

ESET Endpoint Antivirus

Manual de usuario

[Haga clic aquí para ver la versión de la Ayuda en línea de este documento](#)

Copyright ©2021 de ESET, spol. s r.o.

ESET Endpoint Antivirus ha sido desarrollado por ESET, spol. s r.o.

Para obtener más información, visite el sitio www.eset.com.

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

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

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

REV. 20/01/2021

1 ESET Endpoint Antivirus 7	1
1.1 Novedades de la versión 7	2
1.2 Requisitos del sistema	3
1.2.1 Idiomas compatibles	3
1.3 Prevención	4
1.4 Páginas de Ayuda	5
2 Documentación para equipos administrados de forma remota	6
2.1 Introducción a ESET Security Management Center	7
2.2 Introducción a ESET PROTECT Cloud	8
2.3 Configuración protegida con contraseña	8
2.4 ¿Qué son las políticas?	9
2.4.1 Fusión de políticas	9
2.5 ¿Cómo funcionan los indicadores?	10
3 Uso de ESET Endpoint Antivirus exclusivamente	11
3.1 Método de instalación	11
3.1.1 Instalación con ESET AV Remover	12
3.1.1.1 ESET AV Remover	12
3.1.1.2 Desinstalación mediante ESET AV Remover finalizada con error	15
3.1.2 Instalación (.exe)	15
3.1.2.1 Cómo cambiar la carpeta de instalación (.exe)	17
3.1.3 Instalación (.msi)	18
3.1.3.1 Instalación avanzada (.msi)	20
3.1.4 Instalación desde la línea de comandos	21
3.1.5 Implementación con GPO o SCCM	25
3.1.6 Actualización a una versión más reciente	26
3.1.7 Problemas de instalación comunes	26
3.1.7.1 Error de activación	27
3.2 Activación del producto	27
3.3 Análisis del ordenador	27
3.4 Guía para principiantes	28
3.4.1 Interfaz de usuario	28
3.4.2 Configuración de actualizaciones	31
4 Uso de ESET Endpoint Antivirus	33
4.1 Ordenador	35
4.1.1 Motor de detección (7.2 y posteriores)	37
4.1.1.1 Opciones avanzadas del motor de detección	41
4.1.2 Motor de detección (7.1 y anteriores)	41
4.1.3 Detección de una amenaza	42
4.1.4 Caché local compartida	44
4.1.5 Protección del sistema de archivos en tiempo real	44
4.1.5.1 Análisis de protección en tiempo real	46
4.1.5.2 Modificación de la configuración de protección en tiempo real	46
4.1.5.3 Qué debo hacer si la protección en tiempo real no funciona	46
4.1.6 Análisis del ordenador	47
4.1.6.1 Iniciador del análisis personalizado	49
4.1.6.2 Progreso del análisis	50
4.1.6.3 Registro de análisis del ordenador	51
4.1.6.4 Análisis de malware	52
4.1.6.4.1 Análisis en estado inactivo	52
4.1.6.4.2 Perfiles de análisis	52
4.1.6.4.3 Objetos de análisis	53
4.1.6.4.4 Opciones avanzadas de análisis	53
4.1.7 Control del dispositivo	54
4.1.7.1 Editor de reglas de control de dispositivos	54
4.1.7.1.1 Dispositivos detectados	55

4.1.7.2 Grupos de dispositivos	55
4.1.7.3 Adición de reglas de control de dispositivos	56
4.1.8 Sistema de prevención de intrusiones del host (HIPS)	58
4.1.8.1 ventana interactiva de HIPS	61
4.1.8.1.1 Se ha detectado un comportamiento potencial de ransomware	62
4.1.8.2 Gestión de reglas de HIPS	62
4.1.8.2.1 Configuración de regla de HIPS	63
4.1.8.3 Configuración avanzada de HIPS	66
4.1.8.3.1 Controladores con carga siempre autorizada	66
4.1.9 Modo Presentación	67
4.1.10 Análisis en el inicio	67
4.1.10.1 Comprobación de la ejecución de archivos en el inicio	67
4.1.11 Protección de documentos	68
4.1.12 Exclusiones	68
4.1.12.1 Exclusiones de rendimiento	69
4.1.12.1.1 Agregar o modificar la exclusión de rendimiento	70
4.1.12.1.2 Formato de exclusión de ruta de acceso	71
4.1.12.2 Exclusiones de detección	72
4.1.12.2.1 Agregar o editar una exclusión de detección	74
4.1.12.2.2 Asistente de creación de exclusión de detección	75
4.1.12.3 Exclusiones (7.1 y anteriores)	76
4.1.12.4 Exclusiones de procesos	76
4.1.12.4.1 Agregar o modificar exclusiones de procesos	77
4.1.12.5 Exclusiones del HIPS	77
4.1.13 Parámetros de ThreatSense	77
4.1.13.1 Niveles de desinfección	80
4.1.13.2 Extensiones de archivo excluidas del análisis	82
4.1.13.3 Parámetros adicionales de ThreatSense	82
4.2 Red	83
4.2.1 Protección contra los ataques de red	84
4.2.1.1 Opciones avanzadas de filtrado	84
4.2.1.2 Excepciones de IDS	86
4.2.1.3 Sospecha de amenaza bloqueada	87
4.2.1.4 Resolución de problemas de protección de red	88
4.2.2 Lista negra de direcciones IP temporales	88
4.2.3 Solución de problemas con el cortafuegos de ESET	89
4.2.3.1 Asistente de solución de problemas	89
4.2.3.2 Registro y creación de reglas o excepciones del registro	89
4.2.3.2.1 Crear una regla desde un registro	89
4.2.3.3 Creación de excepciones a partir de notificaciones del cortafuegos	90
4.2.3.4 Registro PCAP avanzado	90
4.2.3.5 Solución de problemas con el filtrado de protocolos	90
4.3 Web y correo electrónico	91
4.3.1 Filtrado de protocolos	92
4.3.1.1 Aplicaciones excluidas	93
4.3.1.2 Direcciones IP excluidas	93
4.3.1.3 SSL/TLS	94
4.3.1.3.1 Certificados	95
4.3.1.3.1 Tráfico de red cifrado	96
4.3.1.3.2 Lista de certificados conocidos	96
4.3.1.3.3 Lista de aplicaciones con filtrado SSL/TLS	97
4.3.2 Protección del cliente de correo electrónico	97
4.3.2.1 Protocolos de correo electrónico	99
4.3.2.2 Alertas y notificaciones por correo electrónico	100
4.3.2.3 Integración con clientes de correo electrónico	101
4.3.2.3.1 Barra de herramientas de Microsoft Outlook	101
4.3.2.3.2 Barra de herramientas de Outlook Express y Windows Mail	101
4.3.2.3.3 Cuadro de diálogo de confirmación	101

4.3.2.3.4 Analizar de nuevo los mensajes	102
4.3.3 Protección del tráfico de Internet	102
4.3.3.1 Configuración avanzada de la protección de acceso a la web	104
4.3.3.2 Protocolos web	104
4.3.3.3 Gestión de direcciones URL	105
4.3.3.3.1 Lista de direcciones URL	106
4.3.3.3.2 Creación de nueva lista de direcciones URL	107
4.3.3.3.3 Cómo agregar una máscara URL	108
4.3.4 Protección Anti-Phishing	108
4.4 Actualización del programa	109
4.4.1 Configuración de actualizaciones	113
4.4.1.1 Reversión de actualización	116
4.4.1.2 Actualización de componentes del programa	117
4.4.1.3 Opciones de conexión	118
4.4.1.4 Mirror de actualización	119
4.4.1.4.1 Servidor HTTP	121
4.4.1.4.2 Actualización desde el servidor Mirror	122
4.4.1.4.3 Resolución de problemas de actualización del Mirror	124
4.4.2 Cómo crear tareas de actualización	125
4.5 Herramientas	125
4.5.1 Archivos de registro	126
4.5.1.1 Filtrado de registros	128
4.5.1.2 Registro de configuración	129
4.5.1.3 Registros de auditoría	130
4.5.2 Planificador de tareas	131
4.5.3 Estadísticas de protección	134
4.5.4 Observar actividad	134
4.5.5 ESET SysInspector	135
4.5.6 Protección en la nube	136
4.5.6.1 Filtro de exclusión para protección en la nube	139
4.5.7 Procesos en ejecución	139
4.5.8 Informe de seguridad	141
4.5.9 ESET SysRescue Live	143
4.5.10 Envío de muestras para el análisis	143
4.5.10.1 Seleccionar muestra para el análisis: archivo sospechoso	144
4.5.10.2 Seleccionar muestra para el análisis: sitio sospechoso	144
4.5.10.3 Seleccionar muestra para el análisis: archivo de falso positivo	144
4.5.10.4 Seleccionar muestra para el análisis: sitio de falso positivo	145
4.5.10.5 Seleccionar muestra para el análisis: otros	145
4.5.11 Notificaciones	145
4.5.11.1 Notificaciones de aplicaciones	146
4.5.11.2 Notificaciones en el escritorio	147
4.5.11.3 Notificaciones por correo electrónico	147
4.5.11.4 Personalización de las notificaciones	149
4.5.12 Cuarentena	150
4.5.13 Configuración del servidor Proxy	151
4.5.14 Intervalos de tiempo	152
4.5.15 Microsoft Windows Update	153
4.5.16 Intervalo de comprobación de la licencia	153
4.6 Interfaz de usuario	153
4.6.1 Elementos de la interfaz del usuario	154
4.6.1.1 Estados de la aplicación	155
4.6.2 Configuración de acceso	156
4.6.2.1 Contraseña de Configuración avanzada	157
4.6.3 Cuadros de alertas y mensajes	158
4.6.3.1 Alertas interactivas	160
4.6.3.2 Mensajes de confirmación	161
4.6.3.3 Error de conflicto de configuración avanzada	161

4.6.3.4 Es necesario reiniciar	162
4.6.3.5 Se recomienda reiniciar	163
4.6.3.6 Unidades extraíbles	164
4.6.4 Icono en la bandeja del sistema	165
4.6.5 Menú contextual	166
4.6.6 Ayuda y asistencia técnica	166
4.6.6.1 Acerca de ESET Endpoint Antivirus	167
4.6.6.2 Enviar datos de configuración del sistema	168
4.6.7 Administrador de perfiles	168
4.6.8 Accesos directos del teclado	169
4.6.9 Diagnóstico	169
4.6.10 Análisis de línea de comandos	171
4.6.11 CMD de ESET	173
4.6.12 Detección de estado inactivo	175
4.6.12.1 Importar y exportar configuración	175
4.6.12.2 Restaurar todos los valores de todas las configuraciones	176
4.6.12.3 Restaurar todas las opciones de esta sección	176
4.6.12.4 Error al guardar la configuración	176
4.6.13 Supervisión y administración remotas	177

ESET Endpoint Antivirus 7

ESET Endpoint Antivirus 7 representa un nuevo enfoque de la seguridad informática realmente integrada. La versión más reciente del motor de análisis ThreatSense® 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 7 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 7 está diseñado principalmente para utilizarlo en estaciones de trabajo dentro de un entorno de pequeña empresa.

En la sección [Uso de ESET Endpoint Antivirus exclusivamente](#), 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 Security Management Center](#) 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.
Antivirus y antiespía	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 Security Management Center le permite administrar los productos de ESET en estaciones de trabajo, servidores y dispositivos móviles en un entorno de red desde una ubicación central. Con ESET Security Management Center Consola Web (ESMC 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 los ataques de 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)	El 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 de la versión 7

ESET Endpoint Antivirus 7 se ha publicado y está [disponible para descargar](#).

Novedades de ESET Endpoint Antivirus 7.0

- Nuevo diseño de la interfaz de usuario gráfica.
- Arrastrar y colocar para analizar archivos: puede analizar un archivo o una carpeta de forma manual, con solo mover el archivo o la carpeta hasta la zona marcada.
- La [protección contra los ataques de red](#) está ahora disponible en ESET Endpoint Antivirus. Si desea más información, consulte [Protección contra los ataques de red](#).
- En el estado de protección, la política de ESET Security Management Center puede desactivar el enlace de acción rápida.
- Ahora puede aplicar reglas de control de dispositivos durante un periodo de tiempo específico. Si desea obtener más información, consulte la sección de [Intervalos de tiempo](#).

Novedades de ESET Endpoint Antivirus 7.1

- Nuevo tipo de registro: ahora está disponible un tipo de registro avanzado. Si desea más información, consulte [Registros de auditoría](#).

Novedades de ESET Endpoint Antivirus 7.2

- El aprendizaje automático avanzado es una capa avanzada de protección que mejora la detección gracias al aprendizaje automático. Lea más sobre este tipo de protección en el [glosario](#). La [configuración del motor de detección](#) ya no incluye interruptores de activación/desactivación, como en la versión 7.1 y anteriores. Los botones de activación/desactivación han sido sustituidos por cuatro umbrales: "Agresivo", "Equilibrado", "Precavido" y "Desactivado".
- Localización en letón agregada.
- Cambios de las [exclusiones](#). Las exclusiones de rendimiento le permiten excluir archivos y carpetas del análisis. Las exclusiones de detección le permiten excluir objetos de la desinfección usando el nombre de detección, la ruta de acceso o su hash.
- El nuevo módulo del programa HIPS incluye Análisis profundo del comportamiento, que analiza el comportamiento de todos los programas que se ejecutan en el ordenador y le advierte si el comportamiento del proceso es malicioso. [Más información sobre HIPS en nuestras páginas de ayuda](#).
- Las [alertas interactivas configurables](#) le permiten ajustar el comportamiento de las alertas interactivas configurables (por ejemplo, ocultar la alerta "Se recomienda reiniciar" en las máquinas del punto de conexión).

Novedades de ESET Endpoint Antivirus 7.3

- Esta versión secundaria incluye varias correcciones de errores y mejoras del rendimiento.

Para ver información adicional y capturas de pantalla de las nuevas características de ESET Endpoint Antivirus, lea

el siguiente artículo de la base de conocimiento de ESET:

- [Novedades de ESET Endpoint Antivirus 7](#)

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 de 32 bits (x86) con conjunto de instrucciones SSE2 o procesador de 64 bits (x64), 1 GHz o superior

Sistemas operativos

Microsoft® Windows® 10

Microsoft® Windows® 8.1

Microsoft® Windows® 8

Microsoft® Windows® 7 SP1 con las más recientes actualizaciones de Windows (como mínimo, [KB4474419](#) y [KB4490628](#))

Windows XP y Windows Vista ya [no son compatibles con la versión 7](#).

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 × 768
- Conexión a Internet o conexión de red de área local a una fuente (consulte la nota 3) de actualizaciones del producto

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



Nota

- (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 necesario para descargar el instalador, instalar el producto y conservar una copia del paquete de instalación en los datos del programa, así como 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, el producto se puede actualizar manualmente desde un soporte 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
Noruego	nn-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
*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 el extremo superior derecho).

Prevención

Cuando trabaje con el ordenador y, especialmente, cuando navegue por Internet, tenga en cuenta que ningún sistema antivirus del mundo puede eliminar completamente el riesgo de que se produzcan [amenazas detectadas](#) y [ataques remotos](#). Para disfrutar de una protección y una comodidad máximas, es esencial usar correctamente su 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 del laboratorio de virus de ESET analizan estas amenazas diariamente y preparan y

publican actualizaciones para mejorar continuamente el nivel de protección para los usuarios. Para garantizar la máxima eficacia de estas actualizaciones es importante que estén 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 varias 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 Internet Explorer son dos ejemplos de programas que publican de forma periódica actualizaciones de seguridad.

Copia de seguridad de los datos importantes

Normalmente, a los autores de código malicioso no les importan las necesidades de los usuarios y, con frecuencia, la actividad de los programas malintencionados provoca un funcionamiento incorrecto del sistema operativo y la pérdida de datos importantes. Es importante realizar copias de seguridad periódicas de sus datos importantes y confidenciales 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 precavido 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.

[Páginas de Ayuda](#)

Bienvenido a las páginas de ayuda de ESET Endpoint Antivirus. Esta información se proporciona para que se familiarice con el producto y como ayuda para que el ordenador sea más seguro.

Introducción

Antes de empezar a utilizar ESET Endpoint Antivirus, recuerde que nuestro producto lo pueden utilizar [usuarios conectados a través de ESET Security Management Center](#) y también puede utilizarse [solo](#). 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.



NOTA

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.



Importante

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.



Alerta

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.



Ejemplo

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.
<i>Cursiva</i>	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 Security Management Center o ESET PROTECT Cloud.

- [Introducción a ESET Security Management Center](#)
- [Introducción a ESET PROTECT Cloud](#)

Herramientas de administración remota de terceros

- [Supervisión y administración remotas \(RMM\)](#)

Prácticas recomendadas

- [Conectar todos los equipos con ESET Endpoint Antivirus a ESET Security Management Center](#)
- 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 Security Management Center

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

ESET Security Management Center (ESMC) es una nueva generación de sistema de administración remota que presenta diferencias considerables con respecto a las versiones anteriores de ESET Remote Administrator (ERA). Puesto que la arquitectura es completamente diferente, ESET Security Management Center 7 solo es parcialmente compatible con ERA 6 y no existe compatibilidad con la versión anterior ERA 5. No obstante, [se mantiene la compatibilidad con versiones anteriores de productos de seguridad de ESET](#).

Para realizar una implementación completa de la gama de soluciones de seguridad ESET, deben instalarse los siguientes componentes (plataformas Windows y Linux):

- [Servidor ESMC](#)
- [ESMC Consola web](#)
- [ESET Management Agent](#)

Los siguientes componentes de apoyo son opcionales, pero le recomendamos que los instale para que la aplicación alcance el máximo rendimiento en la red:

- [RD Sensor](#)
- [Apache HTTP Proxy](#)

- [Conector de dispositivo móvil](#)

Con ESET Security Management Center Web Console (ESMC 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.



Más información

Para obtener más información, consulte la guía del usuario de [ESET Security Management Center en línea](#).

Introducción a ESET PROTECT Cloud

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

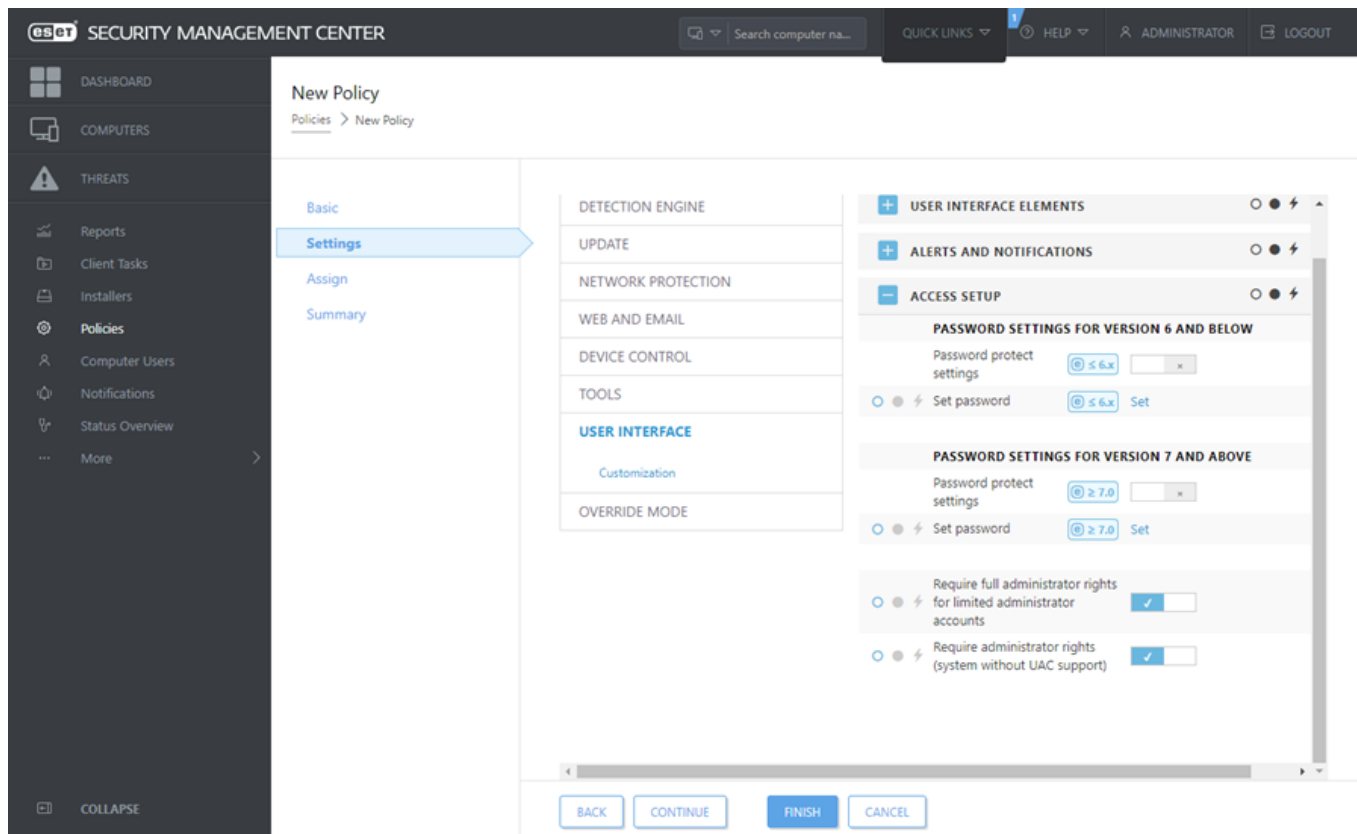
- [Lea más acerca de esto en la guía del usuario de ESET PROTECT Cloud en línea](#)

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. Haga clic en **Políticas** en el menú principal de la izquierda de ESMC Consola Web.
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 barra deslizante para activar **Contraseña para proteger la configuración**. En la versión 7 de los productos de ESET Endpoint se ha mejorado la protección. Si dispone de las versiones 6 y 7 de los productos de Endpoint en su red, configure una contraseña distinta para cada una de ellas. No se recomienda configurar solo la contraseña en el campo correspondiente a la versión 6, ya que hacerlo reducirá la seguridad de los productos de Endpoint de la versión 7.
7. Cree una contraseña nueva en la ventana emergente, 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 ESMC 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 en el que se establezcan los grupos estáticos. No ocurre lo mismo con los grupos dinámicos, ya que en este caso se aplican las políticas a los grupos dinámicos secundarios en primer lugar. Esto le permite aplicar políticas que tienen una mayor repercusión en la parte superior del árbol de grupos y políticas más específicas en los subgrupos. Con el uso de [indicadores](#), un usuario de ESET Endpoint 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 ESMC](#).



Asignación de políticas más genéricas

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



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, anexas, 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 ESMC 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 una política a un ordenador cliente que contiene ajustes con este indicador, esos ajustes modificarán la configuración local del ordenador cliente.



EJEMPLO: Permitir que los usuarios vean todas las políticas

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**.

Uso de ESET Endpoint Antivirus exclusivamente

Este apartado y el apartado [Uso de ESET Endpoint Antivirus](#) de esta guía del usuario se dirigen a aquellos usuarios que utilizan ESET Endpoint Antivirus sin ESET Security Management Center o ESET PROTECT Cloud. Todas las características y funciones de ESET Endpoint Antivirus son totalmente accesibles según los derechos de la cuenta del usuario.

Método de instalación

Existen varios métodos para instalar ESET Endpoint Antivirus versión 7.x 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 Security Management Center o ESET PROTECT Cloud](#).

- [Haga clic aquí si desea instalar ESET Endpoint Antivirus versión 6.6.x o actualizarlo a esa versión](#)

Métodos	Objetivo	Enlace 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
Instalación (.exe)	Proceso de instalación sin ESET AV Remover.	N/A
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 Security Management Center.	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 Security Management Center.	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

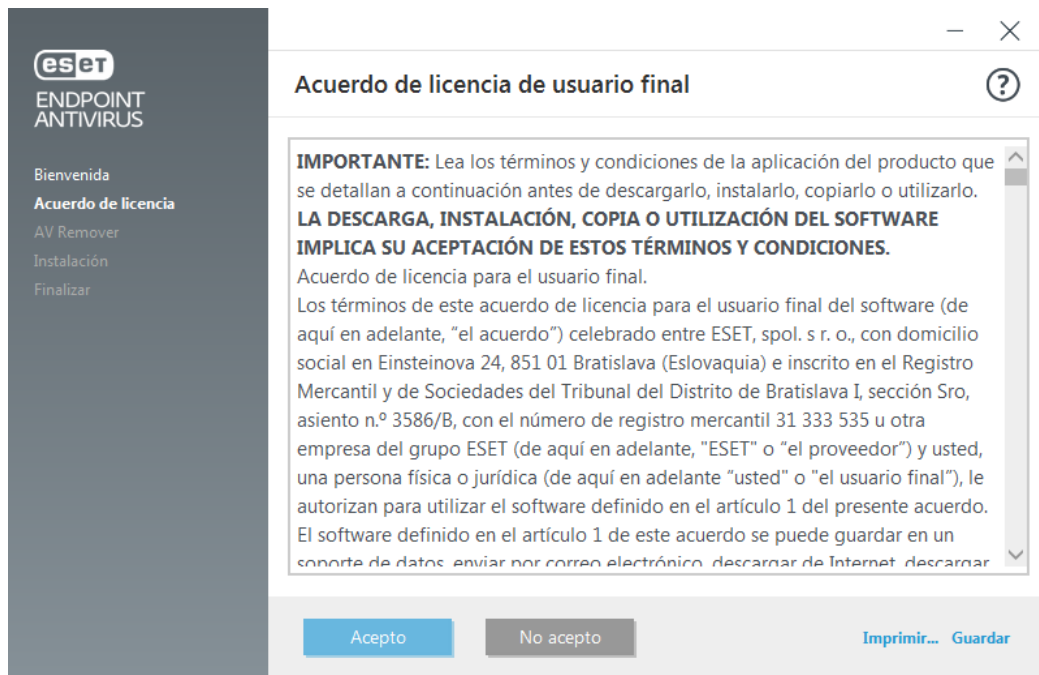
Antes de continuar con el proceso de instalación, es importante que desinstale las posibles aplicaciones de seguridad que tenga en el ordenador. Marque la casilla situada junto a **Quiero desinstalar aplicaciones antivirus con ESET AV Remover** para que ESET AV Remover analice el sistema y quite las [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.



