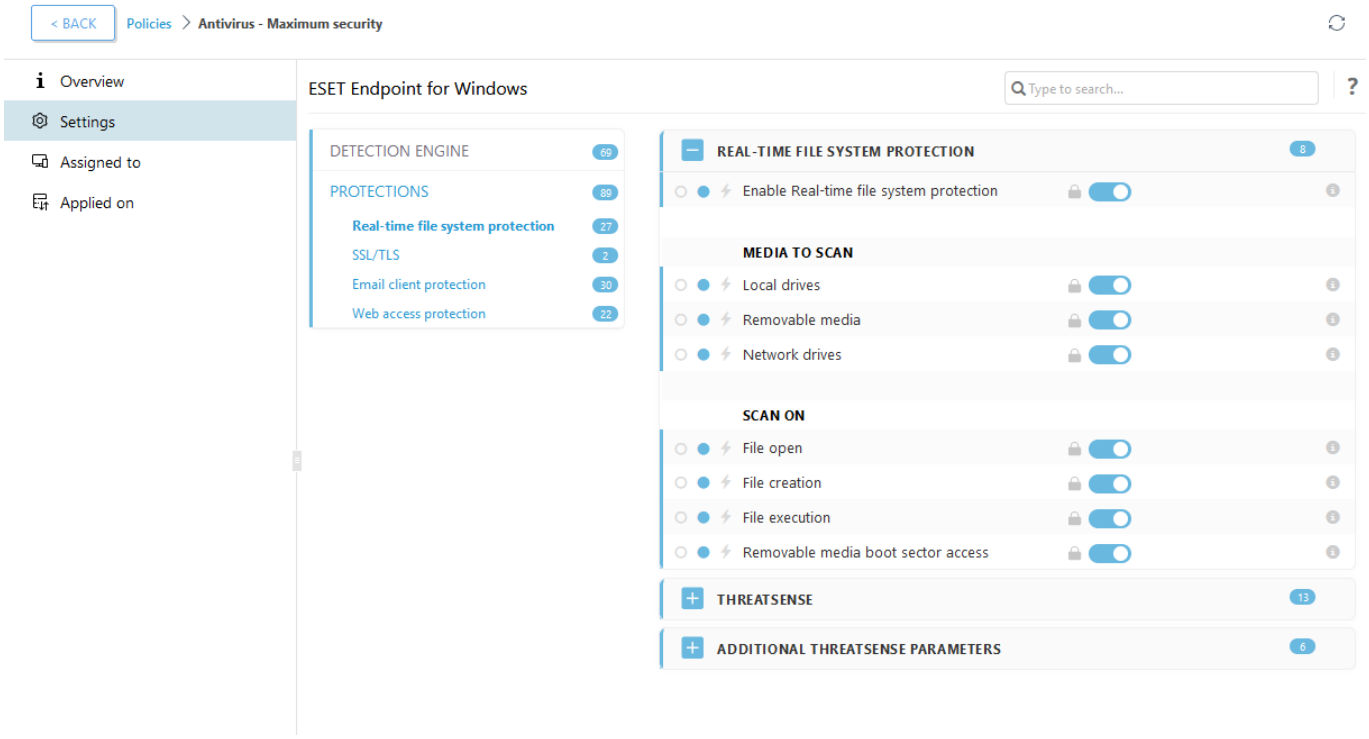
> Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:
> Apply a recommended or predefined policy for ESET Endpoint Antivirus using ESET PROTECT

1. Abra ESET PROTECT Web Console.
2. Vaya a **Políticas** y despliegue **Políticas incorporadas** > **ESET Endpoint para Windows**.
3. Haga clic en **Antivirus: seguridad máxima, opción recomendada**.
4. En la ficha **Asignado a**, haga clic en **Asignar clientes** o **Asignar grupos** y seleccione los ordenadores a los que desea aplicar esta política.



Para ver la configuración que se aplica a esta política, haga clic en la ficha **Configuración** y despliegue el árbol de Configuración avanzada.

- El punto azul representa un ajuste modificado de esta política
- El número del marco azul representa un número de ajustes modificados por esta política
- Obtenga más información acerca de las políticas de ESET PROTECT



Cómo configurar un Mirror

ESET Endpoint Antivirus se puede configurar para que almacene copias de los archivos de actualización del motor de detección y distribuya las actualizaciones a otras estaciones de trabajo en las que se ejecute ESET Endpoint Antivirus o ESET Endpoint Security.

El mirror de actualización crea copias de los archivos de actualización que se pueden usar para actualizar estaciones de trabajo que ejecutan la misma generación de ESET Endpoint Antivirus para Windows (por ejemplo, ESET Endpoint Antivirus para Windows versión 10.x crea archivos de actualización solo para la versión 10.x ESET Endpoint Antivirus para Windows y ESET Endpoint Security para Windows).

Configuración de ESET Endpoint Antivirus como servidor Mirror para proporcionar actualizaciones mediante un servidor HTTP interno

1. Pulse **F5** para acceder a Configuración avanzada y expanda **Actualización** > **Perfiles** > **Mirror de actualización**.
2. Expanda **Actualizaciones** y asegúrese de que la opción **Elegir automáticamente** de **Actualizaciones del módulo** esté activada.
3. Expanda **Mirror de actualización** y active **Crear mirror de actualización** y **Activar servidor HTTP**.

Para obtener más información, consulte:
- Mirror de actualización
- Actualización desde el servidor Mirror

Configuración de un servidor Mirror para proporcionar actualizaciones a través de una carpeta de red compartida

1. Cree una carpeta compartida en un dispositivo local o de red. Todos los usuarios que utilicen soluciones de seguridad de ESET deben tener acceso de lectura a esta carpeta, que, además, debe permitir la escritura desde la cuenta de SISTEMA local.
2. Active **Crear mirror de actualización** en **Configuración avanzada** > **Actualización** > **Perfiles** > **Mirror de actualización**.
3. Para elegir una **Carpeta de almacenamiento** apropiada, haga clic en **Borrar** y, a continuación, en **Editar**. Busque y seleccione la carpeta compartida creada.

Si no desea proporcionar actualizaciones de los módulos mediante el servidor HTTP interno, desactive **Activar servidor HTTP**.

Cómo actualizar a Windows 10 con ESET Endpoint Antivirus

Se recomienda encarecidamente actualizar a la versión más reciente de su producto de ESET y a continuación descargar las actualizaciones de módulos más recientes antes de actualizar a Windows 10. De esta forma se asegurará de disponer de la máxima protección y de conservar la configuración del programa y la información de licencia durante la actualización a Windows 10.