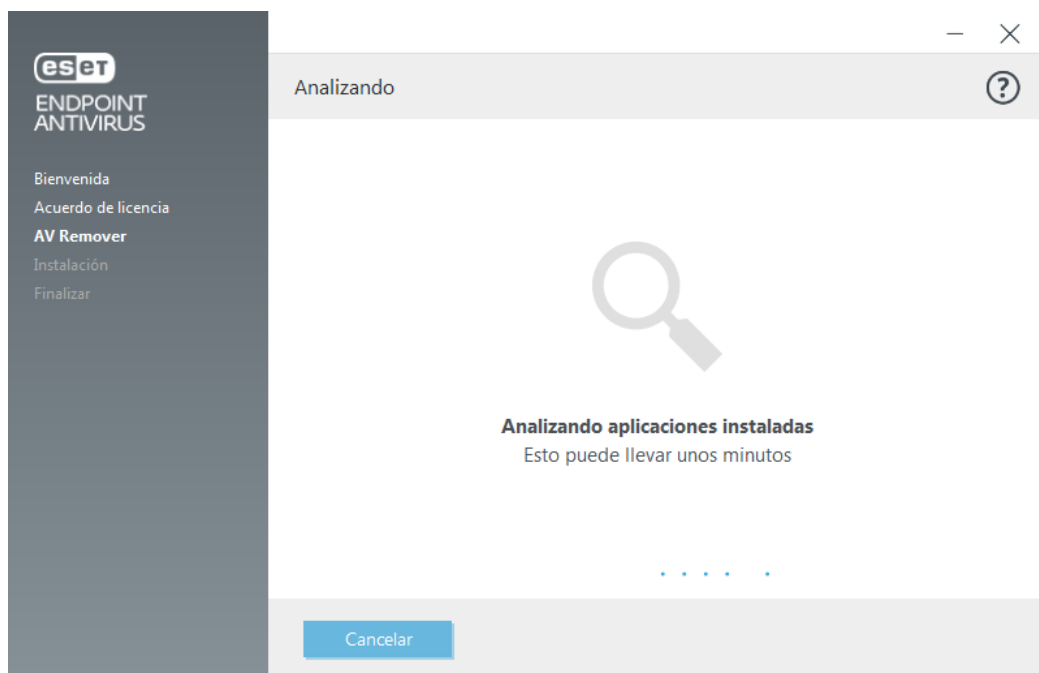
ESET AV Remover

La herramienta ESET AV Remover le ayuda a eliminar casi todos los programas antivirus que haya instalado anteriormente en su sistema. Siga las instrucciones expuestas a continuación para quitar un programa antivirus existente con ESET AV Remover:

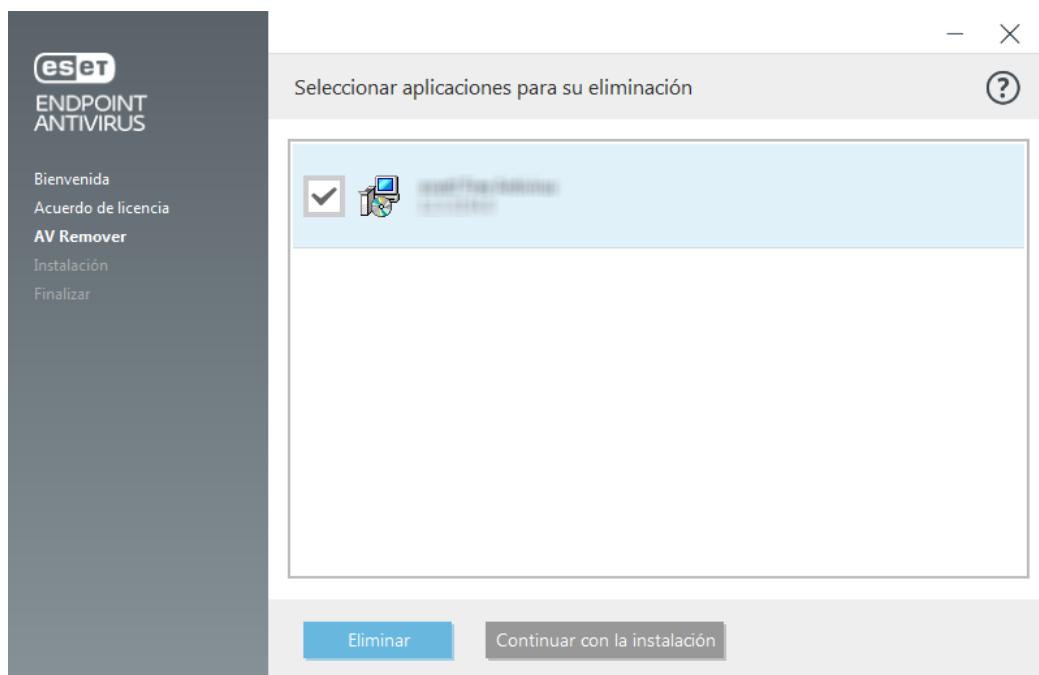
1. Para ver una lista del software antivirus que ESET AV Remover puede quitar, [visite el artículo de la base de conocimiento de ESET](#).
2. Lea el Acuerdo de licencia para el usuario final y haga clic en **Aceptar** para confirmar que acepta dicho acuerdo. Si hace clic en **No acepto**, la instalación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



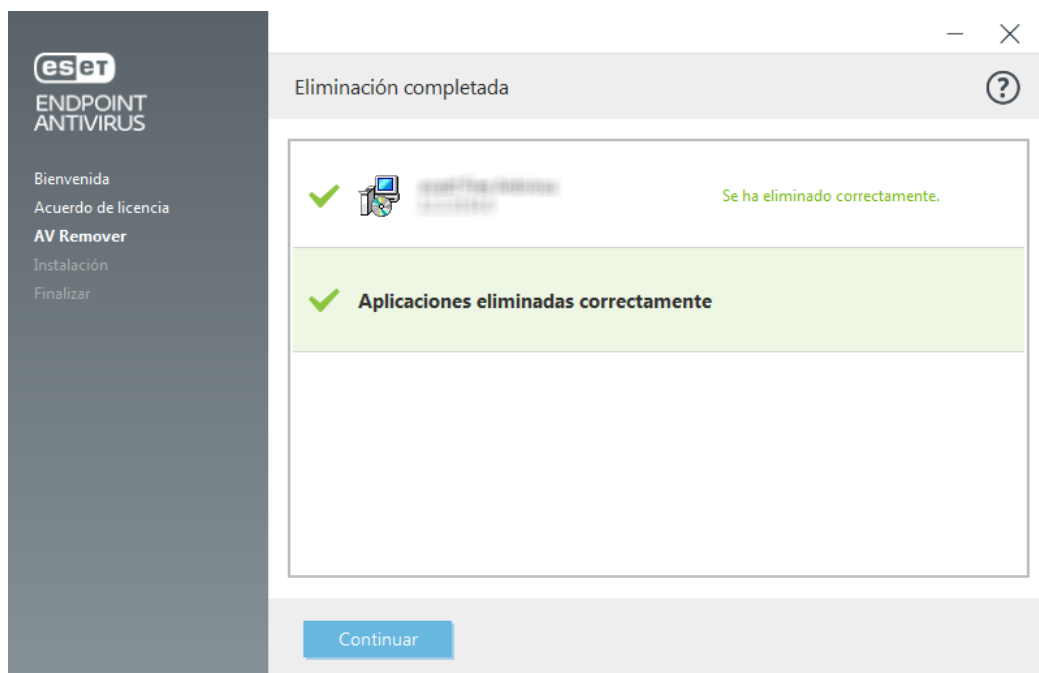
3.ESET AV Remover comenzará a buscar software antivirus en el sistema.



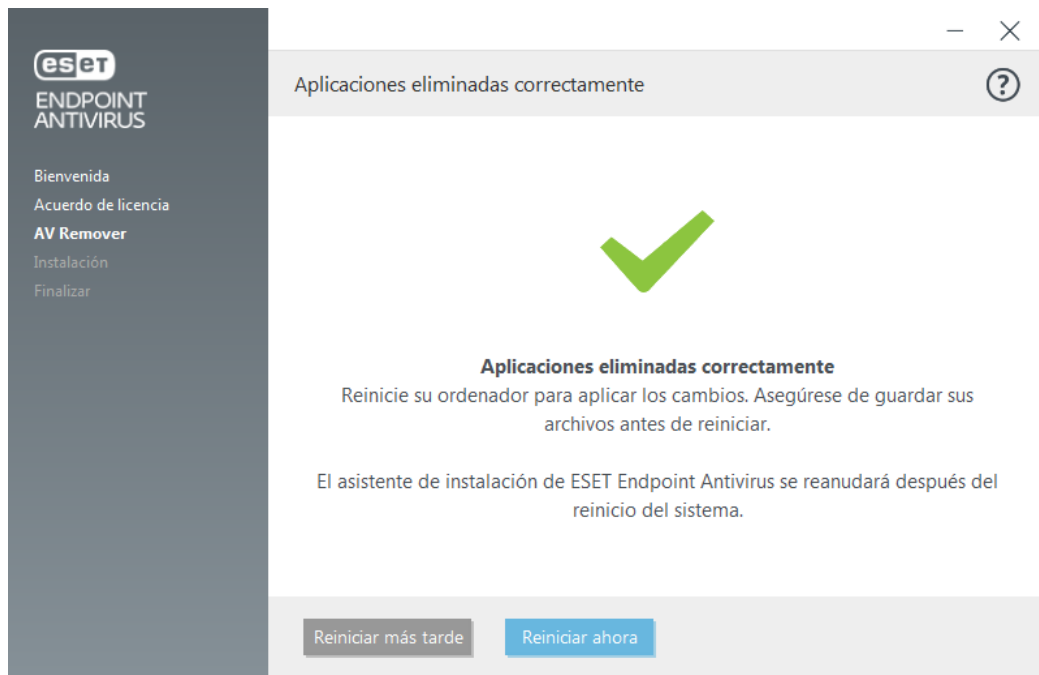
4.Seleccione las aplicaciones antivirus que aparezcan en la lista y haga clic en **Quitar**. Este proceso puede llevar unos minutos.



5. 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.

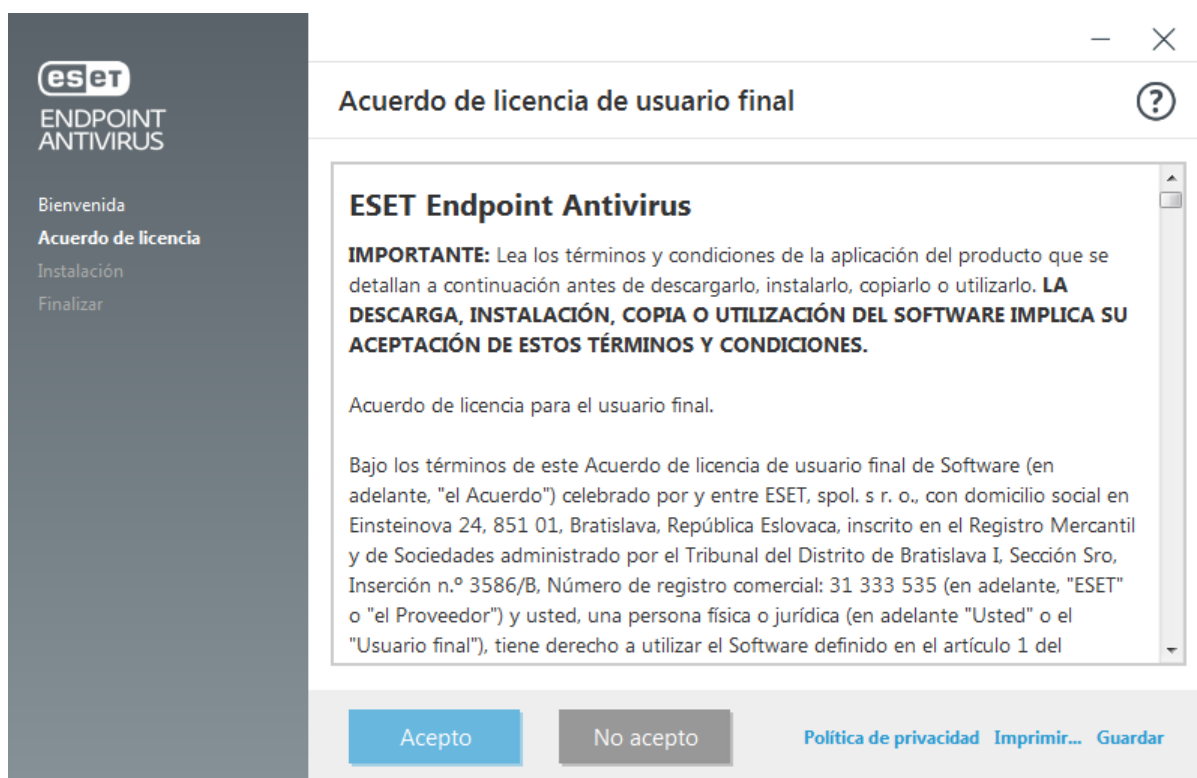


Importante

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



2. 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.

3. El siguiente paso del proceso de instalación consiste en configurar la detección de aplicaciones potencialmente indeseables. Consulte el capítulo [Aplicaciones potencialmente indeseables](#) para ver más detalles.

Para instalar ESET Endpoint Antivirus en una carpeta específica, haga clic en [Cambiar la carpeta de instalación](#).

5.El último paso es hacer clic en **Instalar** para confirmar la instalación. Una vez completada la instalación, se le pedirá que [active ESET Endpoint Antivirus](#).



Cómo cambiar la carpeta de instalación (.exe)

Una vez que haya seleccionado su preferencia para la detección de aplicaciones potencialmente indeseables y hecho clic en **Cambiar la carpeta de instalación**, se le solicitará que seleccione una ubicación para la carpeta de instalación del producto ESET Endpoint Antivirus. De forma predeterminada, el programa se instala en el directorio siguiente:

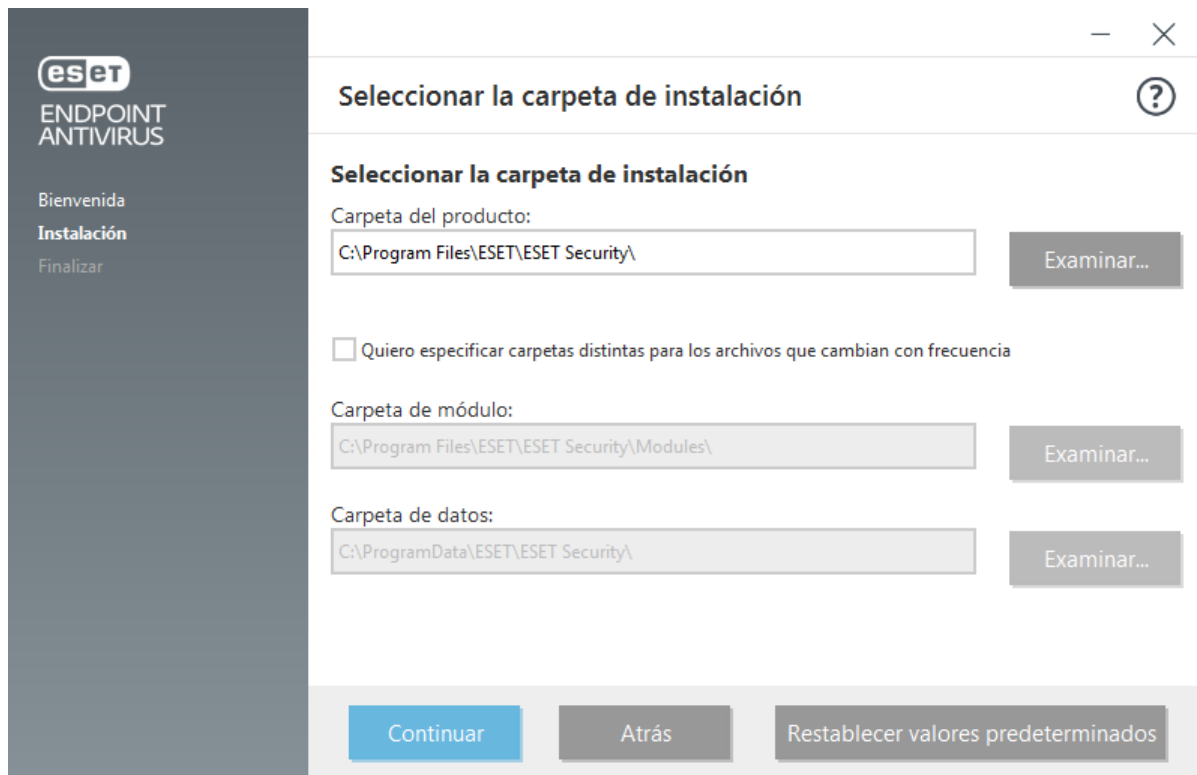
`C:\Program Files\ESET\ESET Security\`

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

`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 **Continuar** y, a continuación, en **Instalar** para iniciar la instalación.

Instalación (.msi)

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



Objetivo del instalador .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 Security Management Center.



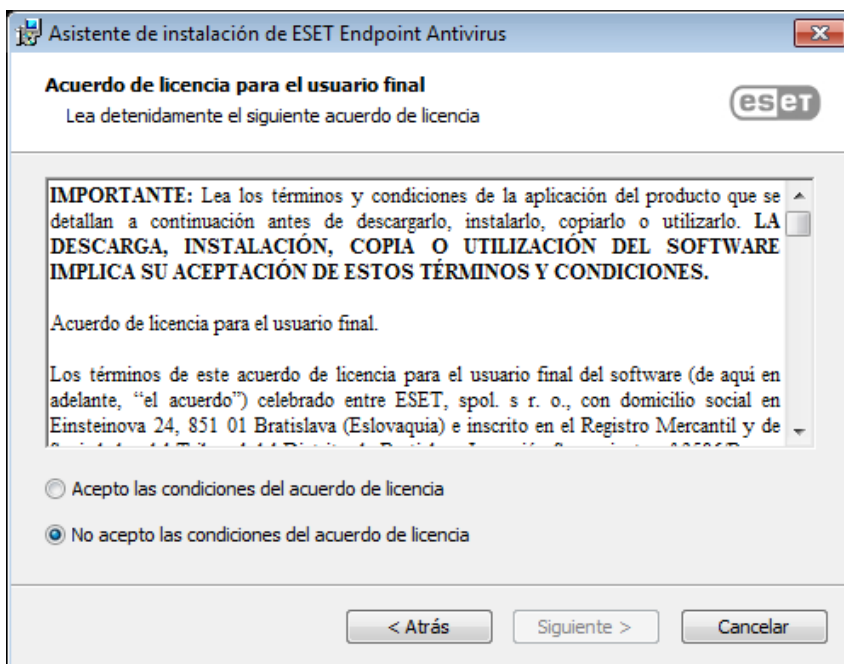
Importante

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).

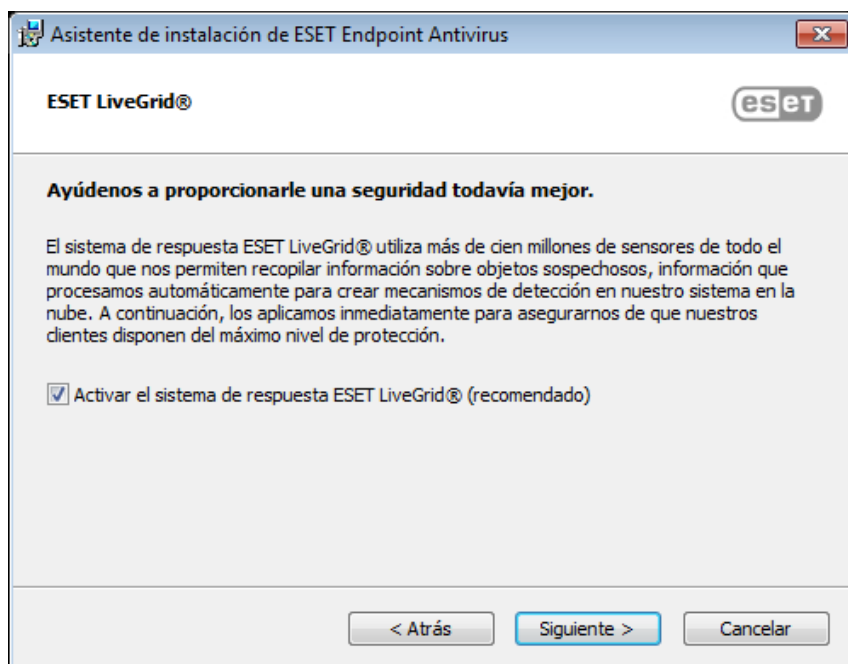
1. Seleccione el idioma que desee y haga clic en **Siguiente**.



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.

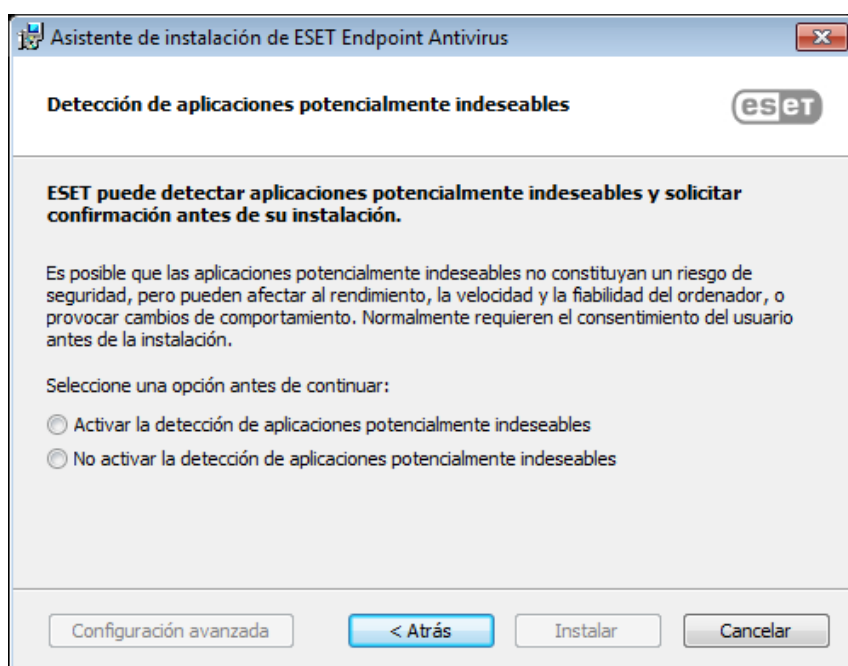


3. Indique si desea activar el sistema de respuesta [ESET LiveGrid®](#). ESET LiveGrid® garantiza que ESET recibe notificaciones inmediatas y continuas sobre nuevas infiltraciones, lo que le permite proteger mejor a sus clientes. El sistema le permite enviar nuevas amenazas al laboratorio de virus de ESET, donde se analizan, procesan y agregan al motor de detección.



4.El siguiente paso del proceso de instalación consiste en configurar la detección de aplicaciones potencialmente indeseables. Consulte el capítulo [Aplicaciones potencialmente indeseables](#) para ver más detalles.

Haga clic en **Configuración avanzada** si desea continuar con [Instalación avanzada \(.msi\)](#).



5.El último paso es hacer clic en **Instalar** para confirmar la instalación. Una vez completada la instalación, se le pedirá que [active ESET Endpoint Antivirus](#).

Instalación avanzada (.msi)

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

5.Una vez que haya seleccionado su preferencia para la detección de [aplicaciones potencialmente indeseables](#) y hecho clic en **Configuración avanzada**, se le solicitará que seleccione una ubicación para la carpeta de instalación del producto ESET Endpoint Antivirus. De forma predeterminada, el programa se instala en el directorio siguiente:

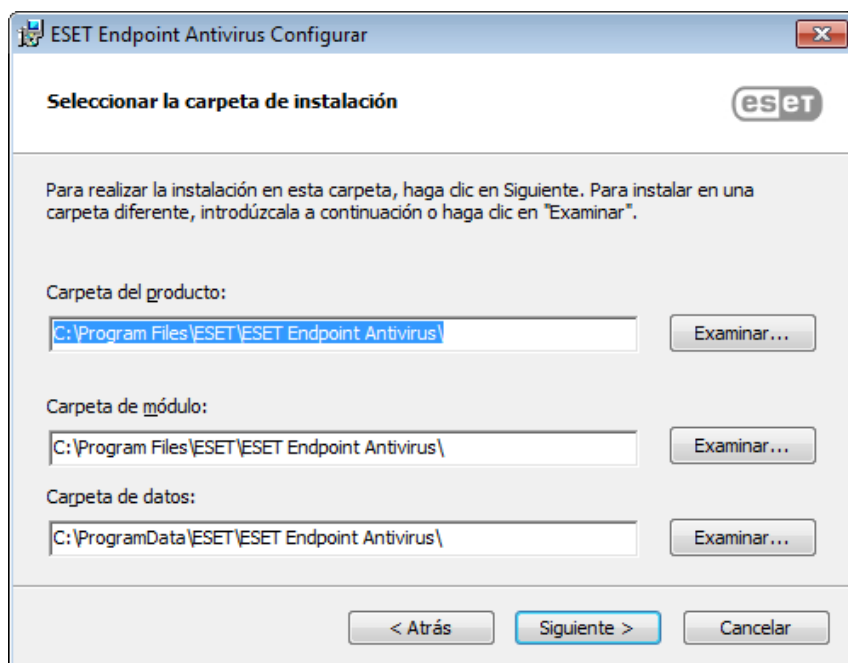
C:\Program Files\ESET\ESET Security\

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

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

C:\ProgramData\ESET\ESET Security\

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



7.El último paso es hacer clic en **Instalar** para confirmar la instalación.

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 Security Management Center.

Parámetros admitidos

APPDIR=<ruta de acceso>

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

APPDATADIR=<ruta de acceso>

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

MODULEDIR=<ruta de acceso>

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

ADDLOCAL=<lista>

- 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](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



Nota

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



Nota

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 del dispositivo	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
Web y correo electrónico	WebAndEmail		Marcador de posición
Web y correo electrónico/Filtrado de protocolos	ProtocolFiltering	WebAndEmail	Invisible
Protección de la web y el correo electrónico/acceso a la web	WebAccessProtection	WebAndEmail	Opcional
Protección de la web y el correo electrónico/cliente de correo electrónico	EmailClientProtection	WebAndEmail	Opcional
Web y correo electrónico/Protección del cliente de correo electrónico/Cientes de correo electrónico	MailPlugins	EmailClientProtection	Invisible
Protección de la web y el correo electrónico/cliente de correo electrónico/antispam	Antispam	EmailClientProtection	Opcional
Control de la web y el correo electrónico/web	WebControl	WebAndEmail	Opcional
Herramientas/ESET RMM	Rmm		Opcional
Actualización/Perfiles/Mirror de actualización	UpdateMirror		Opcional
Complemento de ESET Enterprise Inspector	EnterprisInspector		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 UPDTEMIRROR.

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	Programa 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=	<puerto>	Número de puerto del servidor proxy
CFG_PROXY_USERNAME=	<nombre de usuario>	Nombre de usuario para autenticación
CFG_PROXY_PASSWORD=	<contraseña>	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=	<ruta>	Ruta de acceso de la configuración XML exportada (valor predeterminado <i>cfg.xml</i>)

LiveGrid® propiedad

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

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)
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 .

Ejemplos de instalación desde la línea de comandos



Importante

Asegúrese de leer el [Acuerdo de licencia de usuario final](#) y de tener privilegios administrativos antes de ejecutar la instalación.