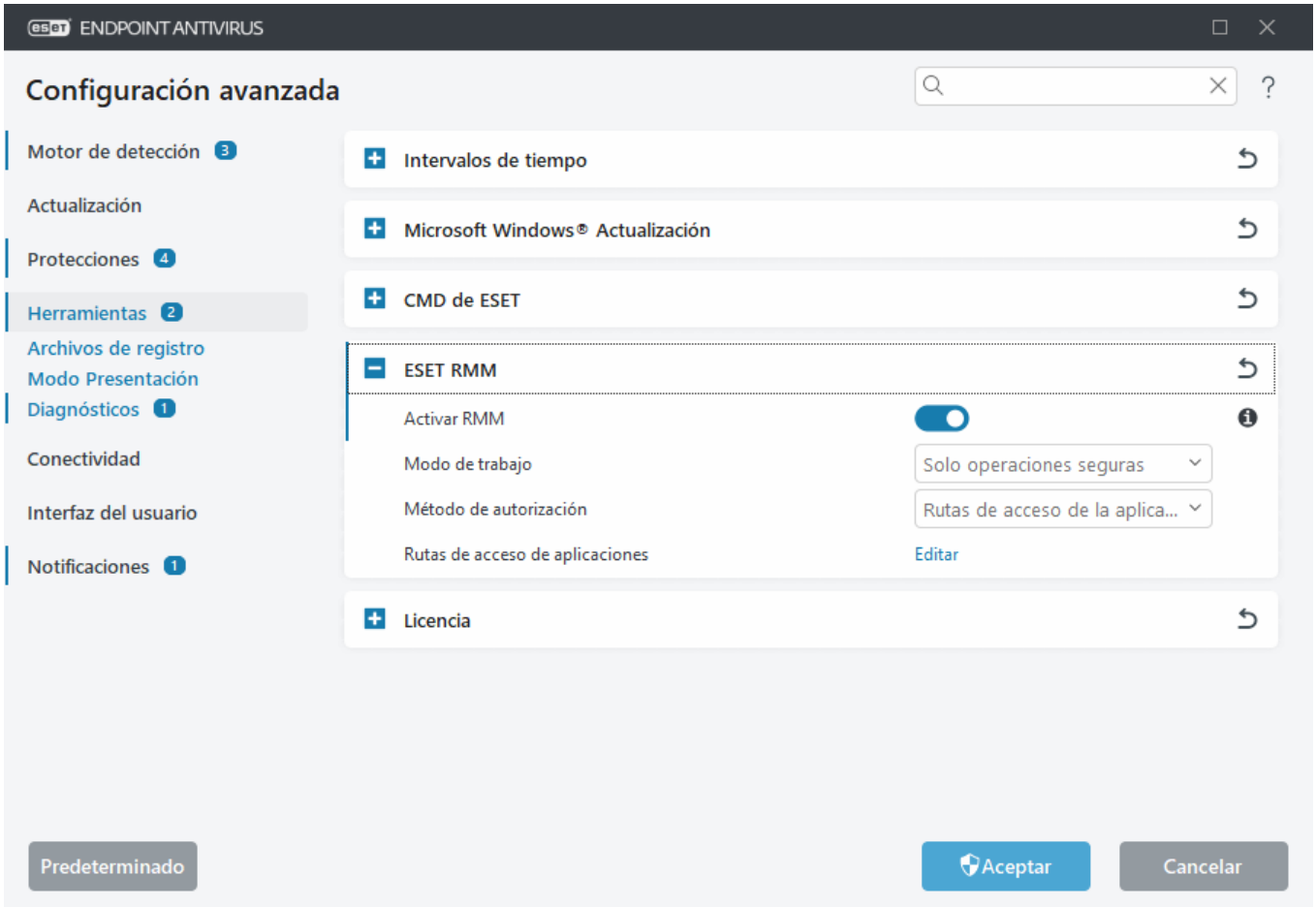
Versiones en otros idiomas:

Si está buscando una versión en otro idioma de su producto ESET Endpoint, visite nuestra página de descargas.

Más información sobre la compatibilidad de los productos empresariales de ESET con Windows 10.

Cómo activar supervisión y administración remotas

La supervisión y administración remotas (RMM) es el proceso de supervisar y controlar sistemas de software (como los de escritorios, servidores y dispositivos móviles) con un agente instalado localmente al que se puede acceder mediante un proveedor de servicios de administración. ESET Endpoint Antivirus se puede administrar mediante RMM a partir de la versión 6.6.2028.0.



De forma predeterminada, ESET RMM está desactivado. Para activar ESET RMM, abra Configuración avanzada > **Herramientas avanzadas** > **ESET RMM** y active el interruptor situado junto a **Activar RMM**.

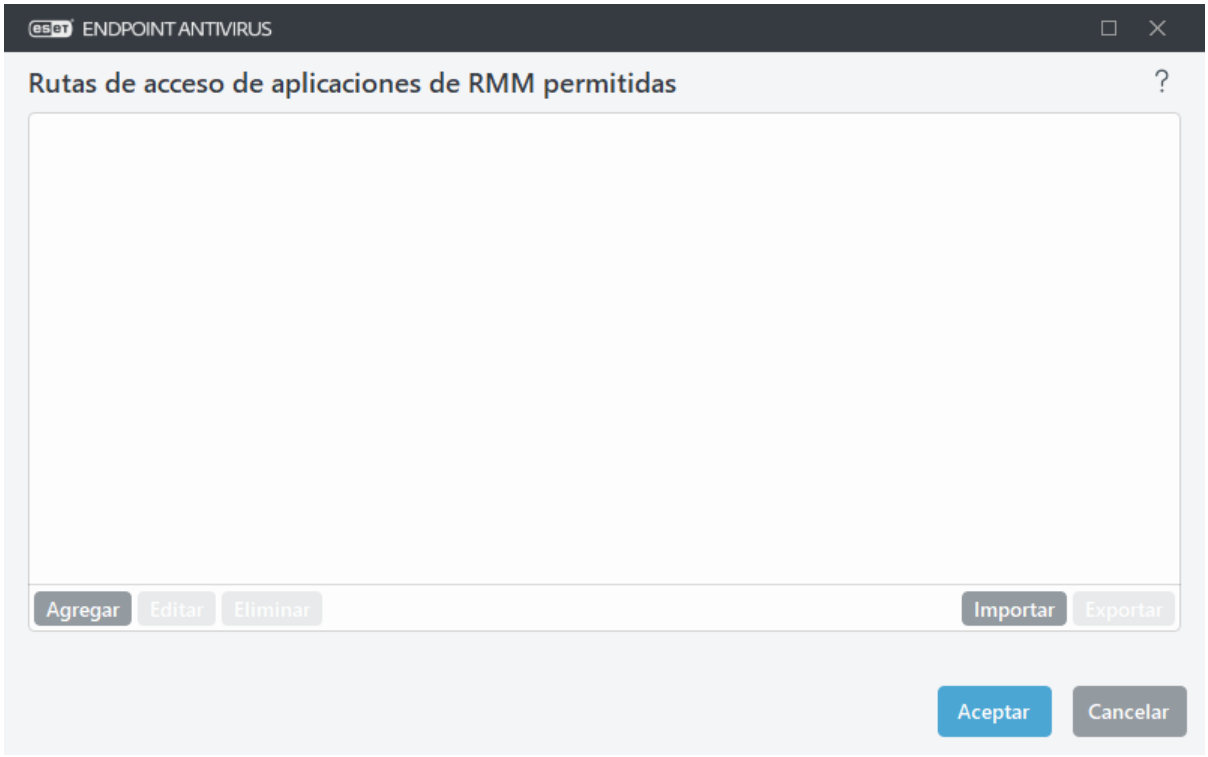
Modo de trabajo: seleccione **Solo operaciones seguras** si quiere activar la interfaz RMM para operaciones seguras y de solo lectura. Seleccione **Todas las operaciones** si desea activar la interfaz RMM para todas las operaciones.

Condición	Modo de solo operaciones seguras	Modo de todas las operaciones
Obtener información-aplicación	✔	✔
Obtener configuración	✔	✔
Obtener información sobre la licencia	✔	✔
Obtener registros	✔	✔
Obtener el estado de la protección	✔	✔
Obtener el estado de actualización	✔	✔
Definir configuración		✔
Iniciar activación		✔
Iniciar análisis	✔	✔
Iniciar actualización	✔	✔

Método de autorización: defina el método de autorización de RMM. Para utilizar la autorización, seleccione **Ruta de acceso de la aplicación** en el menú desplegable; de lo contrario, seleccione **Ninguno**.

RMM siempre debe utilizar la autorización para evitar que el software malintencionado desactive o se salte la protección de ESET Endpoint.

Rutas de acceso de la aplicación: aplicación concreta autorizada para ejecutar RMM. Si ha seleccionado **Ruta de acceso de la aplicación** como método de autorización, haga clic en **Modificar** para abrir la ventana de configuración de **Rutas de acceso de aplicaciones de RMM permitidas**.



Agregar: cree una nueva ruta de acceso de aplicaciones de RMM permitidas. Escriba la ruta o haga clic en el botón **…** para seleccionar un ejecutable.

Modificar: modifique una ruta de acceso permitida existente. Utilice **Modificar** si la ubicación del ejecutable ha cambiado a otra carpeta.

Eliminar: elimine una ruta de acceso permitida existente.