Ejemplo

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



Ejemplo

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
```



Ejemplo

Instale en un directorio de instalación de aplicaciones distinto al [predeterminado](#).

```
msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\
```



Ejemplo

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
```



Ejemplo

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
```



Ejemplo

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](#) o [implementarlo de forma remota con una tarea del servidor en ESMC](#), 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 Security Management Center (ESMC). Debe tener ESMC 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 ESMC.
- 5.[Implemente y active ESET Endpoint Antivirus en sus ordenadores cliente](#).



Instrucciones con ilustraciones

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 \(7.x\)](#)
- [Implementar ESET Management Agent con un Objeto de política de grupo \(GPO\)](#)

^ v

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 Security Management Center, ESET Remote Administrator (solo productos ESET Endpoint versión 6.x) o ESET PROTECT Cloud.
2. Actualización manual mediante la descarga e [instalación de una versión más reciente](#) sobre la instalación existente.

Escenarios de actualización recomendados

[Actualización remota](#)

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

- [ESET Security Management Center | Construcción y dimensionamiento de la infraestructura](#)
- [ESET Remote Administrator | Procedimientos de actualización, migración y reinstalación](#)
- [ESET Security Management Center | Procedimientos de actualización, migración y reinstalación](#)
- [Introducción a ESET PROTECT Cloud](#)

[Actualización manual en una estación de trabajo cliente](#)

Si tiene pensado gestionar las actualizaciones en estaciones de trabajo cliente individuales manualmente:

1. Primero verifique los requisitos previos de actualización de ESET Endpoint Antivirus:

Actualización desde	Actualización a	Requisitos previos de actualización
6.x	7.x	<ul style="list-style-type: none">• Sin requisitos previos• Nota: La versión 7 de ESET Endpoint Antivirus no puede administrarse mediante ESET Remote Administrator
6.x	6.6.x	<ul style="list-style-type: none">• Sin requisitos previos
5.x	7.x	<ul style="list-style-type: none">• Compruebe que su sistema operativo sea compatible. Por ejemplo, Windows XP no es compatible con la versión 7.• Compruebe si sus versiones de productos de ESET Endpoint admiten la actualización desde la versión 5.x.
4.x	7.x	<ul style="list-style-type: none">• Compruebe que su sistema operativo sea compatible.• Desinstale ESET NOD32 Antivirus Business Edition o ESET Smart Security Business Edition. No instale la versión 7 sobre una versión 4.x.

2. Descargue e [instale una versión más reciente](#) sobre la anterior.

Problemas de instalación comunes

Si ocurren problemas durante la instalación, consulte nuestra lista de [errores de instalación comunes y resoluciones](#) para encontrar una solución para su problema.

Error de activación

Si no se puede activar ESET Endpoint Antivirus, las posibles causas más frecuentes son:

- La clave de licencia se encuentra en uso actualmente.
- Clave de licencia no válida. Error en el formulario de activación del producto.
- Falta información adicional necesaria para la activación o la información no es válida.
- Error al establecer la comunicación con la base de datos de activación. Vuelva a intentar la activación en 15 minutos.
- 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](#)

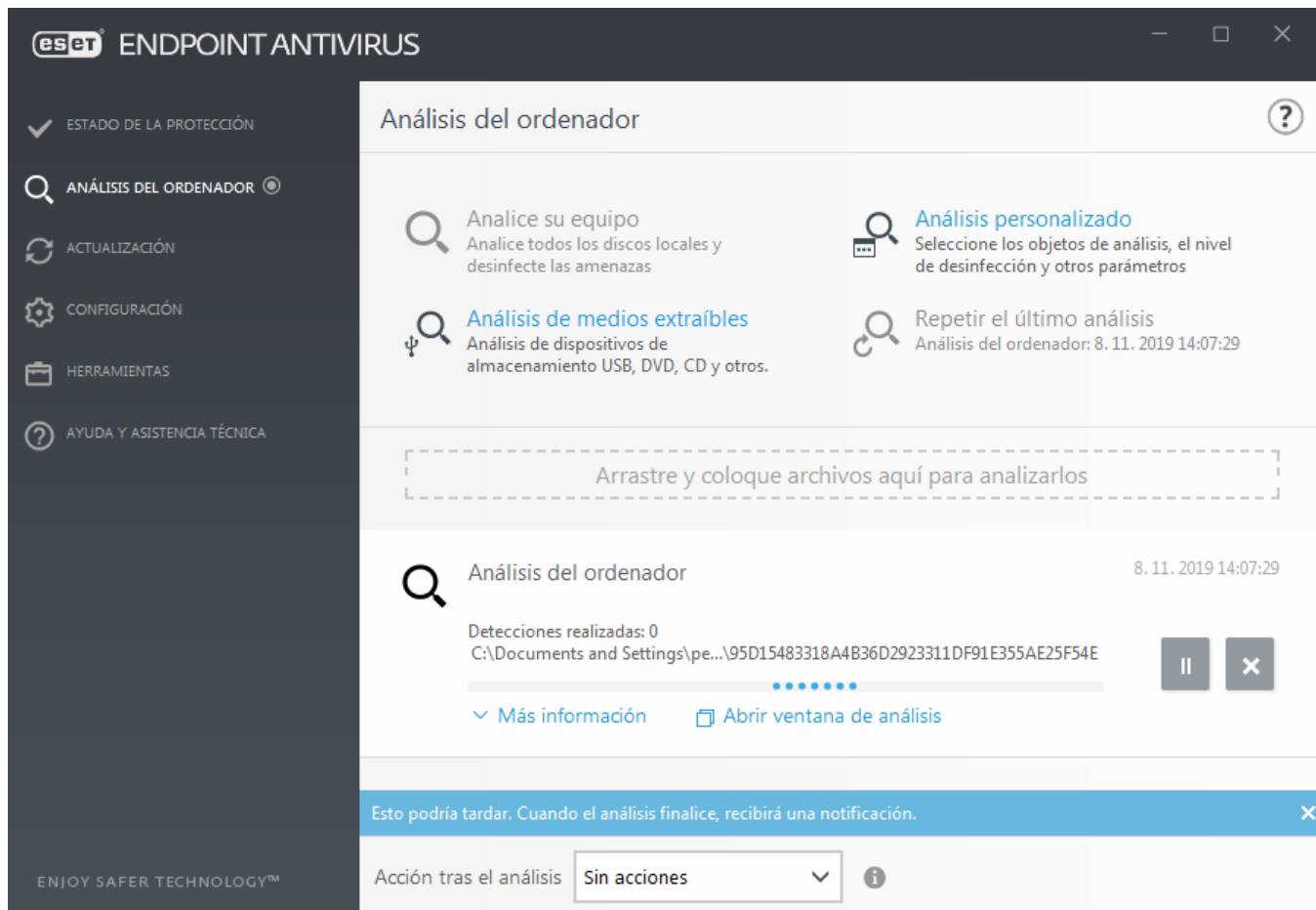
Activación del producto

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

Seleccione uno de los métodos disponibles para activar ESET Endpoint Antivirus. Consulte [Cómo activar ESET Endpoint Antivirus](#) para obtener más información.

Análisis del ordenador

Le recomendamos que realice análisis periódicos del ordenador, o [programe un análisis periódico](#), para detectar amenazas. En la ventana principal del programa, haga clic en **Análisis del ordenador** y, a continuación, en **Análisis estándar**. Encontrará más información sobre los análisis del ordenador en [Análisis del ordenador](#).



Guía para principiantes

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

Interfaz de usuario

La ventana principal del programa ESET Endpoint Antivirus se divide 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.

A continuación, se muestra una descripción de las opciones del menú principal:

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

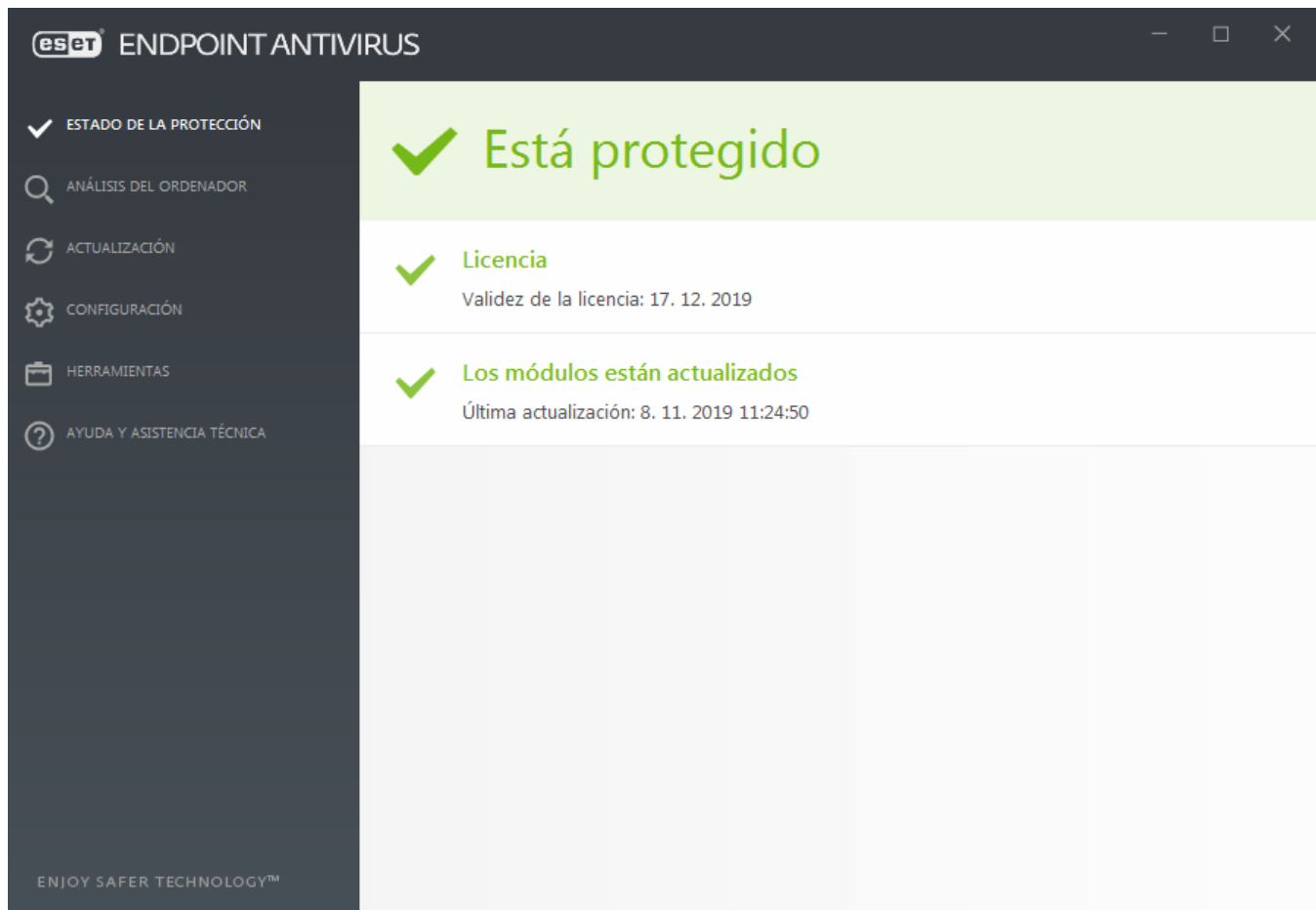
Análisis del ordenador: esta opción le permite configurar e iniciar el análisis estándar, el análisis personalizado o el análisis de medios extraíbles. También se puede repetir el último análisis ejecutado.

Actualización: muestra información sobre el motor de detección y permite buscar manualmente si hay actualizaciones.

Configuración: seleccione esta opción para ajustar su ordenador o configuración de seguridad de la Web y el correo electrónico.

Herramientas: proporciona acceso a Archivos de registro, Estadísticas de protección, Observar actividad, Procesos en ejecución, Planificador de tareas, Cuarentena, ESET SysInspector y ESET SysRescue para crear un CD de recuperación. También puede enviar una muestra para su análisis.

Ayuda y soporte: proporciona acceso a los archivos de ayuda, la [base de conocimiento de ESET](#) y el sitio web de ESET. Aquí también se proporcionan enlaces para abrir una solicitud de soporte técnico, herramientas de soporte e información sobre la activación del producto.

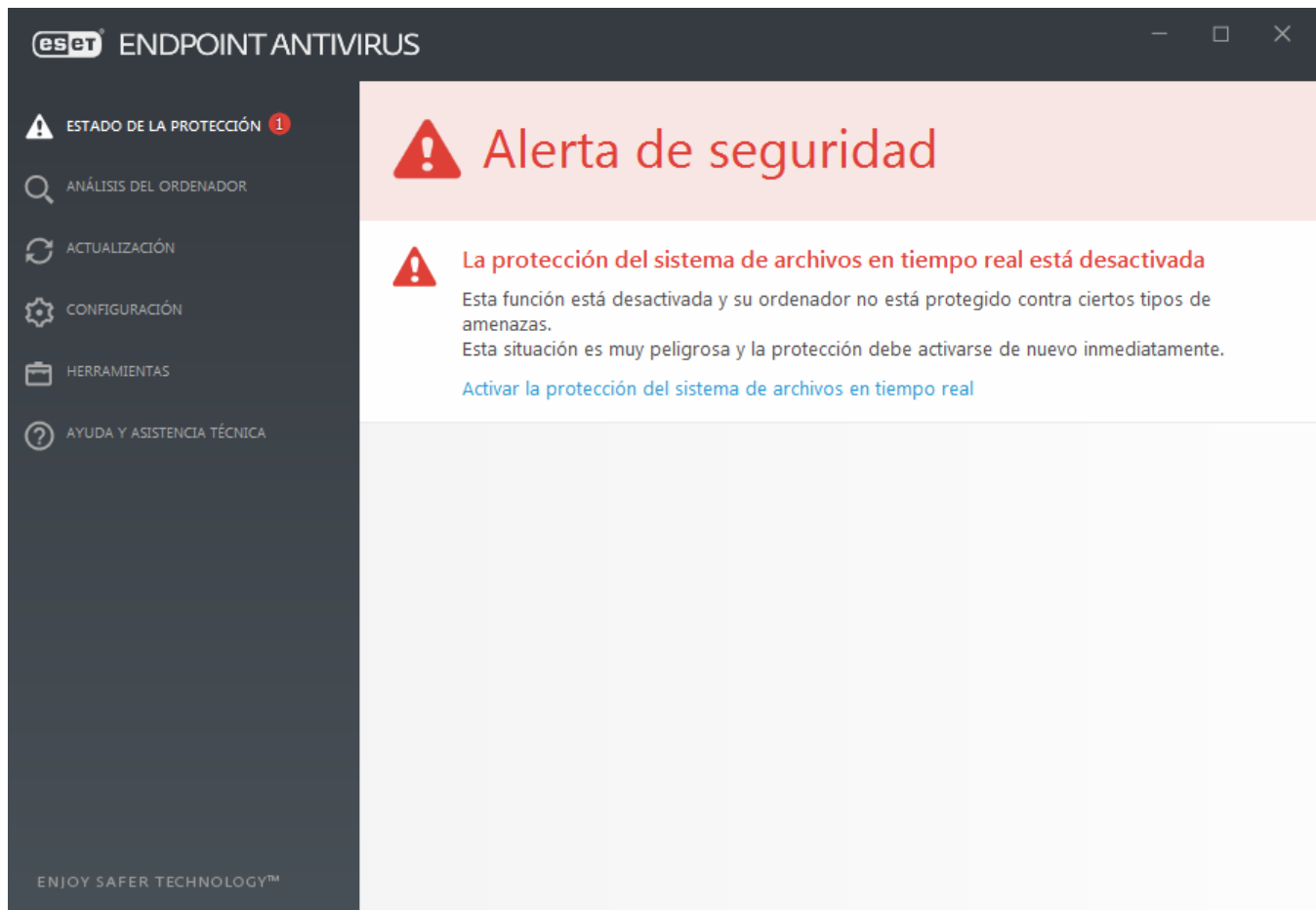


En la pantalla **Estado de la protección** se proporciona información sobre el nivel de seguridad y de protección actual del ordenador. El icono de estado verde de **Máxima protección** indica que se garantiza la protección máxima.

En la ventana de estado también se proporcionan enlaces rápidos a las características más habituales de ESET Endpoint Antivirus e información sobre la última actualización.

¿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 La licencia ha caducado:** 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 en Configuración avanzada. 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**.
- **ESET LiveGrid® está desactivado:** este problema se indica cuando ESET LiveGrid® está desactivado en Configuración avanzada.
- **No hay actualizaciones regulares programadas:** ESET Endpoint Antivirus no buscará ni recibirá actualizaciones importantes a menos que programe la tarea de actualización.

- **Anti-Stealth está desactivado:** haga clic en **Activar Anti-Stealth** para volver a activar esta funcionalidad.
- **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 ESMC. 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**.
- **Su licencia caducará en breve:** esto se indica mediante el icono de estado de la protección, que muestra un signo de exclamación. Cuando expire la licencia, el programa no se podrá actualizar y el icono del estado de la protección se volverá rojo.
- **La protección antispam está en pausa:** haga clic en **Habilitar la protección antispam 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.



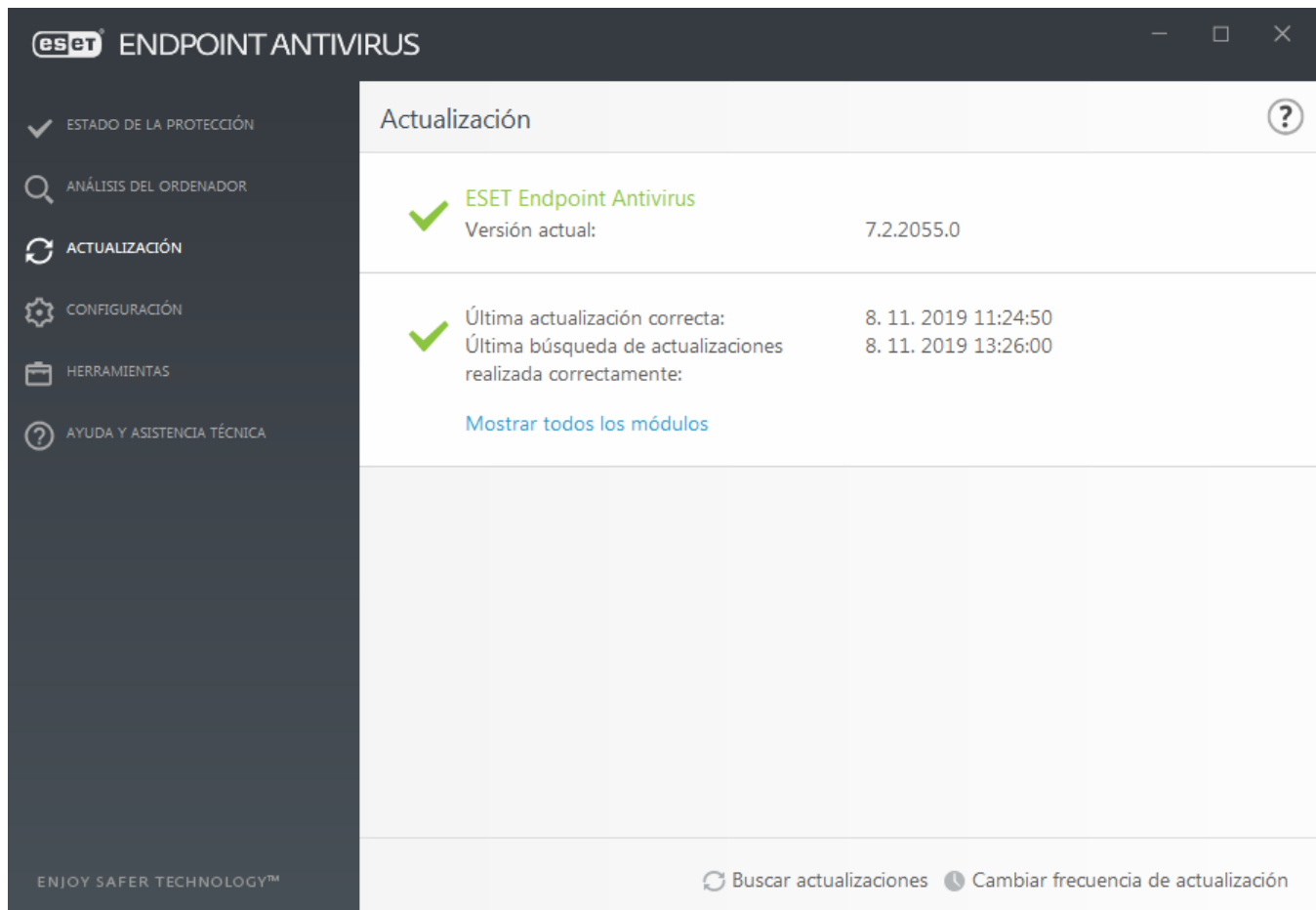
Nota

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

Configuración de actualizaciones

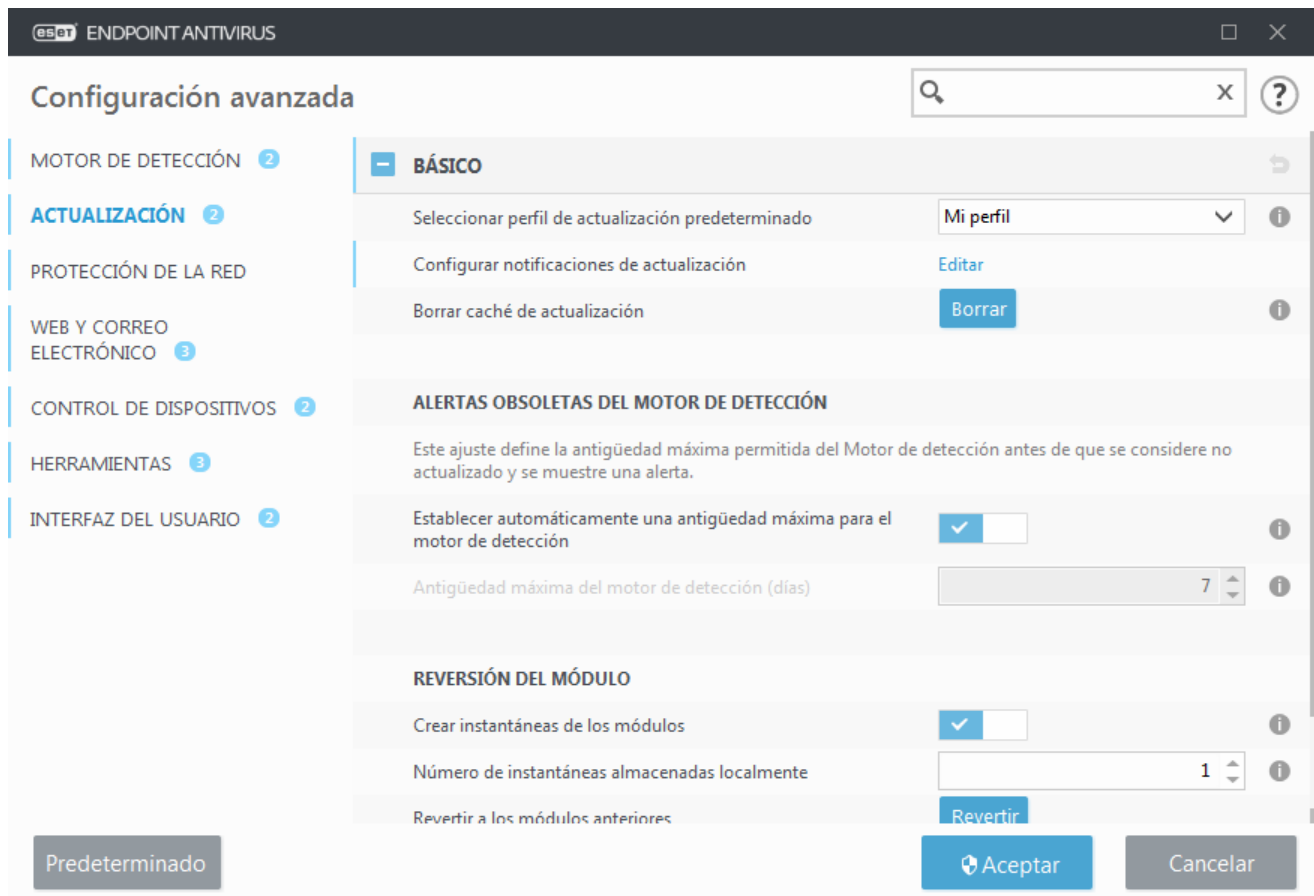
La actualización de los módulos es una parte importante de mantener una protección completa contra el código malicioso. Preste especial atención a la configuración y al funcionamiento de las actualizaciones. En el menú principal, seleccione **Actualizar > Buscar actualizaciones** para comprobar si hay alguna actualización de los módulos más reciente.

Si no introduce su **Clave de licencia**, no podrá recibir actualizaciones nuevas y se le pedirá que active su producto.



La ventana Configuración avanzada (haga clic en **Configuración** > **Configuración avanzada** en el menú principal o pulse **F5** en el teclado) ofrece más opciones de actualización. Para configurar las opciones avanzadas de actualización, como el modo de actualización, el acceso al servidor proxy, las conexiones LAN y los ajustes de creación de copia del motor de detección; haga clic en **Actualizar** en el árbol de configuración avanzada.

- Si está experimentando problemas con una actualización, haga clic en **Borrar** para borrar la caché de actualización temporal.



- La opción **Elegir automáticamente** de **Perfiles > Actualizaciones > Actualizaciones de 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.
- Si no quiere que aparezca en la bandeja del sistema de la parte inferior derecha de la pantalla la notificación que indica que la actualización se ha realizado correctamente, despliegue **Perfiles > Actualizaciones**, haga clic en **Editar** junto a **Seleccionar notificaciones de actualización recibidas** y, a continuación, ajuste las casillas de verificación para la notificación **El motor de detección se ha actualizado correctamente**.

Para optimizar la funcionalidad, es importante que el programa se actualice automáticamente. Esto solo es posible 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 más información detallada sobre la activación, consulte [Cómo activar ESET Endpoint Antivirus](#) e introduzca las credenciales que recibió al adquirir el producto de seguridad de ESET en la ventana **Detalles de la licencia**.

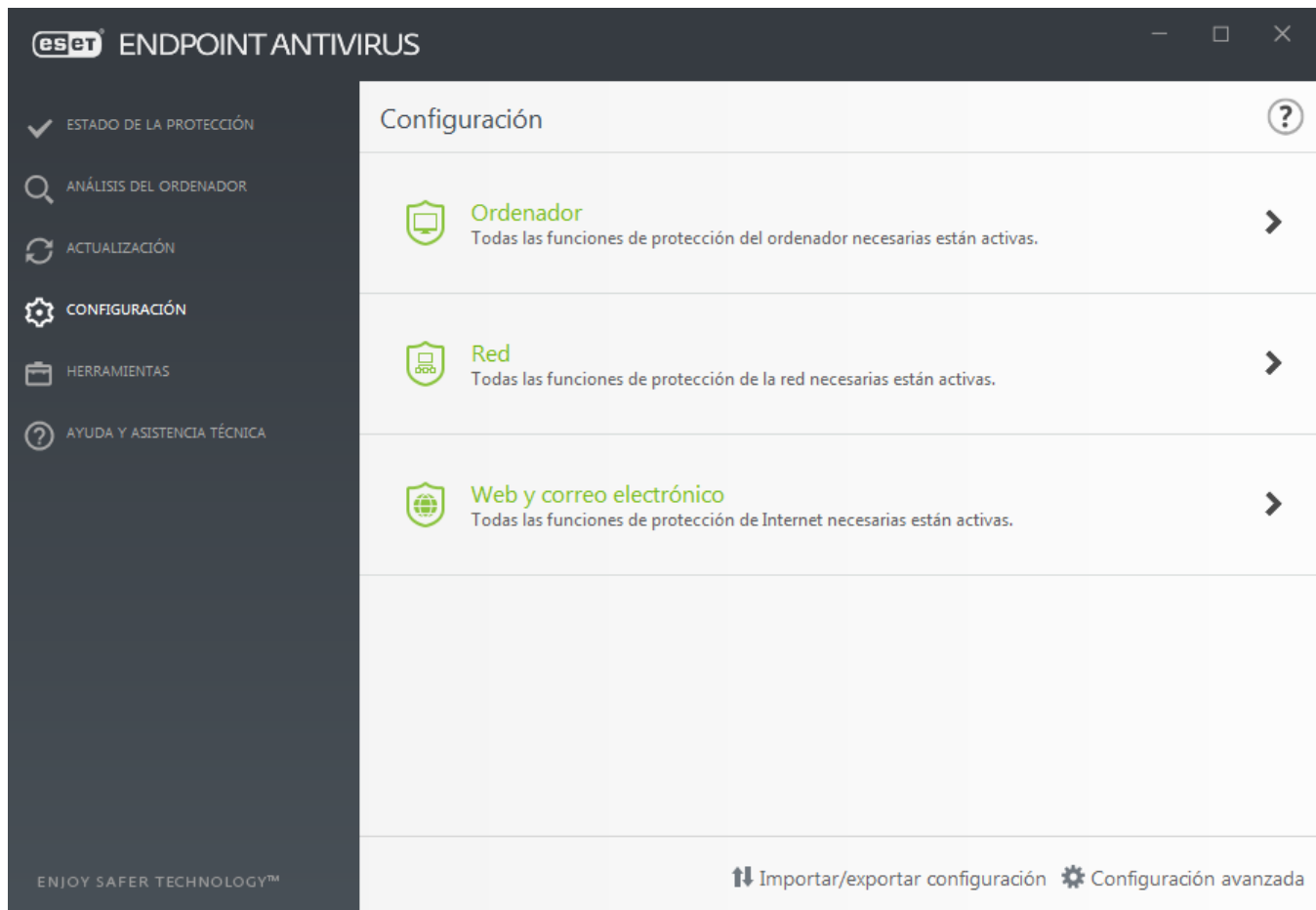
Uso de ESET Endpoint Antivirus

Las opciones de configuración de ESET Endpoint Antivirus le permiten ajustar el nivel de protección del ordenador, la Web y el correo electrónico.



Nota

Al crear una política desde ESET Security Management Center 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 ESMC](#).



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

- **Ordenador**
- **Red**
- **Web y correo electrónico**

La sección **Ordenador** le permite activar o desactivar los siguientes componentes:


- **Protección del sistema de archivos en tiempo real:** se analizan todos los archivos en busca de código malicioso cuando se abren, crean o ejecutan.
- **Control del dispositivo:** permite [controlar](#) los dispositivos (CD, DVD, USB, etc.) automáticamente. Este módulo le permite bloquear o ajustar los filtros/permisos ampliados y definir la capacidad de los usuarios para acceder a un dispositivo y trabajar con 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®. [Puede obtener 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 ventanas emergentes, 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.


La sección **Protección de la red** le permite configurar la Protección contra los ataques de red (IDS) y la [Protección contra botnets](#).

La configuración de protección de **Web y correo electrónico** le permite activar o desactivar los siguientes componentes:

- **Protección del acceso a la Web:** si esta opción está activada, se analiza todo el tráfico a través de HTTP o HTTPS para detectar la presencia de software malicioso.
- **Protección del cliente de correo electrónico:** controla las comunicaciones recibidas a través de los protocolos POP3 e IMAP.
- **Protección Anti-Phishing:** le protege frente a intentos de adquirir contraseñas, datos bancarios y otra información confidencial por parte de sitios web que suplantan a sitios legítimos.

Si desea desactivar temporalmente algún módulo individual, haga clic en el **conmutador verde**  situado junto al módulo deseado. Tenga en cuenta que esto puede disminuir el nivel de protección del ordenador.


Para volver a activar la protección de un componente de seguridad desactivado, haga clic en el conmutador rojo .

Cuando se aplique la política de ESMC/ERA, verá el icono del candado  junto a un componente específico. La política aplicada por ESET Security Management Center 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 ESMC](#).



Nota

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


Para acceder a la configuración detallada de un componente de seguridad determinado, haga clic en la rueda dentada  que aparece junto a cualquier componente.

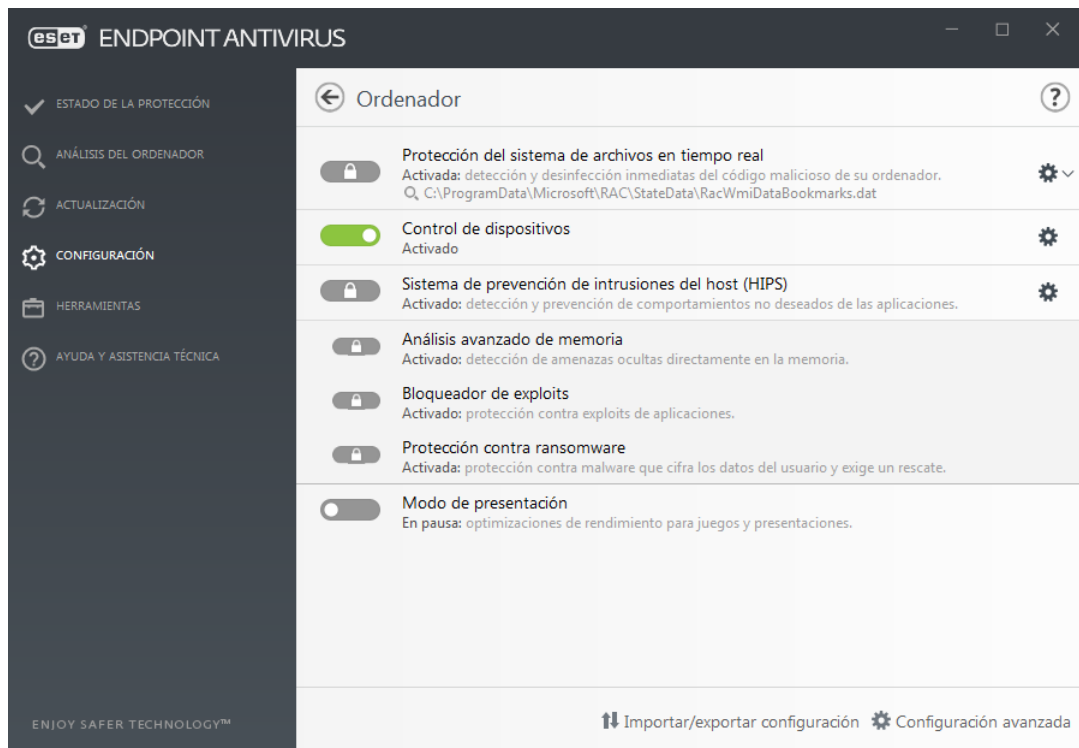
En la parte inferior de la ventana de configuración encontrará opciones adicionales. Para cargar los parámetros de configuración con un archivo de configuración *.xml*, o para guardar los parámetros de configuración actuales en un archivo de configuración, utilice la opción **Importar/exportar configuración**. Consulte [Importar/exportar configuración](#) para obtener más información detallada.

Si desea acceder a opciones más detalladas, haga clic en **Configuración avanzada** o pulse **F5**.

Ordenador

El módulo **Ordenador** está disponible en **Configuración > Ordenador**. En él se muestra una visión general de los módulos de protección que se describen en el [capítulo anterior](#). En esta sección están disponibles los parámetros siguientes:

Haga clic en la rueda dentada  situada junto a **Protección del sistema de archivos en tiempo real** y haga clic en **Editar exclusiones** para abrir la [ventana Configuración de exclusiones](#), que le permite excluir archivos y carpetas del análisis.



La sección **Ordenador** le permite 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.
- **Control del dispositivo:** permite [controlar](#) los dispositivos (CD, DVD, USB, etc.) automáticamente. Este módulo le permite bloquear o ajustar los filtros/permisos ampliados y definir la capacidad de los usuarios para acceder a un dispositivo y trabajar con 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®. [Puede obtener 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 ventanas emergentes, 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**.

Motor de detección (7.2 y posteriores)

El motor de detección protege frente a ataques maliciosos al sistema controlando la comunicación de archivo, correo electrónico e Internet. Por ejemplo, si se detecta un objeto clasificado como malware, se inicia la corrección. El motor de detección puede eliminar este objeto bloqueándolo primero y, a continuación, desinfectándolo, eliminándolo o poniéndolo en cuarentena.

Para configurar los ajustes detallados del motor de detección, haga clic en **Configuración avanzada** o pulse **F5**.

En esta sección:

- [Categorías de protección en tiempo real y de aprendizaje automático](#)
- [Análisis de malware](#)
- [Configuración de informes](#)
- [Configuración de la protección](#)
- [Prácticas recomendadas](#)



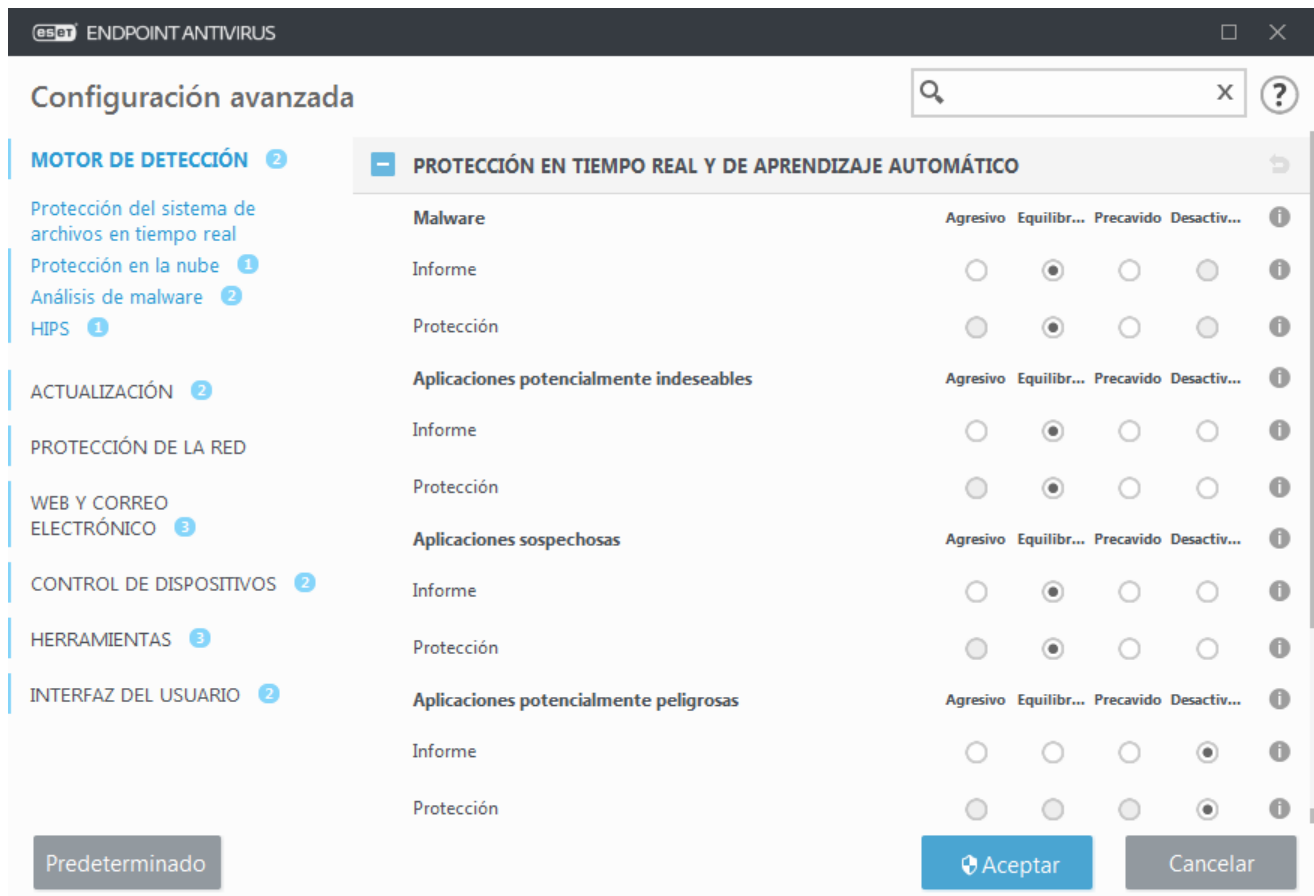
Cambios en la configuración del análisis del motor de detección

A partir de la versión 7.2, la sección Motor de detección ya no incluye interruptores de activación/desactivación [como en la versión 7.1 y anteriores](#). Los botones de activación/desactivación han sido sustituidos por cuatro umbrales: Agresivo, Equilibrado, Precavido y Desactivado.

Categorías de protección en tiempo real y de aprendizaje automático

Protección en tiempo real y de aprendizaje automático en todos los módulos de protección (por ejemplo, Protección del sistema de archivos en tiempo real, Protección de acceso a la web, etc.) le permite configurar informes y niveles de protección de las siguientes categorías:

- **Malware:** un virus informático es un fragmento de código malicioso que antecede o sigue a los archivos existentes en el 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](#).
- **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](#).
- Entre las **aplicaciones sospechosas** se incluyen programas comprimidos con [empaquetadores](#) o protectores. Los autores de código malicioso con frecuencia explotan estos tipos de protectores para evitar ser detectados.



Protección mejorada

Aprendizaje automático avanzado forma ahora parte del motor de detección como capa avanzada de protección que mejora la detección con aprendizaje automático. Lea más información sobre este tipo de protección en el [glosario](#).

Análisis de malware

Los ajustes del análisis se pueden configurar de forma independiente para el análisis en tiempo real y el [análisis a petición](#). De forma predeterminada, **Usar ajustes de protección en tiempo real** está activado. Cuando está activado, los ajustes del análisis a petición relevantes se heredan de la sección **Protección en tiempo real y de aprendizaje automático**.

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. 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. Es posible 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 puede 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

* Disponible en ESET Endpoint Antivirus versión 7.2 y posteriores.