La instalación de ESET Endpoint Antivirus predeterminada contiene el archivo ermm.exe ubicado en el directorio de la aplicación Endpoint (ruta predeterminada C*:\Program Files\ESET\ESET Security*). El archivo ermm.exe intercambia datos con RMM Plugin, que se comunica con RMM Agent, vinculado a un RMM Server.

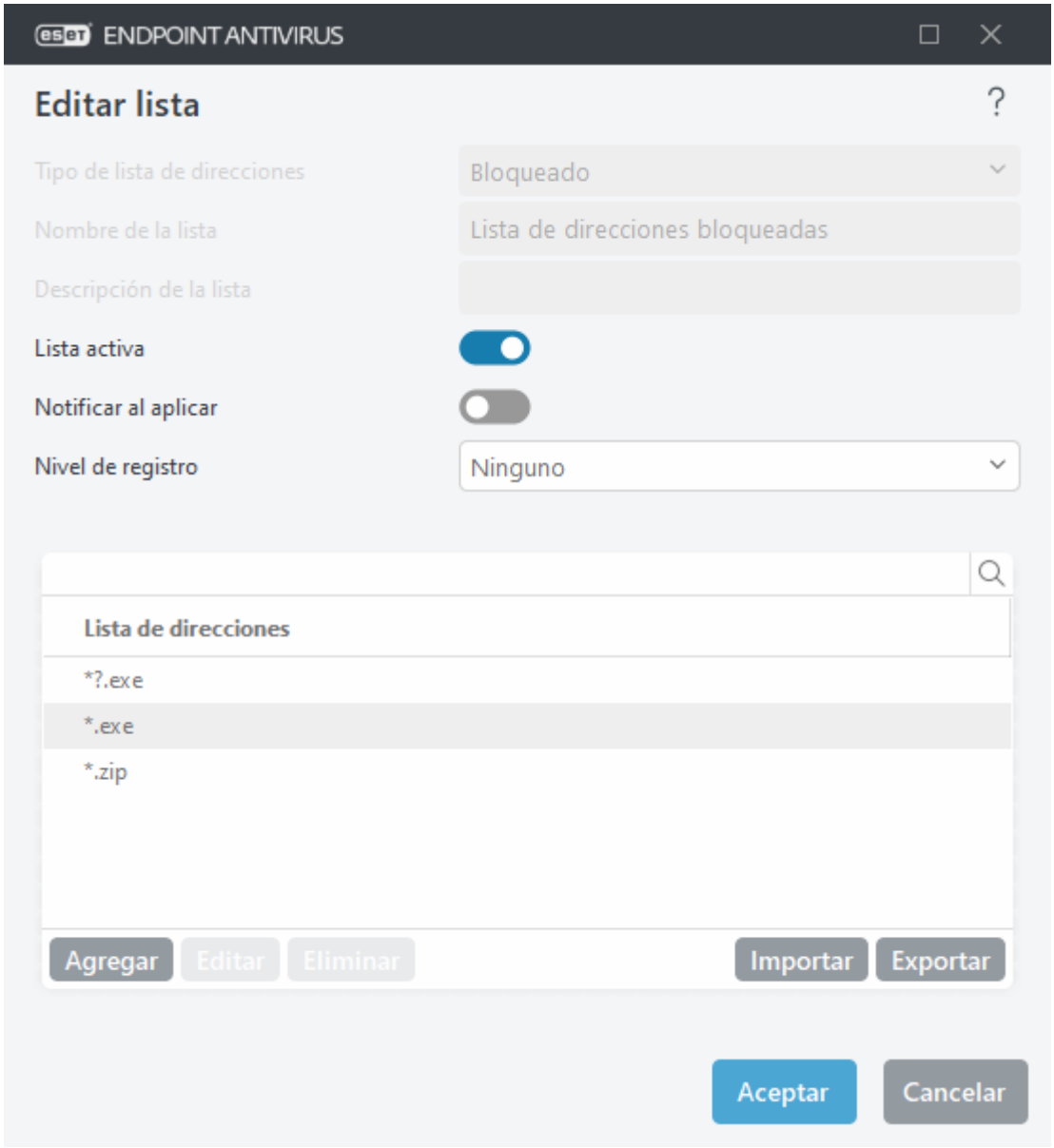
- ermm.exe: utilidad de línea de comandos desarrollada por ESET que permite administrar productos Endpoint y comunicarse con cualquier RMM Plugin.
- RMM Plugin es una aplicación de terceros que se ejecuta localmente en el sistema Endpoint para Windows. El complemento se ha diseñado para comunicarse con un RMM Agent concreto (p. ej., solo Kaseya) y con ermm.exe.
- RMM Agent es una aplicación de terceros (p. ej., de Kaseya) que se ejecuta localmente en el sistema Endpoint para Windows. El agente se comunica con RMM Plugin y con RMM Server.

Cómo bloquear la descarga de tipos de archivo específicos de Internet

Si no quiere permitir que se descarguen de Internet determinados tipos de archivo (como exe, pdf o zip), utilice la Administración de direcciones URL con una combinación de comodines. Pulse la tecla F5 para acceder a **Configuración avanzada**. Haga clic en **Web y correo electrónico** > **Protección de acceso a la web** y despliegue **Administración de direcciones URL**. Haga clic en **Modificar** junto a **Lista de direcciones**.

En la ventana **Lista de direcciones**, seleccione **Lista de direcciones bloqueadas** y haga clic en **Editar**, o haga clic en **Agregar** para crear o modificar una lista. Se abrirá una ventana nueva. Si está creando una lista nueva, seleccione **Bloqueada** en el menú desplegable **Tipo de lista de direcciones** e introduzca un nombre para la lista. Si desea recibir notificaciones cuando se acceda a un tipo de archivo de la lista actual, active la barra deslizante **Notificar al aplicar**. Seleccione la **Gravedad de registro** en el menú desplegable. ESET PROTECT es capaz de recopilar registros con el nivel de detalle **Advertencia**.

Los niveles de registro Información y Advertencia solo están disponibles para las reglas que contienen al menos dos componentes sin comodines dentro del dominio. Por ejemplo:
- *.domain.com/*
- *www.domain.com/*



Haga clic en **Agregar** para introducir una máscara que especifique los tipos de archivos cuya descarga desea bloquear. Introduzca una URL completa si desea bloquear las descargas de un archivo específico de un sitio web específico como, por ejemplo, *http://example.com/file.exe*. Puede utilizar comodines para abarcar un grupo de archivos. El signo de interrogación (?) representa un carácter único variable, y el asterisco (*) una cadena variable de cero o más caracteres. Por ejemplo, la máscara **/*.zip* bloquea la descarga de todos los archivos zip comprimidos.

Tenga en cuenta que solo puede bloquear la descarga de tipos de archivo específicos con este método cuando la extensión del archivo es parte de la URL del archivo. Si la página web usa URL de descarga de archivos, por ejemplo, *www.example.com/download.php?fileid=42*, se descargarán todos los archivos ubicados en este enlace aun si tienen una extensión que haya bloqueado.

Cómo minimizar la interfaz de usuario de ESET Endpoint Antivirus

En la administración remota, puede aplicar una política predefinida de "Visibilidad".

Si no, siga los pasos manualmente:

1. Pulse **F5** para acceder a Configuración avanzada y despliegue **Interfaz de usuario** > **Elementos de la interfaz de usuario**.
2. Configure **Modo de inicio** en el valor deseado. Más información acerca de los modos de inicio.
3. Desactive **Mostrar la pantalla de bienvenida al iniciar el programa** y **Usar señal acústica**.
4. Configure Notificaciones.
5. Configure Estados de la aplicación.
6. Configure Mensajes de confirmación.
7. Configure Cuadros de alertas y mensajes.

Acuerdo de licencia para el usuario final

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

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

Acuerdo de licencia para el usuario final

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

ESTO NO ES UN CONTRATO DE VENTA, SINO UN ACUERDO SOBRE LOS DERECHOS DEL USUARIO FINAL. El proveedor sigue siendo el propietario de la copia del software y del soporte físico incluidos en el paquete de venta, así como de todas las copias que el usuario final pueda realizar en virtud de este acuerdo.