** 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** representa un nivel de protección comparable al de las versiones anteriores de ESET Endpoint Antivirus (7.1 y anteriores). 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.

[Tabla de conversión de políticas de ESMC para ESET Endpoint Antivirus 7.1 y anteriores](#)

A partir de ESMC, el editor de políticas de los ajustes del análisis ya no contiene interruptores de activación/desactivación de cada CATEGORÍA. La tabla que aparece a continuación resume la conversión entre el umbral de protección y el estado final del [interruptor en ESET Endpoint Antivirus 7.1 y anteriores](#).

Estado de umbral de CATEGORÍA Agresivo Equilibrado Precavido Desactivado

Interruptor de CATEGORÍA aplicado ☒ ☒ ☒ ☐ x

Cuando se actualice desde las versiones 7.1 y anteriores a la versión 7.2 y posteriores, el nuevo estado de umbral será el siguiente:

Interruptor de categoría antes de la actualización ☒ ☐ x

Nuevo umbral de CATEGORÍA después de la actualización Equilibrado Desactivado

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 ESMC que no falte ninguna detección.

Opciones avanzadas del motor de detección

La **tecnología Anti-Stealth** es un sofisticado sistema de detección de programas peligrosos como [rootkits](#), que pueden ocultarse del sistema operativo. Esto implica que no es posible detectarlos mediante las técnicas habituales.

Activar análisis avanzado mediante AMSI: herramienta Interfaz de análisis contra el código malicioso de Microsoft que permite que los desarrolladores de aplicaciones creen nuevas defensas contra el código malicioso (solo para Windows 10).

Motor de detección (7.1 y anteriores)

El motor de detección protege frente a ataques maliciosos al sistema controlando la comunicación de archivo, correo electrónico e Internet. Por ejemplo, si se detecta un objeto clasificado como malware, se inicia la corrección. El motor de detección puede eliminar este objeto bloqueándolo primero y, a continuación, desinfectándolo, eliminándolo o poniéndolo en cuarentena.

Para configurar los ajustes detallados del motor de detección, haga clic en **Configuración avanzada** o pulse **F5**.



Cambios en la configuración del análisis del motor de detección
A partir de la versión 7.2, la sección Motor de detección [tiene otro aspecto](#).

Opciones del módulo de análisis de todos los módulos de protección (por ejemplo, Protección del sistema de archivos en tiempo real, Protección de acceso a la Web, etc.) le permiten activar o desactivar la detección de los siguientes elementos:

- **Aplicaciones potencialmente indeseables** – El grayware (o aplicaciones potencialmente indeseables [PUA]) es una amplia categoría de software no inequívocamente malintencionado, al contrario de lo que sucede con otros tipos de malware, como virus o troyanos. Sin embargo, puede instalar software adicional no deseado, 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](#).
- Por **aplicaciones potencialmente peligrosas** se entienden programas de software comercial legítimo que pueden utilizarse con fines maliciosos. Entre los ejemplos de este tipo de programas encontramos herramientas

de acceso remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que registran cada tecla pulsada por un usuario). Esta opción está desactivada de manera predeterminada. Puede obtener más información sobre estos tipos de aplicaciones en el [glosario](#).

- Entre las **aplicaciones sospechosas** se incluyen programas comprimidos con [empaquetadores](#) o protectores. Los autores de código malicioso con frecuencia explotan estos tipos de protectores para evitar ser detectados.

La **tecnología Anti-Stealth** es un sofisticado sistema de detección de programas peligrosos como [rootkits](#), que pueden ocultarse del sistema operativo. Esto implica que no es posible detectarlos mediante las técnicas habituales.

Exclusiones le permite excluir objetos del análisis. Consulte [Exclusiones](#) si desea más información.

Activar análisis avanzado mediante AMSI: herramienta Interfaz de análisis contra el código malicioso de Microsoft que permite que los desarrolladores de aplicaciones creen nuevas defensas contra el código malicioso (solo para Windows 10).

Configuración avanzada

MOTOR DE DETECCIÓN 1

- Protección del sistema de archivos en tiempo real
- Protección en la nube
- Análisis de malware
- HIPS 3

ACTUALIZACIÓN 2

PROTECCIÓN DE LA RED

WEB Y CORREO ELECTRÓNICO 3

CONTROL DE DISPOSITIVOS 1

HERRAMIENTAS 2

INTERFAZ DEL USUARIO 1

BÁSICO

OPCIONES DEL MÓDULO DE ANÁLISIS

- Activar la detección de aplicaciones potencialmente indeseables ☒
- Activar la detección de aplicaciones potencialmente peligrosas ☐
- Activar la detección de aplicaciones sospechosas ☒

ANTI-STEALTH

- Activar la tecnología Anti-Stealth ☒

EXCLUSIONES DE PROCESOS

- Procesos que se excluirán del análisis [Editar](#)

EXCLUSIONES

- Archivos y carpetas que no se analizarán [Editar](#)

Predeterminado [Aceptar](#) Cancelar

Detección de 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](#)

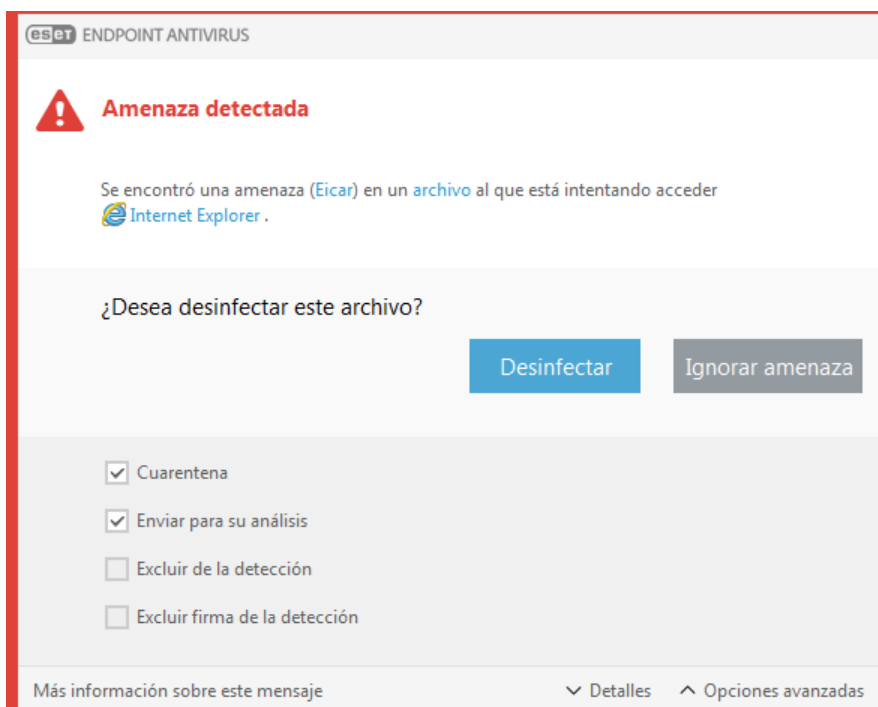
- [Análisis del ordenador a petición](#)

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 tipos de desinfección y el comportamiento, consulte la sección [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).

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.

Caché local compartida

La memoria caché local compartida puede aumentar el rendimiento en entornos aislados (por ejemplo, máquinas virtuales) mediante la eliminación del análisis duplicado en la red. Esto garantiza que cada archivo se analizará solo una vez y se almacenará en la memoria caché compartida.

ESET Shared Local Cache debe haberse instalado y configurado previamente.

- [Descargue ESET Shared Local Cache](#).
- Si desea más información, consulte [Manual de ESET Shared Local Cache](#).

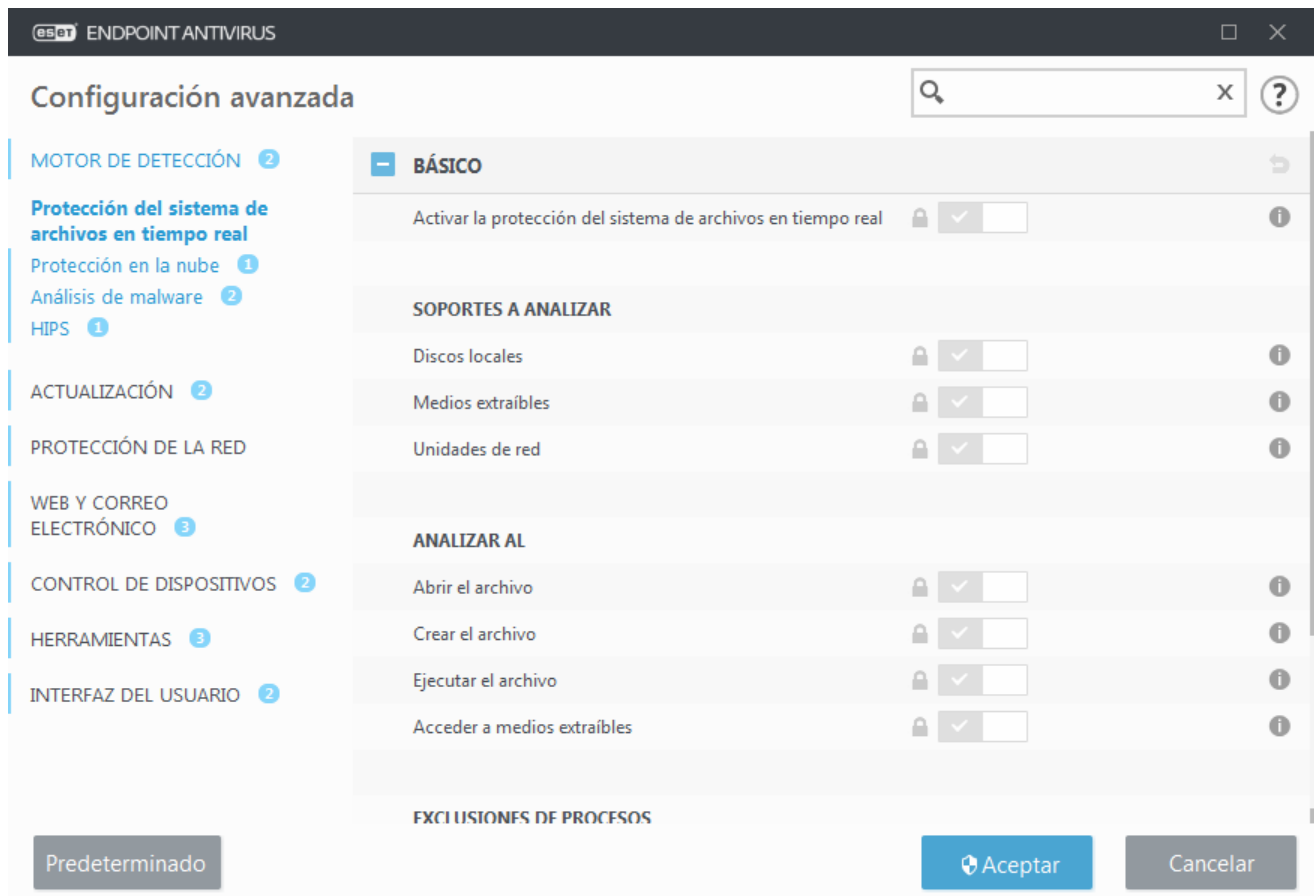
Encienda el interruptor **Activar caché** para guardar información sobre los análisis de archivos y carpetas de su red en ESET Shared Local Cache. Si realiza un nuevo análisis, ESET Endpoint Antivirus buscará los archivos analizados en ESET Shared Local Cache. Si los archivos coinciden, se excluirán del análisis.

La configuración de **Servidor de caché** contiene los campos siguientes:

- **Nombre de host:** nombre de host o dirección IP del ordenador en el que está ESET Shared Local Cache.
- **Puerto:** número de puerto usado para la comunicación (el mismo que se configuró en ESET Shared Local Cache).
- **Contraseña:** especifique la contraseña de ESET Shared Local Cache si es necesario.

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** en **Motor de detección > Protección del sistema de archivos en tiempo real > Básico**.

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, todos los archivos se analizan cuando se abren, crean o 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 los parámetros de ThreatSense.

Procesos que se excluirán del análisis: puede obtener más información sobre este tipo de exclusión en el capítulo [Exclusiones de procesos](#).

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 [Configuración de parámetros del motor 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, pulse **F5** para abrir Configuración avanzada y despliegue **Motor de detección > Protección del sistema de archivos en tiempo real**. Haga clic en **Parámetros de ThreatSense > Otros** y seleccione o anule la selección de **Activar optimización inteligente**.

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.

Modificación de la configuración de protección en tiempo real

La protección del sistema de archivos 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 que se ha instalado ESET Endpoint Antivirus, se optimiza 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 las diferentes fichas de la ventana (**Configuración avanzada > Motor de detección > Protección del sistema de archivos en tiempo real**).

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 desactivó la protección en tiempo real sin darse cuenta, será necesario reactivarla. Para volver a activar la protección en tiempo real, vaya a **Configuración** en la ventana principal del programa y haga clic en **Protección del sistema de archivos en tiempo real**.

Si no se activa al iniciar el sistema, probablemente se deba a que la opción **Iniciar automáticamente la protección del sistema de archivos en tiempo real** no está seleccionada. Si desea activar esta opción, diríjase a **Configuración avanzada (F5)** y haga clic en **Motor de detección > Protección del sistema de archivos en tiempo real > Básico**. Asegúrese de que la opción **Iniciar automáticamente la protección del sistema**

de archivos en tiempo real esté activada.

Si la protección en tiempo real no detecta ni desinfecta amenazas

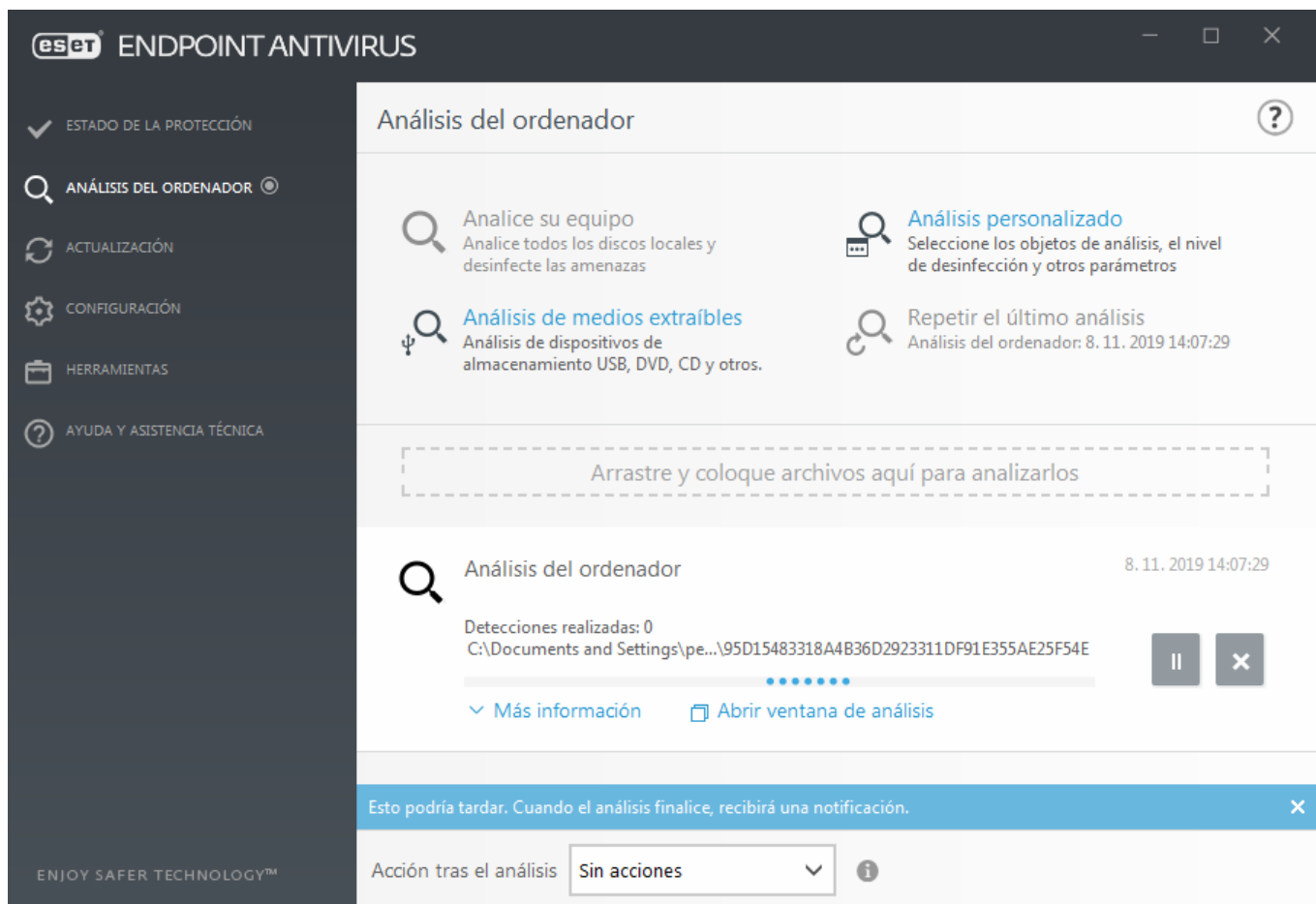
Asegúrese de que no tiene instalados otros programas antivirus en el ordenador. Si están activadas dos protecciones en tiempo real al mismo tiempo, estas pueden entrar en conflicto. Recomendamos que desinstale del sistema cualquier otro programa antivirus que haya en el sistema antes de instalar ESET.

La protección en tiempo real no se inicia

Si la protección en tiempo real no se activa al arrancar 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. Si desea ayuda para resolver este problema, póngase en contacto con el servicio de soporte técnico de ESET.

Análisis del ordenador

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

El análisis estándar 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 es su sencillo funcionamiento, sin configuraciones de análisis detalladas. El análisis estándar comprueba todos los archivos de los discos 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](#).

Análisis personalizado

El análisis personalizado es una solución óptima para especificar parámetros de análisis como, por ejemplo, objetos y métodos de análisis. La ventaja del análisis personalizado es su capacidad para 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.

Para seleccionar objetos de análisis, seleccione **Análisis del ordenador > Análisis personalizado** y elija una opción en el menú desplegable **Explorar objetivos**, o seleccione objetos específicos en la estructura de árbol. Los objetos de análisis también se pueden especificar introduciendo la ruta a la carpeta o los archivos que se desean incluir en el análisis. Si únicamente quiere analizar el sistema, sin realizar acciones de desinfección adicionales, seleccione **Analizar sin desinfectar**. Cuando vaya a realizar un análisis, haga clic en **Configuración.... > Parámetros de ThreatSense > Desinfección**.

Los análisis del ordenador en el modo personalizado son adecuados para usuarios avanzados que tienen experiencia previa con programas antivirus.

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.

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 **Explorar objetivos** y, a continuación, en **Exploración**.

Repetir el último análisis

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

Puede seleccionar **Sin acciones**, **Apagar** o **Reiniciar** en el menú desplegable **Acción tras el análisis**. 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 del mismo. La acción seleccionada se iniciará cuando finalicen todos los análisis que se están ejecutando. Cuando se seleccione **Apagar**, se mostrará un cuadro de diálogo de confirmación de apagado con una cuenta atrás de 30 segundos (haga clic en **Cancelar** para desactivar el apagado solicitado). Consulte [Opciones avanzadas de análisis](#) para obtener más información.



Nota

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 > Planificador de tareas**.
[¿Cómo programar un análisis semanal del ordenador?](#)

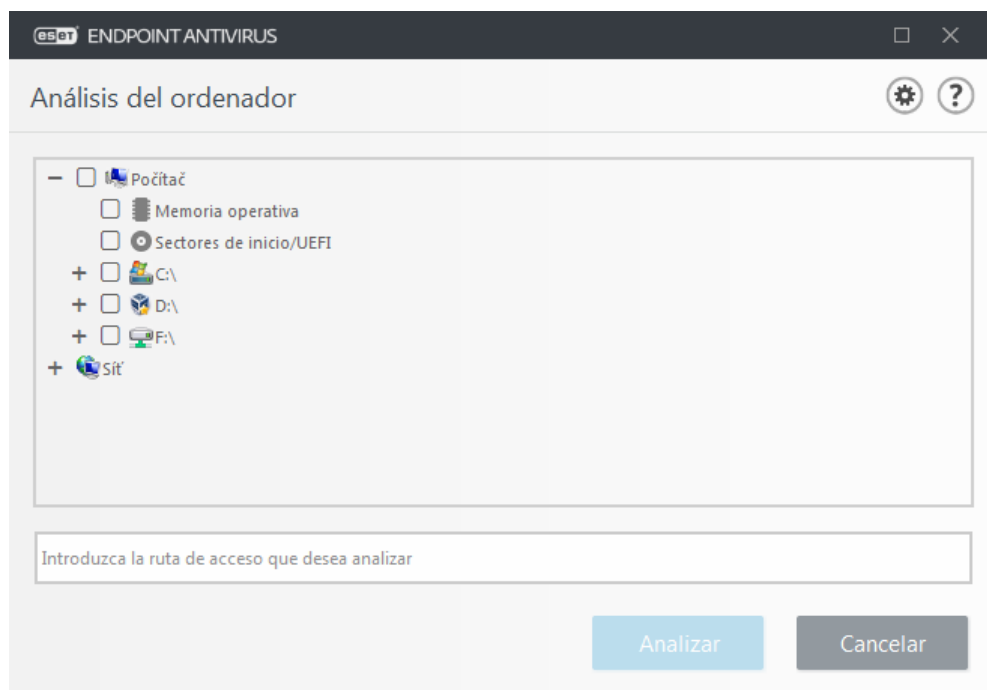
Iniciador del análisis personalizado

Si solo desea analizar un objeto determinado, puede usar la herramienta de análisis personalizado haciendo clic en **Análisis del ordenador > Análisis personalizado** y seleccionando una opción en el menú desplegable **Explorar objetivos** o seleccionando objetos específicos en la estructura de carpetas (árbol).

En la ventana de objetos de análisis puede definir los objetos (memoria, unidades, sectores, archivos y carpetas) que se deben analizar para buscar amenazas. Seleccione los objetos en la estructura de árbol, que incluye todos los dispositivos disponibles en el ordenador. En el menú desplegable **Objetos de análisis**, puede seleccionar objetos predefinidos para el análisis.

- **Por configuración de perfil:** selecciona los objetos definidos en 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:** permite al usuario crear una selección personalizada de destinos.

Para acceder rápidamente a un objeto de análisis o agregar directamente carpetas o archivos, introdúzcalos en el campo en blanco disponible debajo de la lista de carpetas. Esto solo es posible si no se ha seleccionado ningún objeto en la estructura de árbol y el menú **Objetos de análisis** está definido en **Sin selección**.



Los elementos infectados no se desinfectan automáticamente. El análisis sin desinfección sirve para obtener una vista general del estado de protección actual. Además, puede seleccionar uno de los tres niveles de desinfección haciendo clic en **Configuración avanzada > Motor de detección > Análisis a petición > Parámetros de ThreatSense > Desinfección**. Si únicamente quiere analizar el sistema, sin realizar acciones de desinfección adicionales, seleccione **Analizar sin desinfectar**. El historial de análisis se guarda en el registro de análisis.

Cuando se selecciona **Ignorar exclusiones**, se analizan sin excepciones los archivos con extensiones excluidas

anteriormente del análisis.

Puede elegir un perfil en el menú desplegable **Perfil de análisis** que se utilizará para analizar los objetos seleccionados. El perfil predeterminado es **Análisis estándar**. Hay otros dos perfiles de análisis predefinidos llamados **Análisis en profundidad** y **Análisis del menú contextual**. 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 > Parámetros de ThreatSense**.

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. Haga clic en esta opción si el usuario actual no tiene privilegios para acceder a los archivos que se deben analizar. Observe que este botón no está disponible si el usuario actual no puede realizar operaciones de UAC como administrador.



Nota

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.

Análisis del ordenador

8/15/2018 8:19:34 PM

Subprocesos encontrados: 0
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\35c44c5316c1ee4e60a36072a1ee3a30\System.Xml.ni.d

Menos información

Usuario: John-PC\John
Objetos analizados: 20508
Duración: 0:00:30

C:\Users\All Users\Microsoft\Crypto\RSA\5d84a4742f6f35_a110f29a-833e-446a-bfdb-195863caba6e	- no se pudo abrir [4]
C:\Users\All Users\Microsoft\Crypto\RSA\5d84a4742f6f35_a110f29a-833e-446a-bfdb-195863caba6e	- no se pudo abrir [4]
C:\Users\All Users\Microsoft\Crypto\RSA\MachineKeys\c3a84c6dd0bf0eb5da5d84a4742f6f35_a110f29a-833e-446a-bfdb-195863caba6e	- no se pudo abrir [4]
C:\Users\All Users\Microsoft\Crypto\RSA\MachineKeys\dc558a410ecc71a25c9884a937c89d6e_a110f29a-833e-446a-bfdb-195863caba6e	- no se pudo abrir [4]
C:\Users\All Users\Microsoft\Crypto\RSA\MachineKeys\ee0066ce8768d9c2afe613dcf61232c8_a110f29a-833e-446a-bfdb-195863caba6e	- no se pudo abrir [4]
C:\Users\All Users\Microsoft\Crypto\RSA\MachineKeys\ef73ed1b2f5151d2486cbcc4721be893_a110f29a-833e-446a-bfdb-195863caba6e	- no se pudo abrir [4]
C:\Users\All Users\Microsoft\Crypto\RSA\MachineKeys\f080183c2cf12a3df6bc1a8a14723fdb_a110f29a-833e-446a-bfdb-195863caba6e	- no se pudo abrir [4]
C:\Users\All Users\Microsoft\Diagnosis\DownloadedSettings\telemetry.ASM-WindowsDefault.json	- no se pudo abrir [4]
C:\Users\All Users\Microsoft\Diagnosis\DownloadedSettings\utc.app.json	- no se pudo abrir [4]
C:\Users\All Users\Microsoft\Diagnosis\events00.rbs	- no se pudo abrir [4]
C:\Users\All Users\Microsoft\Diagnosis\events01.rbs	- no se pudo abrir [4]
C:\Users\All Users\Microsoft\Diagnosis\events10.rbs	- no se pudo abrir [4]
C:\Users\All Users\Microsoft\Diagnosis\events11.rbs	- no se pudo abrir [4]

☒ Desplazar el registro de análisis

Cerrar



Nota

Es normal que algunos archivos, como los archivos protegidos con contraseña o que solo utiliza el sistema (por lo general, archivos *pagefile.sys* y determinados archivos de registro), no se puedan analizar.

Progreso del análisis: la barra de progreso muestra el estado de objetos ya analizados en comparación con el porcentaje de objetos pendientes. El estado de progreso del análisis se calcula a partir del número total de objetos

incluidos en el análisis.

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

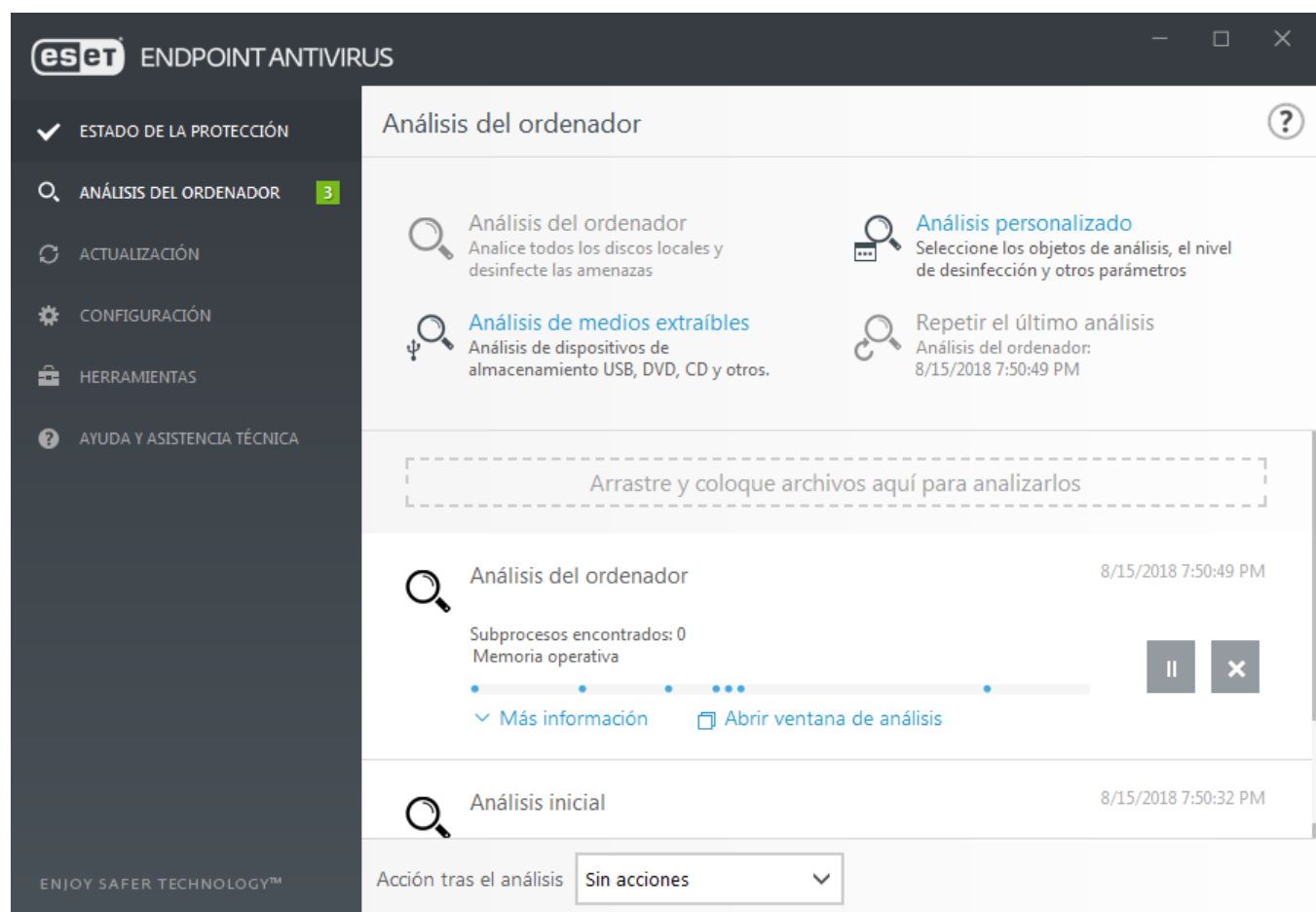
Amenazas detectadas: muestra el número total de amenazas detectadas durante un análisis.

Pausa: pone el análisis en pausa.

Reanudar: esta opción está visible cuando el progreso del análisis está en pausa. Haga clic en **Continuar** para proseguir con el análisis.