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

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

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

del artículo 3 de este Acuerdo. El Software se proporciona únicamente en forma de código objeto ejecutable.

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

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

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

b) **Estipulación del número de licencias.** El derecho de uso del software está sujeto a un número de usuarios finales. La expresión "un usuario final" se utilizará cuando se haga referencia a lo siguiente: (i) la instalación del software en un sistema informático o (ii) un usuario informático que acepta correo electrónico a través de un Agente de usuario de correo (“un AUC”) cuando el alcance de una licencia esté vinculado al número de buzones de correo. Si el AUC acepta correo electrónico y, posteriormente, lo distribuye de forma automática a varios usuarios, el número de usuarios finales se determinará según el número real de usuarios para los que se distribuyó el correo electrónico. Si un servidor de correo realiza la función de una pasarela de correo, el número de usuarios finales será equivalente al número de usuarios de servidor de correo a los que dicha pasarela preste servicios. Si se envía un número indefinido de direcciones de correo electrónico a un usuario, que las acepta (por ejemplo, mediante alias), y el cliente no distribuye los mensajes automáticamente a más usuarios, se necesita una licencia para un ordenador. No utilice la misma licencia en varios ordenadores de forma simultánea. El Usuario final tiene derecho a introducir la Clave de licencia en el Software si tiene derecho a utilizar el Software de acuerdo con la limitación derivada del número de licencias otorgadas por el Proveedor. La Clave de licencia se considera confidencial: no debe compartir la Licencia con terceros ni permitir que terceros utilicen la Clave de licencia, a menos que lo permitan este Acuerdo o el Proveedor. Si su Clave de licencia se ve expuesta, notifíqueselo inmediatamente al Proveedor.

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

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

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

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

g) **Terminación de la licencia.** La licencia se terminará automáticamente cuando concluya su período de vigencia.

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

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

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

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

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

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

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

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

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

A los efectos de este Acuerdo, es necesario recopilar, procesar y almacenar datos que permitan al Proveedor identificarle, de acuerdo con la Política de Privacidad. Acepta que el Proveedor puede comprobar por sus propios

medios si está utilizando el Software de conformidad con las disposiciones de este Acuerdo. Acepta que, a los efectos de este Acuerdo, es necesaria la transferencia de sus datos, durante la comunicación entre el Software y los sistemas informáticos del Proveedor o sus socios comerciales, como parte de la red de distribución y asistencia técnica del Proveedor, para garantizar la funcionalidad del Software y la autorización para utilizar el Software y proteger los derechos del Proveedor.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

13. **LIMITACIÓN DE RESPONSABILIDAD**. HASTA EL ALCANCE MÁXIMO PERMITIDO POR LA LEGISLACIÓN APLICABLE, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O SUS PROVEEDORES DE LICENCIAS SERÁN RESPONSABLES DE PÉRDIDAS DE BENEFICIOS, DE INGRESOS, DE VENTAS O DE DATOS NI DE COSTES DERIVADOS DE LA OBTENCIÓN DE PRODUCTOS O SERVICIOS DE SUSTITUCIÓN, DE DAÑOS A LA PROPIEDAD, DE DAÑOS PERSONALES, DE LA INTERRUPCIÓN DEL NEGOCIO, DE LA PÉRDIDA DE INFORMACIÓN COMERCIAL O DE DAÑOS ESPECIALES, DIRECTOS, INDIRECTOS, ACCIDENTALES, ECONÓMICOS, DE COBERTURA, CRIMINALES O SUCESIVOS,

CAUSADOS DE CUALQUIER MODO, YA SEA A CAUSA DE UN CONTRATO, UNA CONDUCTA INADECUADA INTENCIONADA, UNA NEGLIGENCIA U OTRO HECHO QUE ESTABLEZCA RESPONSABILIDAD, DERIVADOS DE LA INSTALACIÓN, EL USO O LA INCAPACIDAD DE USO DEL SOFTWARE, INCLUSO EN EL CASO DE QUE AL PROVEEDOR O A SUS PROVEEDORES DE LICENCIAS O FILIALES SE LES HAYA NOTIFICADO LA POSIBILIDAD DE DICHOS DAÑOS. DADO QUE DETERMINADOS PAÍSES Y JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE RESPONSABILIDAD, PERO PUEDEN PERMITIR LA LIMITACIÓN DE RESPONSABILIDAD, EN DICHOS CASOS, LA RESPONSABILIDAD DEL PROVEEDOR, SUS EMPLEADOS, LICENCIATARIOS O AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR LA LICENCIA.

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

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

16. **Transferencia de la licencia**. El software se puede transferir de un sistema informático a otro, a no ser que se indique lo contrario en los términos del acuerdo. Si no se infringen los términos del acuerdo, el usuario solo puede transferir la licencia y todos los derechos derivados de este acuerdo a otro usuario final de forma permanente con el consentimiento del proveedor, y con sujeción a las siguientes condiciones: (i) el usuario final original no conserva ninguna copia del software; (ii) la transferencia de derechos es directa, es decir, del usuario final original al nuevo usuario final; (iii) el nuevo usuario final asume todos los derechos y obligaciones correspondientes al usuario final original en virtud de los términos de este acuerdo; (iv) el usuario final original proporciona al nuevo usuario final la documentación necesaria para verificar la autenticidad del software, tal como se especifica en el artículo 17.

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

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

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

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

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

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

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

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

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

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

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

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

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

22. **Disposiciones generales**. El hecho de que alguna de las disposiciones de este acuerdo no sea válida o aplicable no afectará a la validez de las demás disposiciones del acuerdo, que seguirán siendo válidas y aplicables de conformidad con las condiciones aquí estipuladas. Este Acuerdo se ha formalizado en inglés. Si se realiza una

traducción del Acuerdo por motivos de comodidad o por cualquier otro motivo, o en caso de discrepancia entre las versiones de este Acuerdo en diferentes idiomas, prevalecerá la versión en inglés.

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

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

EULAID: EULA-PRODUCT-LG; 3537.0

Política de privacidad

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

- Procesamiento de datos personales
- Confidencialidad de los datos
- Derechos del titular de los datos

Procesamiento de datos personales

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

- Estadísticas sobre actualizaciones y de otro tipo con información relativa al proceso de instalación y a su ordenador, lo que incluye la plataforma en la que está instalado nuestro producto e información sobre las operaciones y la funcionalidad de nuestros productos, como el sistema operativo, información sobre el hardware, identificadores de instalación, identificadores de licencias, dirección IP, dirección MAC o ajustes de configuración del producto.
- Algoritmos hash unidireccionales relativos a infiltraciones que forman parte del sistema de reputación ESET LiveGrid®, lo que mejora la eficiencia de nuestras soluciones contra malware mediante la comparación de los archivos analizados con una base de datos de elementos incluidos en listas blancas y negras disponibles en la

nube.

- Muestras sospechosas y metadatos que forman parte del sistema de respuesta ESET LiveGrid®, lo que permite a ESET reaccionar inmediatamente ante las necesidades de los usuarios finales y responder a las amenazas más recientes. Dependemos de que Usted nos envíe
  - infiltraciones como posibles muestras de virus y otros programas malintencionados y sospechosos; objetos problemáticos, potencialmente no deseados o potencialmente peligrosos, como archivos ejecutables, mensajes de correo electrónico marcados por Usted como spam o marcados por nuestro producto;
  - información sobre dispositivos de la red local, como el tipo, el proveedor, el modelo o el nombre del dispositivo;
  - información relativa al uso de Internet, como dirección IP e información geográfica, paquetes de IP, URL y marcos de Ethernet;
  - archivos de volcado de memoria y la información contenida en ellos.

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

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

Confidencialidad de los datos

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

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

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

Derechos del titular de los datos.

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

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

Toda la información que tratamos es valiosa y necesaria para los fines de nuestro interés legítimo, que es la prestación de servicios y productos a nuestros clientes.

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

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