Detener: termina 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.



Registro de análisis del ordenador

El [registro de análisis del ordenador](#) contiene información general sobre el análisis, como la siguiente:

- Fecha y hora del análisis
- Discos, carpetas y archivos analizados
- Número de objetos analizados
- Número de amenazas detectadas
- Hora de finalización
- Tiempo total de análisis

Análisis de malware

Puede acceder a la sección **Análisis de malware** en el menú Configuración avanzada. Pulse la tecla **F5**, haga clic en **Motor de detección > Análisis de malware** y verá las opciones para seleccionar los parámetros de análisis. Esta sección incluye las siguientes opciones:

- **Perfil seleccionado:** un conjunto específico de parámetros usados por el análisis a petición. Para crear un nuevo perfil, haga clic en **Editar** junto a **Lista de perfiles**. Consulte [Perfiles de análisis](#) si desea más información.
- **Protección a petición y de aprendizaje automático:** consulte [Motor de detección \(7.2 y posteriores\)](#).
- **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 el menú desplegable o seleccionar objetos específicos en la estructura de carpetas (árbol). Consulte [Objetos de análisis](#) si desea más información.
- **Parámetros de ThreatSense:** en esta sección, es posible encontrar opciones de configuración avanzada como, por ejemplo, las extensiones de archivo que desea analizar, los métodos de detección utilizados, etc. Haga clic para abrir una ficha con opciones de análisis avanzado.

Análisis en estado inactivo

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

Análisis en estado inactivo

Coloque el conmutador situado junto a Activar el análisis de estado inactivo en la posición **Activado** para activar esta característica. Cuando el ordenador se encuentra en estado inactivo, se lleva a cabo un análisis silencioso de todos los discos locales del ordenador.

De forma predeterminada, el análisis de estado inactivo no se ejecutará si el ordenador (portátil) está funcionando con batería. Puede anular este parámetro activando el conmutador situado junto a **Ejecutar aunque el ordenador esté funcionando con la batería** en Configuración avanzada.

Active **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 **Registrar**).

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.

Haga clic en [Configuración de parámetros del motor ThreatSense](#) para modificar los parámetros de análisis (por ejemplo, métodos de detección) del análisis de estado inactivo.

Perfiles de análisis

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 la ventana Configuración avanzada (F5) y haga clic en **Motor de detección > Análisis de malware > Análisis a petición > Lista de perfiles**. 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 [Configuración de parámetros del motor ThreatSense](#) para ver una descripción de los diferentes parámetros de la configuración del análisis.



Nota

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 **Desinfección estricta**. 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 la ventana de objetos de análisis puede definir los objetos (memoria, unidades, sectores, archivos y carpetas) que se deben analizar para buscar amenazas. Seleccione los objetos en la estructura de árbol, que incluye todos los dispositivos disponibles en el ordenador. En el menú desplegable **Objetos de análisis**, puede seleccionar objetos predefinidos para el análisis.

- **Por configuración de perfil:** selecciona los objetos definidos en 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:** permite al usuario crear una selección personalizada de destinos.

Opciones avanzadas de análisis

En esta ventana, puede especificar opciones avanzadas para una tarea de análisis programada del ordenador. En el menú desplegable puede establecer la acción que desea efectuar automáticamente cuando concluya el análisis:

- **Apagar:** el ordenador se apaga cuando finaliza el análisis.
- **Reiniciar:** cierra todos los programas abiertos 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.
- **Sin acciones:** cuando el análisis concluya no se realizará ninguna acción.



Nota

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 usuario no puede cancelar la acción** para privar a los usuarios sin privilegios de la capacidad de detener 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 el capítulo [Progreso del análisis](#).

Control del dispositivo

ESET Endpoint Antivirus permite controlar los dispositivos automáticamente (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
- Impresora USB
- Almacenamiento FireWire
- Dispositivo Bluetooth
- Lector de tarjetas inteligentes
- Dispositivo de imagen
- Módem
- Puerto LPT/COM
- Dispositivo portátil
- Todos los tipos de dispositivos

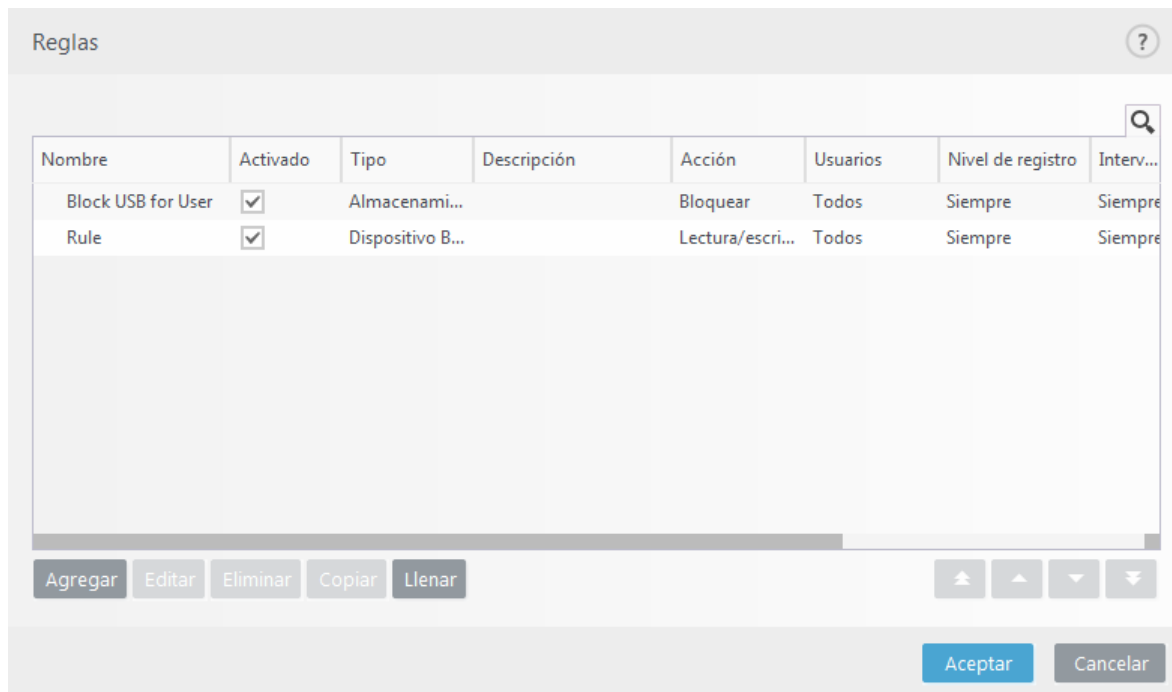
Las opciones de configuración del control del dispositivo se pueden modificar en **Configuración avanzada** (F5) > **Control del dispositivo**.

Al activar el conmutador situado junto a **Integrar en el sistema** se activa la característica de Control del dispositivo en ESET Endpoint Antivirus; deberá reiniciar el ordenador para que se aplique este cambio. Una vez que Control del dispositivo esté activado, se activarán las **Reglas**, lo que le permitirá abrir la ventana [Editor de reglas](#).

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 para dispositivos externos que los usuarios conectan al ordenador y permite controlarlos de forma precisa.





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).

Si selecciona un dispositivo (en la lista de dispositivos detectados) y hace clic en **Aceptar**, se abre una ventana del editor de reglas con información predefinida (es posible ajustar toda la configuración).

Grupos de dispositivos



Advertencia

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 el grupo que contiene la lista de dispositivos que quiere ver 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 un dispositivo de la lista para agregarlo al grupo haciendo clic en **Aceptar**.

Elementos de control

Agregar: puede agregar un grupo escribiendo su nombre o un dispositivo a un grupo existente (también puede especificar, si lo desea, datos como el nombre del proveedor, el modelo y el número de serie), 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.

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).

Cuando haya finalizado la personalización, haga clic en **Aceptar**. Haga clic en **Cancelar** si desea cerrar la ventana **Grupos de dispositivos** sin guardar los cambios.



Ejemplo
puede crear varios grupos de dispositivos a los que se aplicarán reglas distintas. También puede crear solo un grupo de dispositivos al que se aplicará la regla con la acción **Lectura/Escritura** o **Solo lectura**. Esto garantiza el bloqueo de dispositivos no reconocidos por el control de dispositivos pero conectados al ordenador.

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, **Solo lectura** no está disponible para Bluetooth, lo que significa que los dispositivos Bluetooth solo se pueden permitir, bloquear o emitir una advertencia sobre ellos).

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.

Editar regla

?

Nombre

Rule

Regla activada

☒

Aplicar durante

Siempre

▼

Tipo de dispositivo

Dispositivo Bluetooth

▼

Acción

Lectura/escritura

▼

Tipo de criterios

Dispositivo

▼

Proveedor

Modelo

Número de serie

Nivel de registro

Siempre

▼

Lista de usuarios

Editar

Aceptar

Introduzca una descripción de la regla en el campo **Nombre** para mejorar la identificación. Haga clic en el conmutador situado junto a **Regla activada** para activar o desactivar esta regla, lo cual puede ser de utilidad cuando no se quiere eliminar una regla de forma permanente.

Aplicar durante: le permite aplicar la regla creada durante determinado tiempo. En el menú desplegable, seleccione el intervalo de tiempo creado. Si desea obtener más información, haga clic [aquí](#).

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.



Nota

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:

- **Lectura/Escritura:** se permitirá el acceso completo al dispositivo.
- **Bloquear:** se bloqueará el acceso al dispositivo.
- **Solo lectura:** 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, **Solo lectura** 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 y adaptarlas a dispositivos. Todos los parámetros distinguen entre mayúsculas y minúsculas:

- **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.



Nota

si estos parámetros están sin definir, la regla ignorará estos cambios a la hora de establecer la coincidencia. Los parámetros de filtrado de todos los campos de texto no distinguen entre mayúsculas y minúsculas, y no admiten caracteres comodín (*, ?).



Nota

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.



Nota

no todos los dispositivos se pueden filtrar mediante reglas de usuario (por ejemplo, los dispositivos de imagen no proporcionan información sobre los usuarios, sino únicamente sobre las acciones).

Sistema de prevención de intrusiones del host (HIPS)

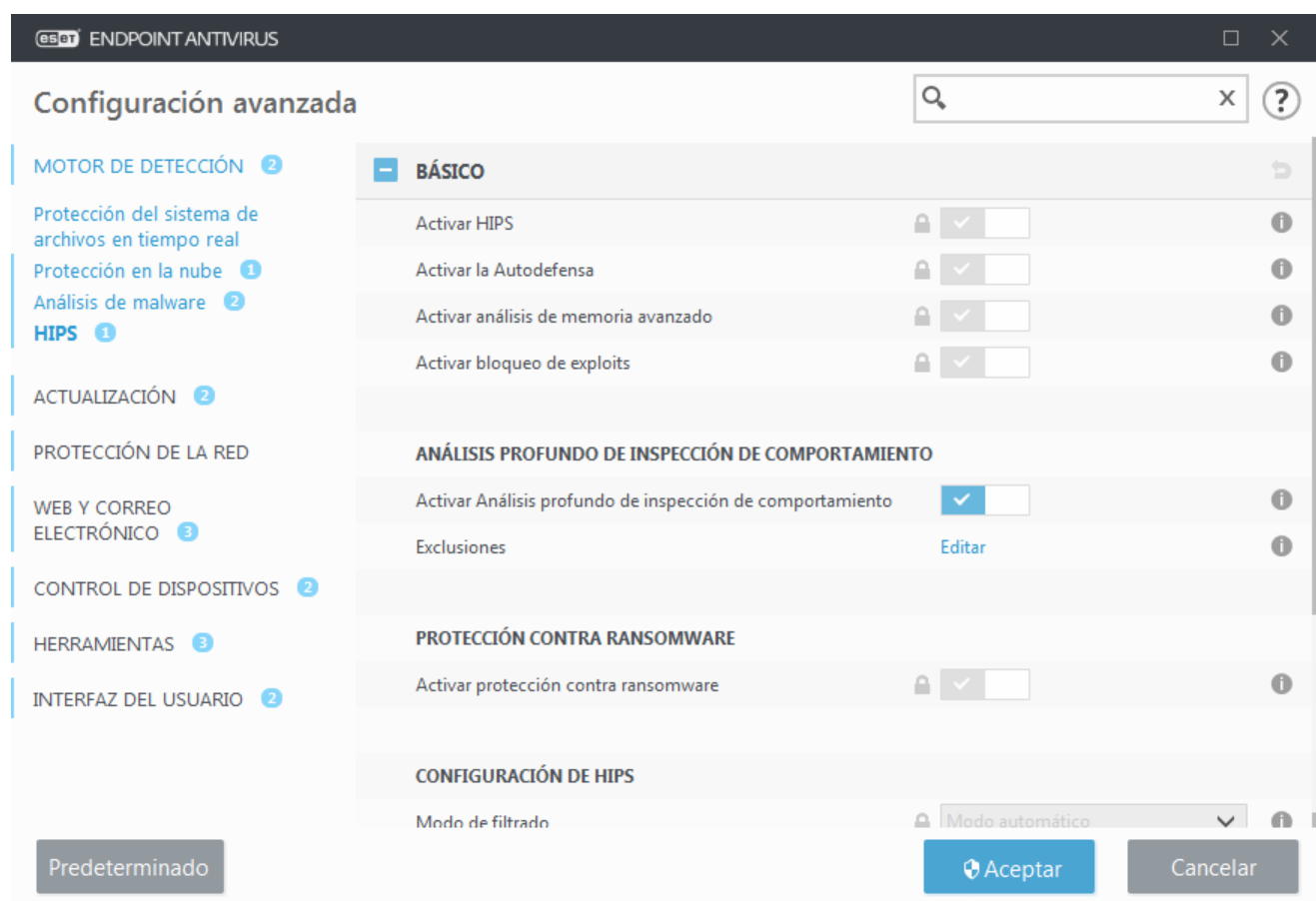


Advertencia

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.

Los ajustes de HIPS están en **Configuración avanzada (F5) > Motor de detección > HIPS > Básico**. El estado de HIPS (activado/desactivado) se muestra en la ventana principal del programa de ESET Endpoint Antivirus, en **Configuración > Ordenador**.



Básico

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 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 ESMC o en el editor de configuración de políticas de ESET PROTECT Cloud.

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 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 de 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](#).

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.

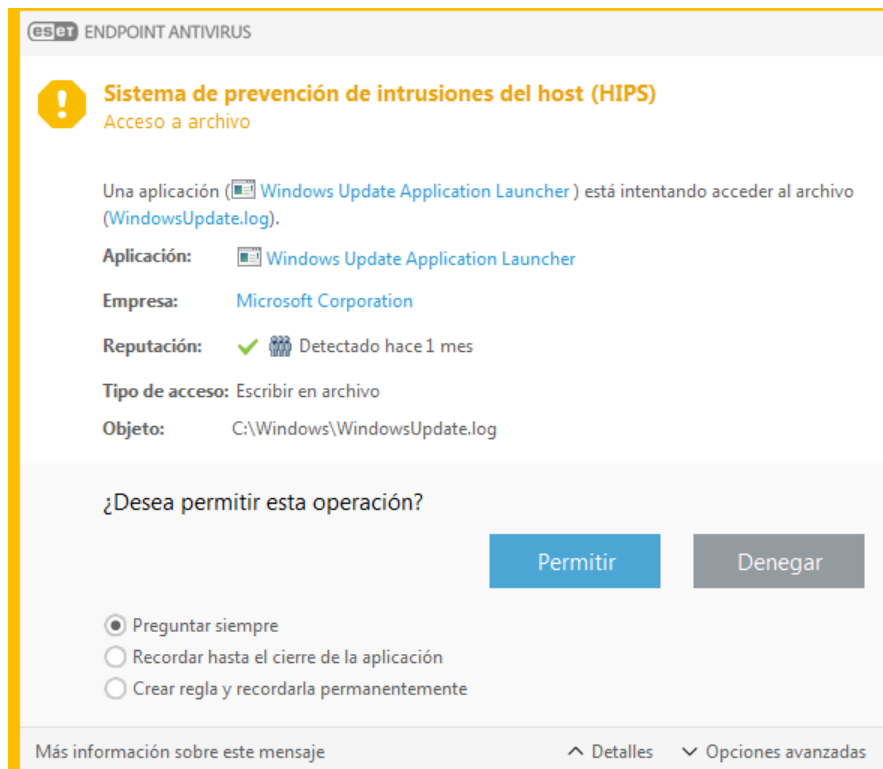
Para acceder a los ajustes de los parámetros más detallados de la regla, haga clic en **Opciones avanzadas**. Las siguientes opciones están disponibles si selecciona **Crear regla y recordar permanentemente**:

- **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.



¿Infinitas notificaciones de HIPS?

Para que dejen de aparecer las notificaciones, cambie el modo de filtrado a **Modo automático** en **Configuración avanzada (F5) > 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 entre **Bloquear** y **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**.



Importante

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: 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 pequeña notificación emergente 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 de 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 este conmutador si desea conservar la regla en la lista pero no aplicarla.

Registro: si activa esta opción, la información acerca de esta regla se anotará en el [registro de HIPS](#).

Advertir al usuario: cuando se activa un suceso, se abre una ventana emergente pequeña 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: 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 todos 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.



Nota

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.

Descripción de las operaciones importantes:

Operaciones del archivo

- **Eliminar archivo:** la aplicación solicita permiso para eliminar el archivo objetivo.
- **Escribir en archivo:** la aplicación solicita permiso para escribir en el archivo objetivo.
- **Acceso directo al disco:** la aplicación está intentando realizar una operación de lectura o escritura en el disco de una forma no convencional que burlará los procedimientos habituales de Windows. Esto puede provocar la modificación de archivos sin la aplicación de las reglas correspondientes. Esta operación puede estar provocada por un código malicioso que intente evadir el sistema de detección, un software de copia de seguridad que intente realizar una copia exacta de un disco o un gestor de particiones que intente reorganizar los volúmenes del disco.
- **Instalar enlace global:** hace referencia a la invocación de la función SetWindowsHookEx desde la biblioteca MSDN.
- **Cargar controlador:** instalación y carga de controladores en el sistema.

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.



Nota

no es posible interceptar operaciones de procesos en Windows XP de 64 bits.

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.



Nota

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.



Advertencia

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.

Configuración de regla de HIPS

Nombre de la regla

Sin título

Acción

Permitir

Operaciones afectadas

Archivos

Aplicaciones

Entradas del registro

Activado

☒

Nivel de registro

Ninguno

Notificar al usuario

☐

Atrás

Siguiente

Cancelar

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: todas las operaciones bloqueadas se anotarán en el registro de HIPS.

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.



Nota

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.

Modo de presentación

El modo de presentación es una característica para usuarios que exigen un uso del software sin interrupciones y sin ventanas emergentes, 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. Cuando está activado, se desactivan todas las ventanas emergentes y las tareas programadas no se ejecutan. La protección del sistema sigue ejecutándose en segundo plano, pero no requiere la intervención del usuario.

Haga clic en **Configuración > Ordenador** y, a continuación, haga clic en el conmutador situado junto a **Modo de presentación para activarlo de forma manual**. En **Configuración avanzada** (F5), haga clic en **Herramientas > Modo de presentación** y, a continuación, haga clic en el conmutador situado junto a **Activar el modo de presentación automáticamente, al ejecutar aplicaciones en modo de pantalla completa para que ESET Endpoint Antivirus active este modo automáticamente cuando se ejecuten aplicaciones a pantalla completa**. 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 **El modo de presentación está activado** en naranja.

Si selecciona **Activar el modo de presentación automáticamente, al ejecutar aplicaciones en modo de pantalla completa**, el modo de presentación se activará cuando inicie una aplicación a pantalla completa y se detendrá automáticamente cuando cierre dicha aplicación. Esta función es muy útil para que el modo de presentación se inicie de inmediato al empezar un juego, abrir una aplicación a pantalla completa o iniciar una presentación.

También puede seleccionar **Desactivar el modo de presentación automáticamente después de** para definir la cantidad de tiempo, en minutos, que tardará en desactivar el modo de presentación automáticamente.

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 de los módulos. Este análisis depende de las [tareas y la configuración del Planificador de tareas](#).

Las opciones de análisis en el inicio forman parte de la tarea **Verificación de archivos de inicio del sistema** del Planificador de tareas. Para modificar la configuración del análisis en el inicio, seleccione **Herramientas > Planificador de tareas**, haga clic en **Verificación automática de los archivos de inicio** y en **Modificar**. En el último paso, aparece la ventana [Verificación de la ejecución de archivos en el inicio](#) (consulte el siguiente capítulo para obtener más detalles).

Para obtener instrucciones detalladas acerca de la creación y gestión de tareas del Planificador de tareas, consulte [Creación de tareas nuevas](#).

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 secreto. 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.

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.

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 la protección de documentos, abra la ventana **Configuración avanzada** (pulsando F5) > **Motor de detección** > **Análisis de malware** > **Protección de documentos** y haga clic en el conmutador **Integrar en el sistema**.



Nota

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).

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.

Las [exclusiones de rendimiento](#) le permiten excluir del análisis archivos y carpetas. 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.

Las [exclusiones de la versión 7.1 y anteriores](#) combinan Exclusiones de rendimiento y Exclusiones de detección en un solo elemento.

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 (F5) > 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.



NOTA

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":"7.2.2055","path":"plugins.01000600.settings.PerformanceExclusions","columns":["Path","Description"]}
C:\Backup\*,custom comment
C:\pagefile.sys,
```

Agregar o modificar la exclusión de rendimiento

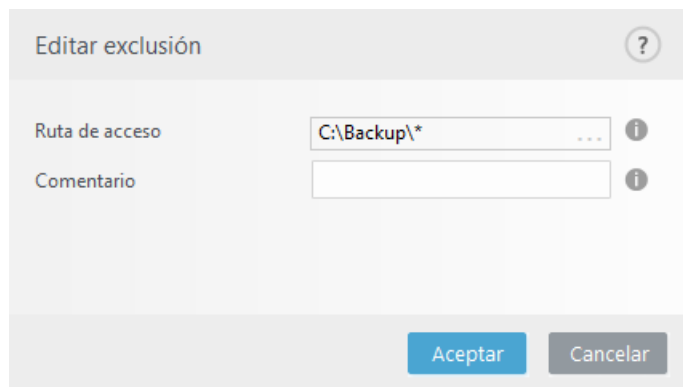
Este cuadro de diálogo excluye una ruta de acceso (archivo o directorio) específica de este ordenador.



Elegir ruta de acceso o introducirla manualmente

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.



Formato de exclusión

- Si desea excluir todos los archivos 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 los caracteres que faltan o que no se conocen).



Variables del sistema en exclusiones

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 rutas de acceso con un asterisco

Algunos ejemplos de exclusión más con el uso de asteriscos:

`C:\Tools*`: la ruta de acceso debe terminar con la barra invertida y el asterisco para indicar que es una carpeta y que se excluyen todas sus subcarpetas.

`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.

Excepción para exclusiones de rendimiento:

`C:\Tools*.*`: mismo comportamiento que `C:\Tools*` (no confundir con que la máscara `*.*` excluirá solo archivos con extensiones en la carpeta `Tools`).

Ejemplo de exclusión incorrecta introducida manualmente:

`C:\Tools`: no se excluirá la carpeta `Tools`. Desde la perspectiva del análisis, `Tools` también puede ser un nombre de archivo.

`C:\Tools\`: no olvide agregar el asterisco al final de la ruta de acceso: `C:\Tools*`



Comodines en el medio de una ruta de acceso

Le recomendamos encarecidamente no usar comodines en el medio de una ruta de acceso (por ejemplo, `C:\Tools*Data\file.dat`) a menos que la infraestructura de su sistema lo requiera. Consulte el [artículo de la Base de conocimiento](#) que se indica a continuación si desea 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 de 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.



Formato de exclusión

- Si desea excluir todos los archivos 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 los caracteres que faltan o que no se conocen).



Variables del sistema en exclusiones

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.



Cómo funcionan las exclusiones de detección

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.

Exclusiones de detección

?

Criterios de objeto

Excluir detección

Comentario

C:\Recovery*.*

Win32/Adware.Optmedia

2723cb8ca015209528d3fbdcaa801124f40ad4

Cualquier detección

SuperApi.exe

Agregar

Editar

Eliminar

Importar

Exportar

Aceptar

Cancelar

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, **Configuración avanzada (F5) > 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**.

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 hay un nombre de una [detección](#) junto a un archivo excluido, significa que el archivo solo se excluye de esa detección, no completamente. Si ese archivo se infecta más tarde con otro malware, se detectará. Este tipo de exclusión solo se puede usar con determinados tipos de infiltraciones y puede crearse en la ventana de alerta que informa de la infiltración (haga clic en **Mostrar opciones avanzadas** y, a continuación, seleccione **Excluir de la detección**) o 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.
- **Hash:** excluye un archivo según el hash especificado (SHA1), 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](#)

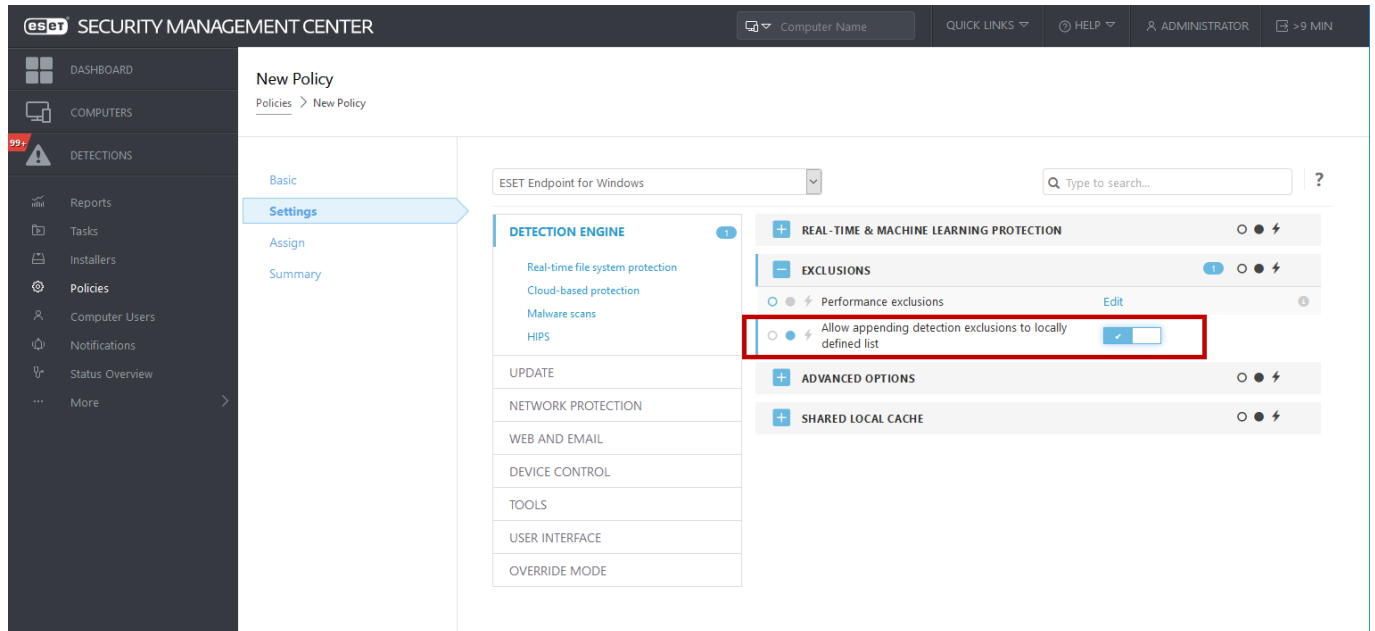
```
# {"product": "endpoint", "version": "7.2.2055", "path": "Settings.ExclusionsManagement.DetectionExclusions", "columns": [{"id", "Path", "ThreatName", "Description", "FileHash"}]}
4c59cd02-357c-4b20-a0ac-ca8400000001,,,SuperApi.exe,00117F70C86ADB0F979021391A8AEAA497C2C8DF
2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,,
```

Configuración de exclusiones de detección en ESMC

ESMC 7.1 incluye un [nuevo asistente para administrar las exclusiones de detección](#): cree una exclusión de detección y aplíquela a más ordenadores/grupos.

Posible anulación de exclusiones de detección desde ESMC

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 ESMC funcionará como se espera.



Agregar o editar una exclusión de detección

Excluir detección

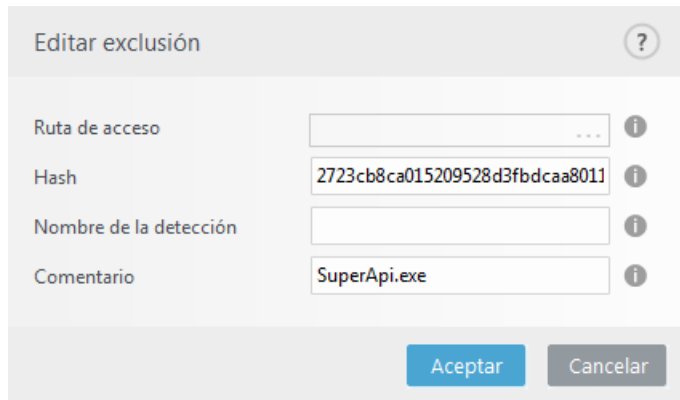
Se debe facilitar un nombre de detección de ESET válido. Para obtener un nombre de detección válido, consulte [Archivos de registro](#) y, a continuación, seleccione **Detecciones** en el menú desplegable Archivos de registro. Esta opción resulta útil cuando se está detectando un [falso positivo](#) 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 (SHA1), sea cual sea el tipo de archivo, la ubicación, el nombre o su extensión.



Exclusiones por nombre de la detección

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**.

Exclusiones (7.1 y anteriores)

Las exclusiones de la versión 7.1 y anteriores combinan [Exclusiones de rendimiento](#) y [Exclusiones de detección](#) en un solo elemento.

Exclusiones

Tipo	Detalles
Ruta de acceso: Descripción:	C:\Backup*.*
Ruta de acceso: Descripción:	C:\pagefile.sys
Amenaza: Ruta de acceso: Descripción:	@NAME=Win32/Adware.Optmedia C:\Recovery*.*
Hash: Descripción:	678C1422DE867141B947EA700E8A2D6114AFAE97 SuperApi.exe

Agregar

Editar

Eliminar

Guardar

Cancelar

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. Se pueden producir problemas similares cuando intentamos realizar migraciones de máquinas virtuales en tiempo real. 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.

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 (F5) > Motor de detección > 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.



Ejemplo

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.



Importante

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.



Nota

[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).



Ejemplo

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 introduzca 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.



Importante

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.

Exclusiones del HIPS

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

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.

Parámetros de 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

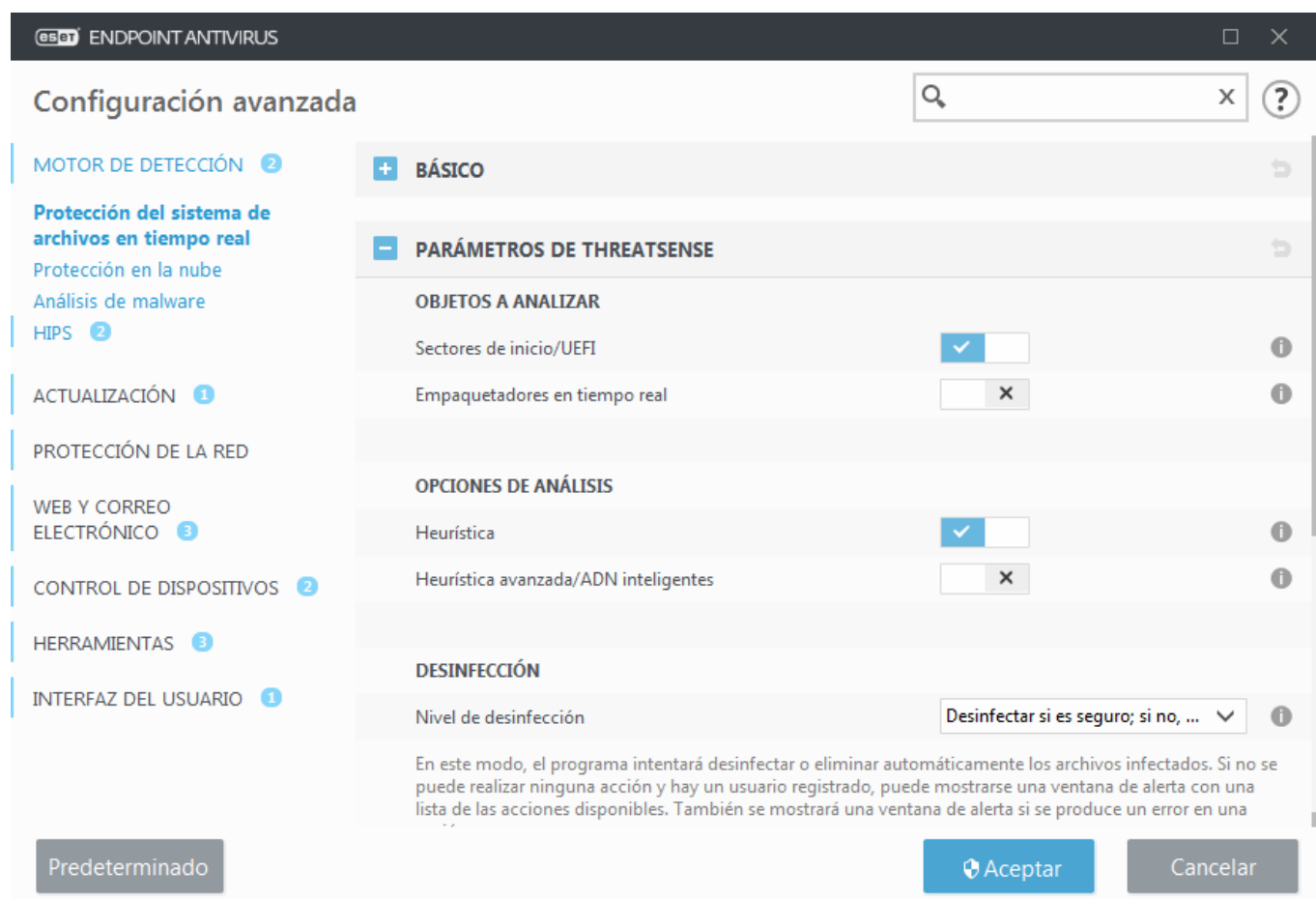
forma conjunta para mejorar en gran medida la seguridad del sistema. El motor de análisis es capaz de controlar varios flujos de datos de forma simultánea, de manera que maximiza la eficacia y la velocidad de detección. Además, la tecnología ThreatSense elimina eficazmente los programas peligrosos (rootkits).

Las opciones de configuración del motor ThreatSense permiten al usuario especificar distintos 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 **Parámetros de 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 en estado inactivo
- Análisis en el inicio
- Protección de documentos
- Protección de clientes de correo electrónico
- Protección del acceso a la Web
- 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 electrónico: el programa es compatible con las 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 de tiempo de ejecución: después de su ejecución, los empaquetadores de 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/Firmas de ADN: 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 que define el tipo y el contenido del archivo. En esta sección de la configuración de parámetros de ThreatSense, es posible definir los tipos de archivos que se desean analizar.

Otros

Al configurar parámetros del 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 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 (seg.): define el tiempo máximo asignado para analizar un objeto. Si se especifica un valor definido por el usuario, el módulo antivirus detendrá el análisis de un objeto cuando se haya agotado el tiempo, independientemente de si el análisis ha finalizado o no. 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. Valor predeterminado: ilimitado.



Nota

No se recomienda cambiar los valores predeterminados; en circunstancias normales, no debería haber motivo para hacerlo.

Niveles de desinfección

Para acceder a la configuración del nivel de desinfección de un módulo de protección deseado, despliegue **Parámetros de ThreatSense** (por ejemplo, **Protección del sistema de archivos en tiempo real**) y, a continuación, haga clic en **Desinfección**.

La protección en tiempo real y otros módulos de protección presentan los siguientes niveles de corrección (es decir, desinfección).

Corrección en ESET Endpoint Antivirus 7.2 y posteriores

Nivel de desinfección	Descripción
-----------------------	-------------

Corregir siempre las detecciones

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](#).

Corregir la detección si es seguro; de lo contrario, conservar

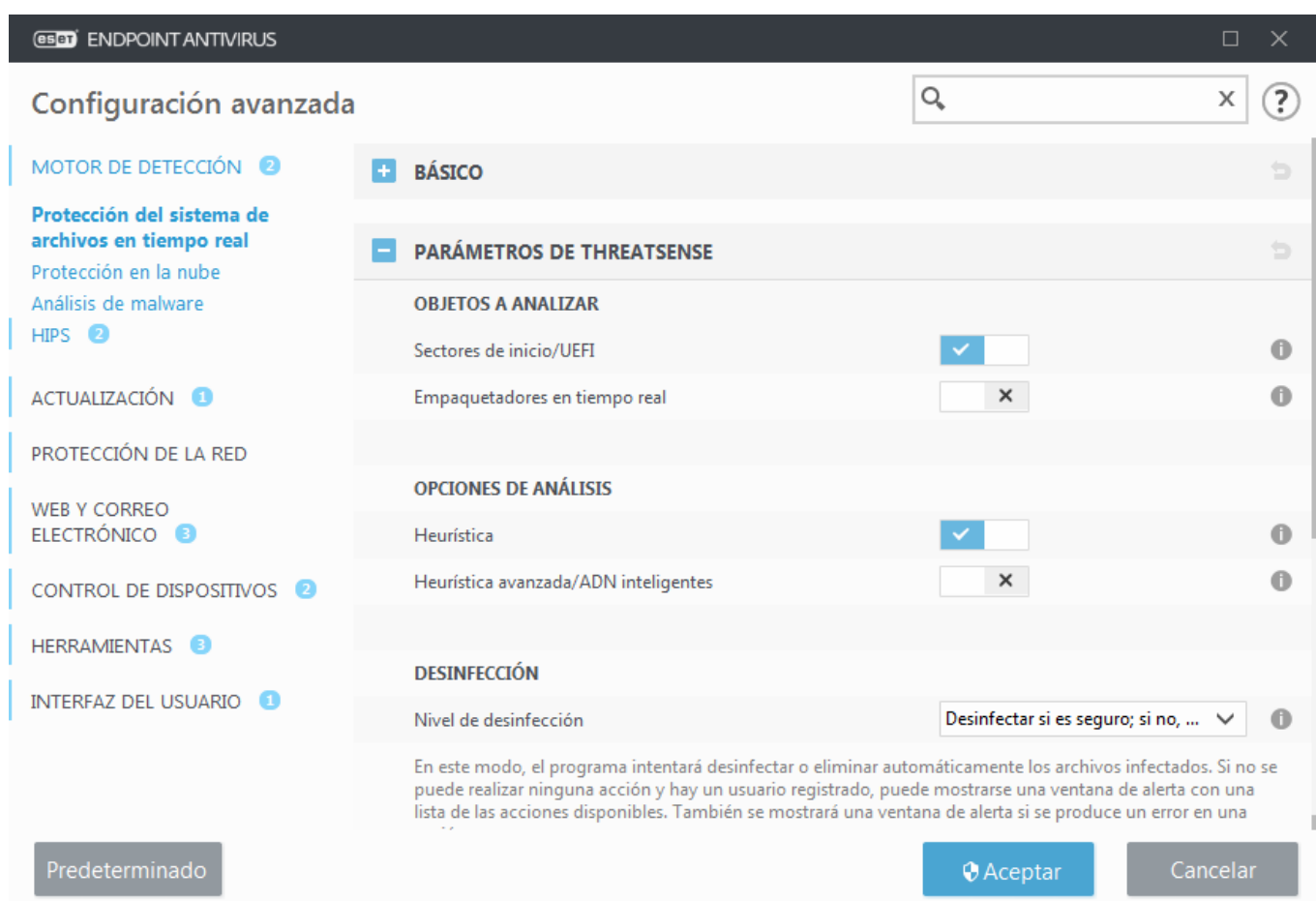
Intentar corregir la detección durante la desinfección de [objetos](#) sin la intervención del usuario final. En algunos casos (por ejemplo, archivos del sistema o archivos comprimidos con archivos limpios e infectados), si la detección no se puede corregir, el objeto del que se informa se deja en su ubicación original.

Corregir la detección si es seguro; de lo contrario, preguntar

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.



Niveles de desinfección en ESET Endpoint Antivirus 7.1 y anteriores

Nivel de desinfección	Descripción
-----------------------	-------------

Sin desinfección	Las detecciones no se desinfectan automáticamente. El programa muestra una ventana de advertencia y permite al usuario elegir una acción. Este nivel está diseñado para usuarios más avanzados que saben los pasos que hay que dar en caso de detección.
Desinfección normal	El programa intenta desinfectar o eliminar automáticamente las detecciones de acuerdo con una acción predefinida (en función del tipo de infiltración). La detección y la eliminación de un objeto las señala una notificación en la esquina inferior derecha de la pantalla. Si no es posible seleccionar la acción correcta automáticamente, el programa ofrece otras acciones de seguimiento. Lo mismo sucede cuando no se puede completar una acción predefinida.
Desinfección estricta	El programa desinfecta o elimina todas las detecciones. Las únicas excepciones son los archivos del sistema. Si no es posible desinfectarlos, se solicita al usuario que seleccione una acción en una ventana de advertencia.

El nivel de desinfección mencionado se aplica al configurar una política de ESMC para versiones anteriores de ESET Endpoint Antivirus:

Nivel de desinfección en la política de ESMC	Nivel de desinfección aplicado
Corregir siempre las detecciones	Desinfección estricta
Corregir la detección si es seguro; de lo contrario, conservar	Desinfección normal
Corregir la detección si es seguro; de lo contrario, preguntar*	Desinfección normal
Preguntar siempre al usuario final	Sin desinfección

* Valor predeterminado al actualizar a la versión 7.2 y posteriores con la opción **Desinfección normal** establecida en ESET Endpoint Antivirus.

Extensiones de archivo excluidas del análisis

Una extensión es una parte del nombre de archivo delimitada por un punto que define el tipo y el contenido del archivo. En esta sección de la configuración de parámetros de ThreatSense, es posible definir los tipos de archivos que se desean analizar.



Nota

No deben confundirse con otros tipos de [Exclusiones](#).

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.



Ejemplo

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).



Nota

Para ver la extensión concreta (en caso de tener alguna) de un archivo en un sistema operativo Windows, tiene que desmarcar la opción **Ocultar extensiones de tipos de archivo conocidos** en **Panel de control > Opciones de carpeta > Ver** (ficha) y aplicar este cambio.

Parámetros adicionales de ThreatSense

Parámetros adicionales de ThreatSense para archivos nuevos o modificados: la probabilidad de infección en archivos modificados o recién creados es superior que en los archivos existentes, por eso el programa


comprueba estos archivos con parámetros de análisis adicionales. Además de los métodos de análisis basados en firmas habituales, se utiliza la heurística avanzada, que detecta amenazas nuevas antes de que se publique la actualización del motor de detección. El análisis se realiza también en archivos de autoextracción (.sfx) y empaquetadores en tiempo real (archivos ejecutables comprimidos internamente), no solo en los archivos nuevos. Los archivos se analizan, de forma predeterminada, hasta el 10º nivel de anidamiento; además, se analizan independientemente de su tamaño real. Para modificar la configuración de análisis de archivos comprimidos, desactive la opción **Configuración por defecto para archivos comprimidos**.

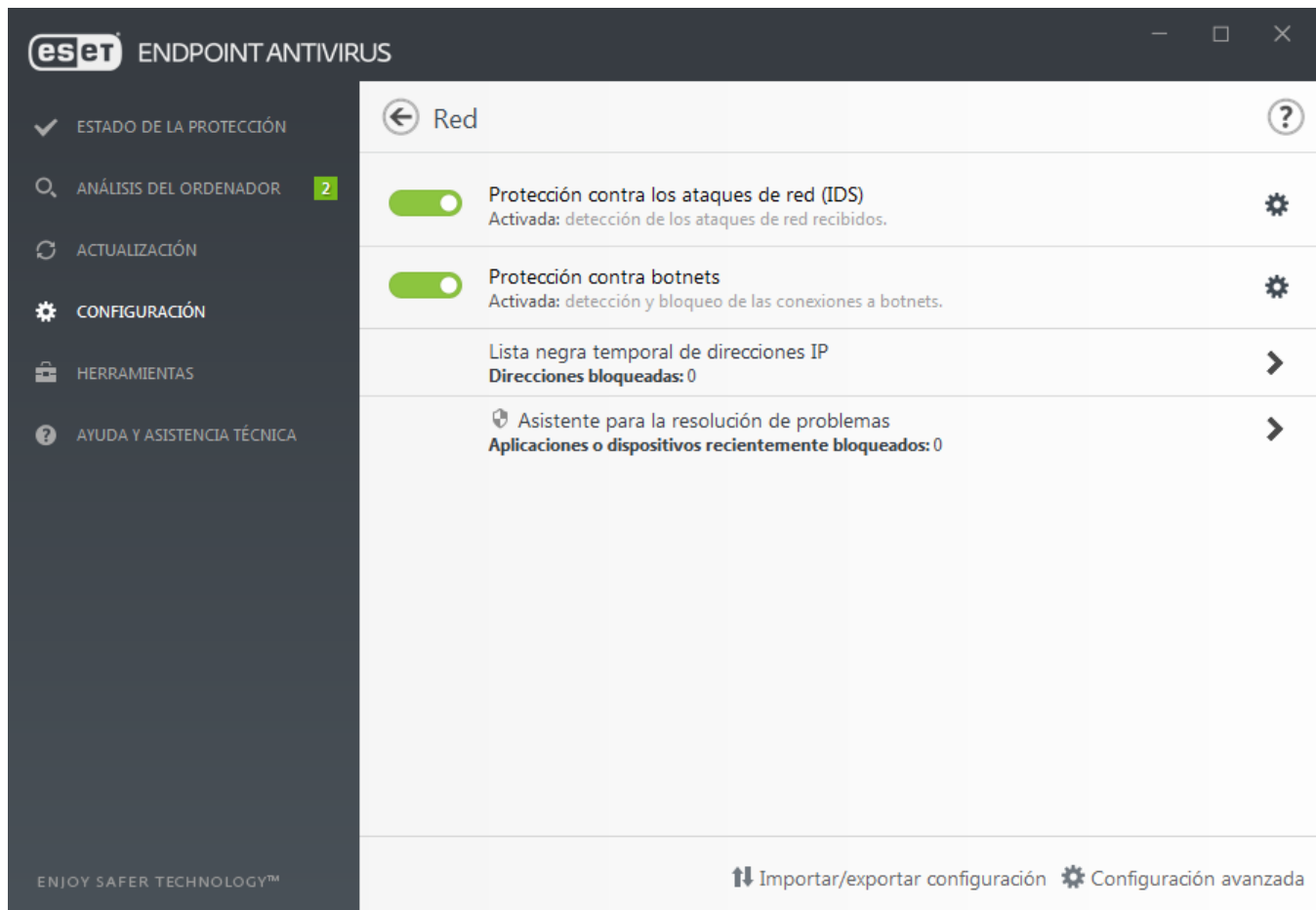
Para obtener más información sobre los **empaquetadores en tiempo real, archivos comprimidos de autoextracción y heurística avanzada**, consulte [Configuración de parámetros del motor ThreatSense](#).

Parámetros adicionales de ThreatSense para los archivos ejecutados: de forma predeterminada, la [heurística avanzada](#) no se utiliza cuando se ejecutan 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.

Red

La sección **Red** le permite acceder rápidamente a los siguientes componentes o ajustes en la configuración avanzada:

- **Protección contra los ataques de red (IDS):** analiza el contenido del tráfico de red y protege frente a ataques de red. El tráfico considerado perjudicial se bloqueará. ESET Endpoint Antivirus le informará cuando se conecte a una red inalámbrica sin protección o a una red con una protección débil.
- **Protección contra botnets:** identifica código malicioso en el sistema de forma rápida y precisa. Para desactivar la protección contra los ataques de red durante un periodo de tiempo determinado, haga clic en . (no recomendado).
- **Lista negra temporal de direcciones IP:** muestra 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. Para obtener más información, haga clic en esta opción y pulse F1.
- **Asistente para la resolución de problemas:** le ayuda a solucionar los problemas de conectividad provocados por el cortafuegos de ESET. Encontrará más información detallada en [Asistente de solución de problemas](#).



Protección contra los 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.](#)

Excepciones de IDS: esta opción le permite configurar opciones de filtrado avanzadas para detectar varios tipos de ataques y exploits que se pueden usar para dañar su ordenador.

Opciones avanzadas de filtrado

La sección de protección contra ataques de red le permite configurar opciones avanzadas de filtrado para detectar varios tipos de ataques y vulnerabilidades que pueden llevarse a cabo contra su ordenador.



Notificaciones y registro
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.



Disponibilidad de opciones concretas en esta página de ayuda

La disponibilidad de opciones determinadas en la Configuración avanzada (**F5**) > **Protección de la red** > **Protección contra ataques en la red** puede variar según el tipo o la versión de su producto ESET para equipos y el módulo de firewall, y según la versión de su sistema operativo. Es posible que algunas estén disponibles solo para ESET Endpoint Security.

- 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](https://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.
- **Mostrar notificación tras la detección de un ataque:** activa la notificación de la bandeja del sistema 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** – 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).
- **Verificar el estado de conexión TCP:** comprueba si todos los paquetes TCP pertenecen a una conexión existente. Si un paquete no existe en una conexión, este se eliminará.
- **Mantener las conexiones TCP inactivas:** para funcionar, algunas aplicaciones necesitan que la conexión TCP que establecen se mantenga, aunque esté inactiva. Active esta opción para evitar que finalicen las conexiones TCP inactivas.
- **Detección de sobrecarga del protocolo TCP:** el principio de este método implica exponer el ordenador/servidor a varias solicitudes. Consulte también [DoS \(ataques por denegación de servicio\)](#).
- **Verificación de mensajes para el protocolo ICMP:** impide los ataques que explotan los puntos débiles del protocolo ICMP y podrían hacer que el ordenador deje de responder. Consulte también [DoS \(ataques por denegación de servicio\)](#).
- **Detección de canales ocultos del protocolo ICMP:** comprueba si se utiliza el protocolo ICMP para la transferencia de datos. Muchas técnicas maliciosas utilizan el protocolo ICMP para burlar el cortafuegos.

Consulte el siguiente [artículo de la base de conocimiento de ESET](#) para ver una versión actualizada de esta página de ayuda.

Excepciones 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.



Instrucciones con ilustraciones


Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:

- [Create IDS exclusions on client workstations in ESET Endpoint Antivirus](#)
- [Create IDS exclusions for client workstations in ESET Security Management Center](#)

Columnas

- **Alerta:** tipo de alerta.
- **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 introduzca el nombre de la aplicación.
- **IP remota:** una lista de direcciones/rangos/subredes IPv4 o IPv6 remotos. Las direcciones deben separarse con comas.
- **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**.

Administración de excepciones de IDS

- **Agregar:** haga clic aquí para crear una nueva excepción de IDS.
- **Modificar:** haga clic aquí para editar una excepción de IDS.
- **Eliminado:** seleccione y haga clic aquí para quitar una excepción de la lista de excepciones de IDS.
-  **Superior/Arriba/Abajo/Inferior:** le permite ajustar el nivel de prioridad de las excepciones (las excepciones se evalúan de arriba abajo).



Ejemplo

Desea mostrar una notificación y recopilar un registro cada vez que se produzca el suceso:

- 1.Haga clic en **Agregar** para agregar una nueva excepción de IDS.
- 2.Seleccione una alerta en el menú desplegable **Alerta**.
- 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.



Ejemplo

Desea quitar las notificaciones recurrentes para un tipo de alerta que no considere una amenaza:

- 1.Haga clic en **Agregar** para agregar una nueva excepción de IDS.
- 2.Seleccione una alerta en el menú desplegable **Alerta**, por ejemplo, **Sesión SMB sin extensiones de seguridad** o.
- 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.

Sospecha de amenaza bloqueada

Esta situación puede darse cuando alguna de las aplicaciones del ordenador está intentando transmitir tráfico malicioso a otro ordenador de la red, aprovechando una vulnerabilidad de seguridad, o incluso si alguien intenta analizar puertos de su red.

Amenaza: nombre de la amenaza.

Fuente: dirección de red de la fuente.

Objeto: dirección de red del objeto.

Detener bloqueo: crea una excepción de IDS para la sospecha de amenaza con parámetros que permiten la comunicación.

Mantener bloqueo: bloquea la amenaza detectada. Si desea crear una excepción de IDS con parámetros de bloqueo de la comunicación de esta amenaza, seleccione **No volver a notificarme**.



Nota

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](#).

Resolución de problemas de protección de red

El asistente de solución de problemas le ayuda a solucionar los problemas de conectividad provocados por el cortafuegos de ESET. 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 continúa experimentando problemas con una aplicación, o su dispositivo no funciona según lo esperado, haga clic en **La aplicación sigue sin funcionar** para permitir todas las comunicaciones bloqueadas anteriormente para ese dispositivo. Reinicie el ordenador si el problema persiste.

Haga clic en **Mostrar cambios** para ver las reglas creadas por el asistente. También puede ver las reglas creadas por el asistente en **Configuración avanzada > Protección de la red > Cortafuegos > Avanzado > Reglas**.

Haga clic en **Desbloquear otro para resolver problemas de comunicación con un dispositivo o aplicación diferente**.

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, en ESET Endpoint Antivirus, vaya a **Configuración > Protección de la red > Lista negra de direcciones IP temporales**.

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.

Solución de problemas con el cortafuegos de ESET

Si tiene problemas de conectividad cuando ESET Endpoint Antivirus está instalado, tiene a su disposición varias maneras de comprobar si el cortafuegos de ESET es la causa del problema. Además, el cortafuegos 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 cortafuegos de ESET:

- [Asistente de solución de problemas](#)
- [Registro y creación de reglas o excepciones del registro](#)
- [Creación de excepciones a partir de notificaciones del cortafuegos](#)
- [Registro PCAP avanzado](#)
- [Solución de problemas con el filtrado de protocolos](#)

Asistente de solución de problemas

El asistente de solución de problemas supervisa silenciosamente todas las conexiones bloqueadas y le guía por el proceso de solución de problemas para corregir los problemas del cortafuegos con aplicaciones o dispositivos específicos. A continuación, el asistente le sugerirá un nuevo conjunto de reglas para que las aplique si está de acuerdo con ellas. El **asistente de solución de problemas** se encuentra en el menú principal, debajo de **Configuración > 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 consultar los bloqueos del cortafuegos, active el registro avanzado de Protección de la red en la sección **Diagnóstico** de la **Configuración avanzada** en **Herramientas > Diagnóstico**. Si ve en el registro algo que no desea que el cortafuegos bloquee, puede crear una regla o una excepción de IDS si hace clic con el botón derecho del ratón en dicho elemento y selecciona **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](#).



Nota

Utilice el registro para ver el orden en que el cortafuegos 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:

- defina el nivel mínimo de detalle al registrar en **Diagnóstico**, en **Configuración avanzada (F5) > Herramientas > Archivos de registro**,
- active **Mostrar notificaciones al recibir ataques que aprovechen de fallos de seguridad** en

Creación de excepciones a partir de notificaciones del cortafuegos

Cuando el cortafuegos de ESET detecta actividad de red maliciosa, se muestra una ventana de notificación donde se describe el suceso. Esta notificación contiene un enlace con más información sobre el suceso y que le permite configurar una excepción para dicho suceso, si desea hacerlo.



Nota

Si un dispositivo o una aplicación de red no implementa correctamente los estándares de red, puede desencadenar notificaciones de IDS del cortafuegos repetidas. Puede crear una excepción directamente desde la notificación para impedir que el cortafuegos de ESET detecte este dispositivo o esta aplicación.

Registro PCAP avanzado

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

1. Vaya a **Configuración avanzada > Herramientas > Diagnóstico** y active **Activar el registro avanzado del filtrado de protocolos**.

2. Intente repetir los pasos que provocaron el problema.

3. Desactive el registro PCAP avanzado.

4. El archivo de registro PCAP se encuentra en el mismo directorio donde se generan los volcados de memoria de diagnóstico:

- Microsoft Windows Vista o versiones posteriores

C:\ProgramData\ESET\ESET Security\Diagnostics

- Microsoft Windows XP

C:\Documents and Settings\All Users\...

Solución de problemas con el filtrado de protocolos

Si tiene problemas con su navegador o cliente de correo electrónico, lo primero que debe hacer es comprobar si la causa es el filtrado de protocolos. Para ello, desactive de forma temporal el filtrado de protocolos de la aplicación en la configuración avanzada (no se olvide de volver a activarlo cuando haya terminado, de modo que el navegador y el cliente de correo electrónico estén 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 el filtrado del protocolo SSL, desactívelo temporalmente. Si esto soluciona el problema, siga utilizando el filtrado SSL y excluya la comunicación problemática en el proceso de actualización: Establezca en interactivo el modo de filtrado del protocolo SSL. 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 no es un navegador o un cliente de correo electrónico, puede excluirla totalmente del filtrado de protocolos (si hace esto para 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 de un dispositivo de la red (como abrir una 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 del filtrado de protocolos 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"

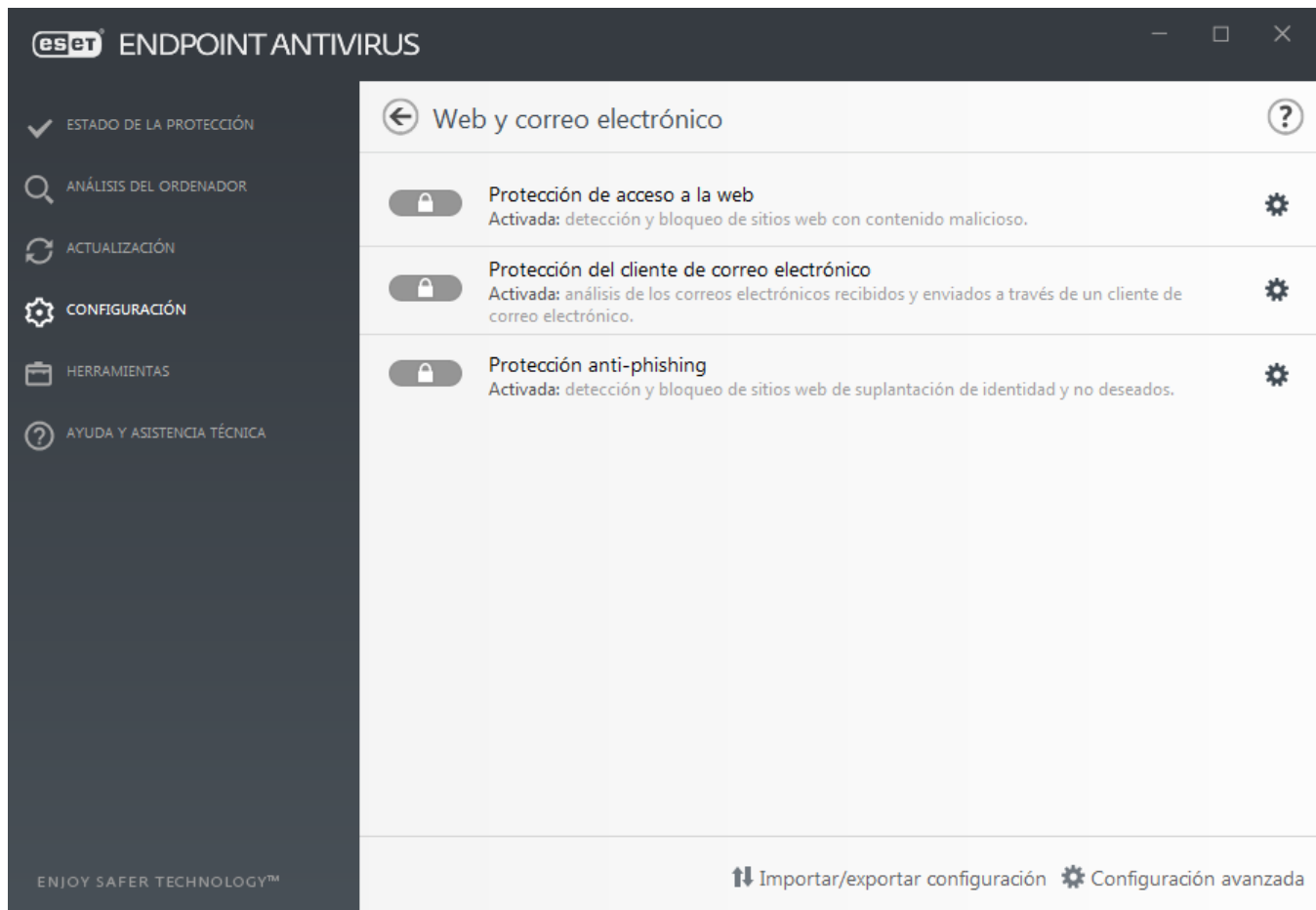
Cuando se activa el filtrado del protocolo SSL, ESET Endpoint Antivirus un certificado a su almacén de certificados para asegurarse de que las aplicaciones instaladas confíen en su método de filtrado del protocolo SSL. Esta operación no se puede realizar en algunas aplicaciones mientras se ejecutan, como en Firefox y Opera. 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). A continuación, 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 el filtrado del protocolo SSL y vuelva a activarlo. El proceso de importación se volverá a ejecutar.

Web y correo electrónico


Las opciones de configuración de la Web y el correo electrónico se encuentra en **Configuración > Web y correo electrónico**. Desde aquí puede acceder a configuraciones más detalladas del programa.



La conectividad de Internet es una característica estándar de cualquier ordenador personal. Lamentablemente, también se ha convertido en el principal medio de transferencia de código malicioso. Por eso, es fundamental prestar la debida atención a la [protección del tráfico de Internet](#).

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.

La [Protección antiphishing](#) es otra capa de protección que aumenta la defensa frente a sitios web ilegítimos que intentan adquirir contraseñas y otra información confidencial. La protección antiphishing se puede activar en el panel **Configuración** disponible en **Web y correo electrónico**. Consulte [Protección antiphishing](#) para obtener más información.

Puede desactivar temporalmente el módulo de protección de web/correo electrónico/anti-phishing haciendo clic en .

Filtrado de protocolos

El motor de análisis ThreatSense, que integra a la perfección todas las técnicas avanzadas de análisis de malware, proporciona la protección antivirus para los protocolos de aplicación. El filtrado de protocolos funciona de manera automática, independientemente del navegador de Internet o el cliente de correo electrónico utilizados. Para editar la configuración cifrada (SSL), vaya a **Configuración avanzada (F5) > Web y Web y correo electrónico > [SSL/TLS](#)**.

Activar el filtrado del contenido de los protocolos de aplicación: se puede utilizar para desactivar el filtrado de protocolos. Tenga en cuenta que muchos componentes de ESET Endpoint Antivirus (Protección del tráfico de Internet, Protección de protocolos de correo electrónico, Anti-Phishing, Control de acceso web) dependen de esto para funcionar.

Aplicaciones excluidas: le permite excluir determinadas aplicaciones del filtrado de protocolos. Esta opción es útil cuando el filtrado de protocolos provoca problemas de compatibilidad.

Direcciones IP excluidas: le permite excluir determinadas direcciones remotas del filtrado de protocolos. Esta opción es útil cuando el filtrado de protocolos provoca problemas de compatibilidad.



Ejemplo de direcciones IP excluidas

Direcciones IPv4 y máscara:

- 192.168.0.10: agrega la dirección IP de un ordenador individual al que debe aplicarse la regla.
- 192.168.0.1 a 192.168.0.99: especifique las direcciones IP inicial y final para delimitar el intervalo de direcciones (de varios ordenadores) al que se aplicará la regla.
- Subred (grupo de ordenadores) definida por una dirección IP y una máscara. Por ejemplo, 255.255.255.0 es la máscara de red del prefijo 192.168.1.0/24 (es decir, el intervalo de direcciones de 192.168.1.1 a 192.168.1.254).

Dirección IPv6 y máscara:

- 2001:718:1c01:16:214:22ff:fec9:ca5: agrega la dirección IPv6 de un ordenador individual al que debe aplicarse la regla.
- 2002:c0a8:6301:1::1/64: dirección IPv6 con la longitud de prefijo de 64 bits, lo que significa 2002:c0a8:6301:0001:0000:0000:0000:0000 a 2002:c0a8:6301:0001:ffff:ffff:ffff:ffff

Aplicaciones excluidas

Para excluir del filtrado de protocolos la comunicación de aplicaciones de red específicas, añádalas a esta lista. No se comprobará la presencia de amenazas en la comunicación HTTP, POP3 e IMAP de las aplicaciones seleccionadas. Solo recomendamos utilizar esta técnica cuando las aplicaciones no funcionen correctamente con el filtrado de protocolos activado.

Las aplicaciones y los servicios que ya se hayan visto afectados por el filtrado de protocolos se mostrarán automáticamente al hacer clic en **Agregar**.

Modificar: modifique las entradas seleccionadas de la lista.

Eliminado: elimina las entradas seleccionadas de la lista.

Direcciones IP excluidas

Las direcciones IP de esta lista no se incluirán en el filtrado de contenidos del protocolo. No se comprobará la presencia de amenazas en las comunicaciones HTTP/POP3/IMAP 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.

SSL/TLS

ESET Endpoint Antivirus puede buscar amenazas en las comunicaciones que utilizan el protocolo SSL. Puede utilizar varios modos de análisis 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.

Activar el filtrado del protocolo SSL/TLS: el filtrado de protocolos está activado de forma predeterminada. Puede desactivar el filtrado de protocolos SSL/TLS en **Configuración avanzada > Web y correo electrónico > SSL/TLS** o mediante una política. Si está desactivado el filtrado de protocolos, el programa no analizará las comunicaciones a través de SSL.

El **modo de filtrado del protocolo SSL/TLS** ofrece las opciones siguientes:

Modo de filtrado	Descripción
Modo automático	El modo predeterminado solo analizará las aplicaciones correspondientes, como navegadores de Internet y clientes de correo. Puede anular esta opción seleccionando las aplicaciones para las que se analizarán las comunicaciones.
Modo 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.
Modo de política	Modo de política: 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.

La **Lista de aplicaciones con filtrado SSL/TLS** permite personalizar el comportamiento de ESET Endpoint Antivirus para aplicaciones específicas

Lista de certificados conocidos le permite personalizar el comportamiento de ESET Endpoint Antivirus para

certificados SSL específicos.

Excluir la comunicación con los dominios de confianza: cuando esta opción está activada, la comunicación con los dominios de confianza se excluye de la comprobación. La confianza en los dominios se determina mediante la lista blanca integrada.

Bloquear la comunicación cifrada utilizando el protocolo obsoleto SSL v2: la comunicación establecida con la versión anterior del protocolo SSL se bloqueará automáticamente.



Nota

No se filtrarán las direcciones si ha activado el ajuste **Excluir la comunicación con los dominios de confianza** y el dominio se considera de confianza.

Certificado raíz

Certificado raíz: 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). **Agregar el certificado raíz a los navegadores conocidos** debe estar activada. Seleccione esta opción para agregar el certificado raíz de ESET a los navegadores conocidos (por ejemplo, Opera y Firefox) de forma automática. En los navegadores que utilicen el almacén de certificados del sistema, el certificado se agregará automáticamente (por ejemplo, en Internet Explorer).

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.

Validez del certificado

Si el certificado no se puede verificar mediante el almacén de certificados TRCA: a veces no es posible verificar el certificado de un sitio web con el almacén de autoridades certificadoras de confianza (TRCA). Esto significa que el certificado ha sido firmado por algún usuario (por ejemplo, el administrador de un servidor web o una pequeña empresa) y que el hecho de confiar en él no siempre representa un riesgo. La mayoría de las empresas grandes (como los bancos) utilizan certificados firmados por TRCA. Si se ha seleccionado **Preguntar sobre la validez del certificado** (predeterminada), se le pedirá al usuario que seleccione la acción que desea realizar cuando se establezca la comunicación cifrada. Puede seleccionar **Bloquear las comunicaciones que usan el certificado** para finalizar siempre las conexiones cifradas a sitios que tienen certificados sin verificar.

Si el certificado no es válido o está dañado: significa que el certificado ha caducado o que la firma no es correcta. En este caso, se recomienda dejar seleccionada la opción **Bloquear las comunicaciones que usan el certificado**.



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 de ESET](#)
- [Se muestra "Tráfico de red cifrado: certificado no de confianza" al visitar páginas web](#)

Certificados

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). **Añadir el certificado raíz a los navegadores conocidos** debe estar activada. Seleccione esta opción para agregar el certificado raíz de ESET a los navegadores conocidos (por ejemplo, Opera y Firefox) de forma automática. En los navegadores que utilicen el almacén de certificados del sistema, el certificado se agregará automáticamente (por ejemplo, en Internet Explorer). 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.

En algunos casos, el certificado no se puede comprobar mediante el archivo de autoridades certificadoras de confianza (por ejemplo, VeriSign). Esto significa que el certificado ha sido autofirmado por algún usuario (por ejemplo, el administrador de un servidor web o una pequeña empresa) y que el hecho de confiar en él no siempre

representa un riesgo. La mayoría de empresas grandes (como los bancos) utilizan certificados firmados por TRCA. Si se ha seleccionado **Preguntar sobre la validez del certificado** (predeterminada), se le pedirá al usuario que seleccione la acción que desea realizar 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, y si está en dicha lista, 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.

Si el certificado no es válido o está dañado, significa que ha expirado o que la autofirma no es correcta. En este caso, se recomienda bloquear las comunicaciones que utilicen dicho certificado.

Tráfico de red cifrado

Si su sistema está configurado para utilizar el análisis del protocolo SSL, 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 de filtrado del protocolo SSL** 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 de ESET](#)
- [Se muestra "Tráfico de red cifrado: certificado no de confianza" al visitar páginas web](#)

En ambos casos, el usuario tiene la opción de recordar la acción seleccionada. Las acciones guardadas se almacenan en la [Lista de certificados conocidos](#).

Lista de certificados conocidos

La **Lista de certificados conocidos** se puede utilizar para personalizar el comportamiento de ESET Endpoint Antivirus para determinados certificados SSL, así como para recordar las acciones elegidas al seleccionar el **Modo interactivo** en el **Modo de filtrado de protocolos SSL/TLS**. La lista se puede ver y modificar en **Configuración avanzada** (F5) > **Web y correo electrónico** > **SSL/TLS** > **Lista de certificados conocidos**.

La ventana **Lista de certificados conocidos** consta de estos elementos:

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: puede cargarse un certificado manualmente como un archivo con la extensión *.cer*, *.crt* o *.pem*. Haga clic en **Archivo** para cargar un certificado local, o haga clic en **URL** para especificar la ubicación de un certificado en línea.

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.

Lista de aplicaciones con filtrado SSL/TLS

La **Lista de aplicaciones con filtrado SSL/TLS** se puede utilizar para personalizar el comportamiento de ESET Endpoint Antivirus para determinadas aplicaciones, así como para recordar las acciones elegidas al seleccionar el **Modo interactivo** en el **Modo de filtrado de protocolos SSL/TLS**. La lista se puede ver y modificar en **Configuración avanzada** (F5) > **Web y correo electrónico** > **SSL/TLS** > **Lista de aplicaciones con filtrado SSL/TLS**.

La ventana **Lista de aplicaciones con filtrado SSL/TLS** consta de estos elementos:

Columnas

Aplicación: nombre de la aplicación.

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.

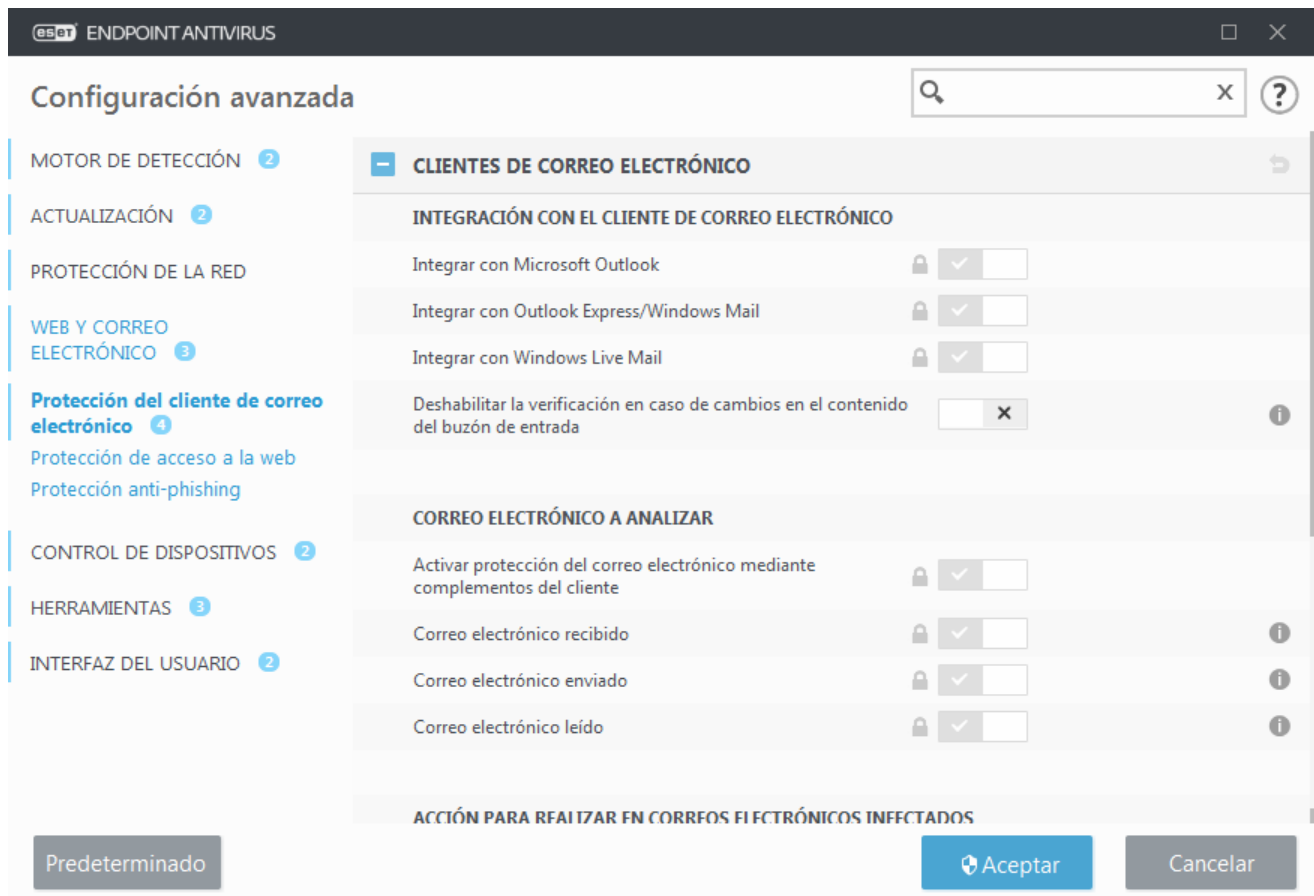
Editar: seleccione el certificado que desea configurar y haga clic en **Editar**.

Eliminar: seleccione el certificado que desea eliminar y haga clic en **Eliminado**.

Aceptar/Cancelar: haga clic en **Aceptar** para guardar los cambios o en **Cancelar** para salir sin guardarlos.

Protección del cliente de correo electrónico

La integración de ESET Endpoint Antivirus con su cliente de correo electrónico aumenta el nivel de protección activa frente a código malicioso en los mensajes de correo electrónico. Si su cliente de correo electrónico es compatible, la integración se puede activar 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. Las opciones de integración están disponibles en **Configuración avanzada** (F5) > **Web y correo electrónico** > **Protección de clientes de correo electrónico** > **Clientes de correo electrónico**.



Integración con el cliente de correo electrónico

Actualmente se admiten los siguientes clientes de correo electrónico: [Microsoft Outlook](#), [Outlook Express](#), [Windows Mail](#) y Windows Live Mail. La protección de correo electrónico funciona como un complemento para estos programas. 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 de clientes de correo electrónico compatibles y sus versiones, consulte el siguiente [artículo de la base de conocimientos de ESET](#).

Active **Deshabilitar la verificación en caso de cambios en el contenido del buzón de entrada** si el sistema se ralentiza al recuperar correos electrónicos.

Correo electrónico a analizar

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.

Correo electrónico recibido: cuando esta opción está activada, comprueba los mensajes de correo electrónico recibidos.

Correo electrónico enviado: cuando esta opción está activada, comprueba los mensajes de correo electrónico enviados.

Correo electrónico leído: cuando esta opción está activada, comprueba los mensajes de correo electrónico leídos.



Nota

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 [Filtrado de protocolos](#) (IMAP/IMAPS y POP3/POP3S).

Acción para realizar en correos electrónicos infectados

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.

Repetir el análisis tras la actualización: cuando esta opción está activada, repite el análisis de los correos electrónicos infectados tras una actualización del motor de detección.

Aceptar los resultados de los análisis realizados por otros módulos: permite que el módulo de protección del correo electrónico use los resultados de los análisis recibidos de los demás módulos de protección en lugar de repetir el análisis.

Protocolos de correo electrónico

Los protocolos IMAP y POP3 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.

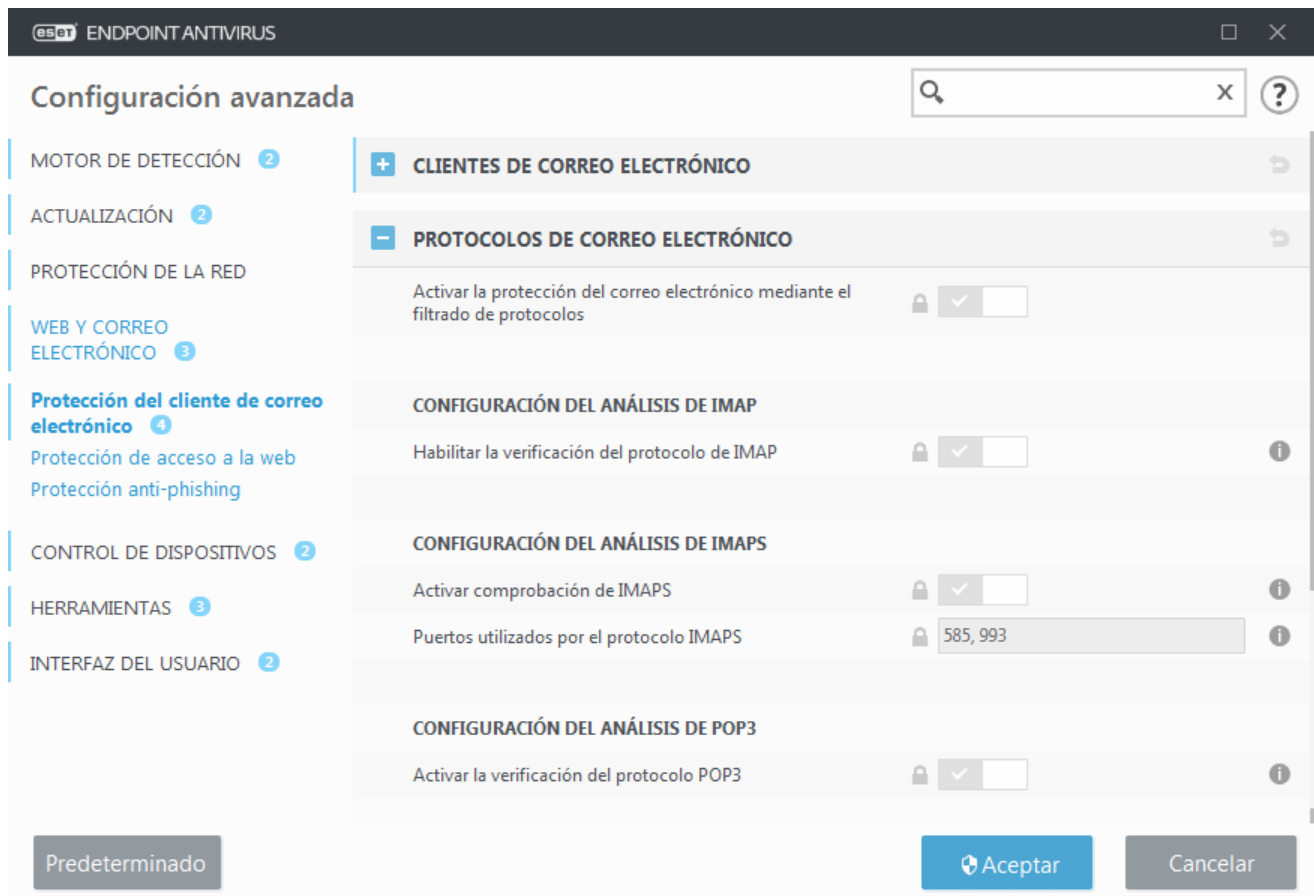
ESET Endpoint Antivirus proporciona protección para estos protocolos, independientemente del cliente de correo electrónico utilizado, y sin necesidad de volver a configurar el cliente de correo electrónico. De forma predeterminada, se analiza toda la comunicación a través de los protocolos POP3 e IMAP, 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.

Se recomienda dejar la opción **Activar la protección del correo electrónico mediante el filtrado de protocolos** activada. Para configurar la comprobación de los protocolos IMAP/IMAPS y POP3/POP3S, vaya a Configuración avanzada > **Web y correo electrónico** > **Protección de clientes de correo electrónico** > **Protocolos de correo electrónico**.

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). El programa solo analizará el tráfico de los puertos definidos en **Puertos usados por el protocolo IMAPS/POP3S**, independientemente de la versión del sistema operativo. Se pueden agregar otros puertos de comunicación si es necesario. Cuando haya varios números de puerto, deben delimitarse con una coma.

La comunicación cifrada se analizará de forma predeterminada. Para ver la configuración del análisis, vaya a [SSL/TLS](#) en la sección Configuración avanzada, haga clic en **Web y correo electrónico** > **SSL/TLS** y active la opción **Activar el filtrado del protocolo SSL/TLS**.



Alertas y notificaciones por correo electrónico

Las opciones de esta función están disponibles en **Configuración avanzada, en Web y correo electrónico > Protección del cliente de correo electrónico > Alertas y notificaciones**.

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 con 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 enviados: desactive esta casilla de verificación si no desea que la protección de correo electrónico incluya una alerta de virus en el asunto de los mensajes infectados. Esta función permite el filtrado sencillo y por asunto de los mensajes infectados (si su programa de correo electrónico lo admite). Además, aumenta la credibilidad ante el destinatario y, si se detecta una amenaza, proporciona información valiosa sobre el nivel de amenaza de un correo electrónico o remitente determinado.

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.

Integración con clientes de correo electrónico

Actualmente se admiten los siguientes clientes de correo electrónico: [Microsoft Outlook](#), [Outlook Express](#), [Windows Mail](#) y Windows Live Mail. La protección de correo electrónico funciona como un complemento para estos programas. 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 de clientes de correo electrónico compatibles y sus versiones, consulte el siguiente [artículo de la base de conocimientos de ESET](#).

Barra de herramientas de Microsoft Outlook

La protección de Microsoft Outlook funciona como un módulo de complemento. Después de instalar ESET Endpoint Antivirus, la barra de herramientas con las opciones de protección antivirus y se añade a Microsoft Outlook:

ESET Endpoint Antivirus: al hacer clic en el icono, se abre la ventana principal del programa 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 cliente de correo electrónico](#).

Configuración del análisis: muestra las opciones de configuración de la [Protección del cliente de correo electrónico](#).

Barra de herramientas de Outlook Express y Windows Mail

La protección para Outlook Express y Windows Mail funciona como un módulo de complemento. Después de instalar ESET Endpoint Antivirus, la barra de herramientas con las opciones de protección antivirus y se añade a Outlook Express o Windows Mail:

ESET Endpoint Antivirus: al hacer clic en el icono, se abre la ventana principal del programa 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 cliente de correo electrónico](#).

Configuración del análisis: muestra las opciones de configuración de la [Protección del cliente de correo electrónico](#).

Interfaz de usuario

Personalizar la apariencia: la apariencia de la barra de herramientas se puede modificar para el cliente de correo electrónico. Desactive la opción que personaliza la apariencia independientemente de los parámetros del programa de correo electrónico.

Mostrar texto: muestra descripciones de los iconos.

Texto a la derecha: las descripciones se mueven de la parte inferior al lado derecho de los iconos.

Iconos grandes: muestra iconos grandes para las opciones de menú.

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.

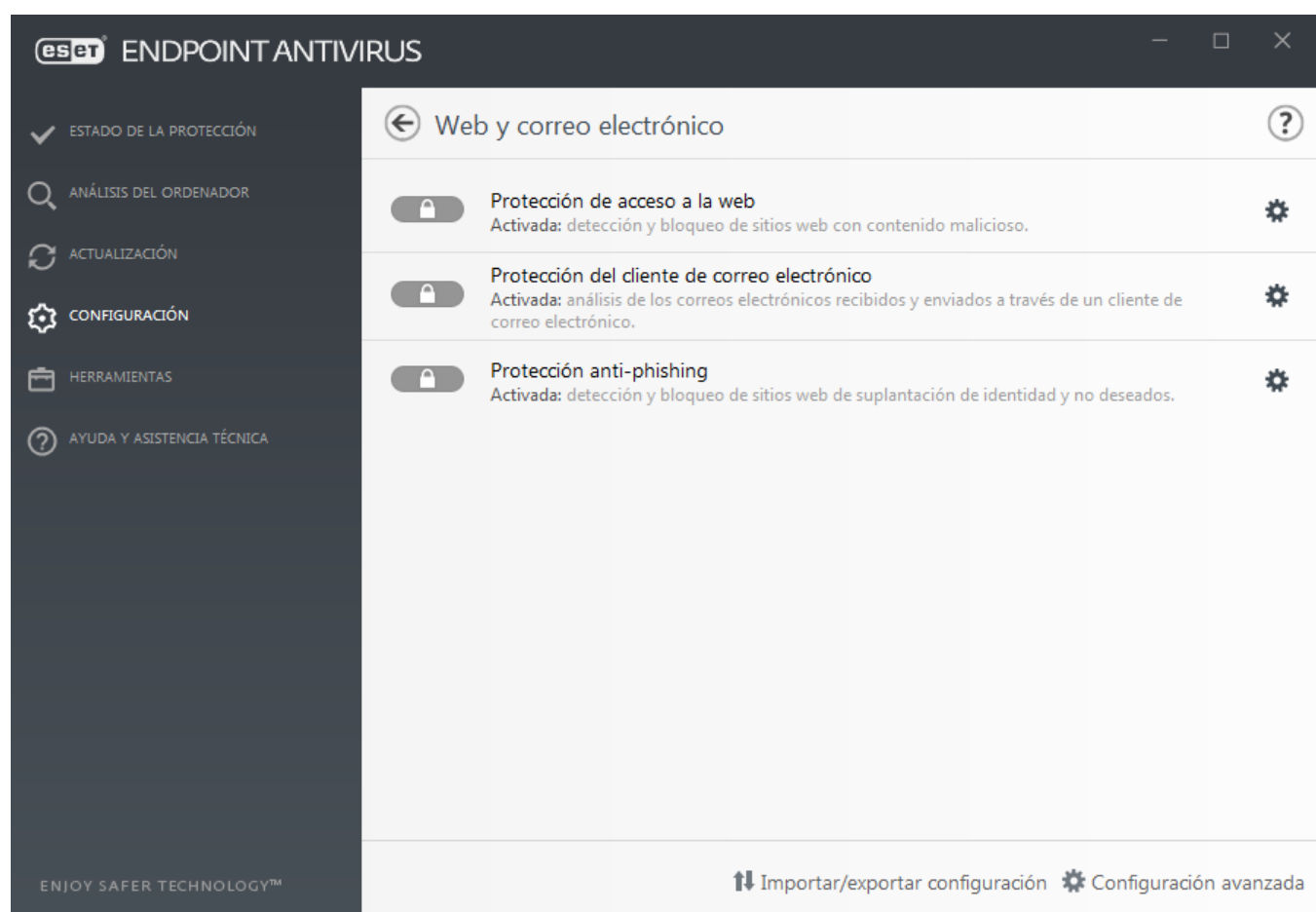
La casilla de verificación **Volver a analizar los mensajes ya analizados** proporciona una opción para ejecutar otro análisis en mensajes ya analizados.

Protección del tráfico de Internet

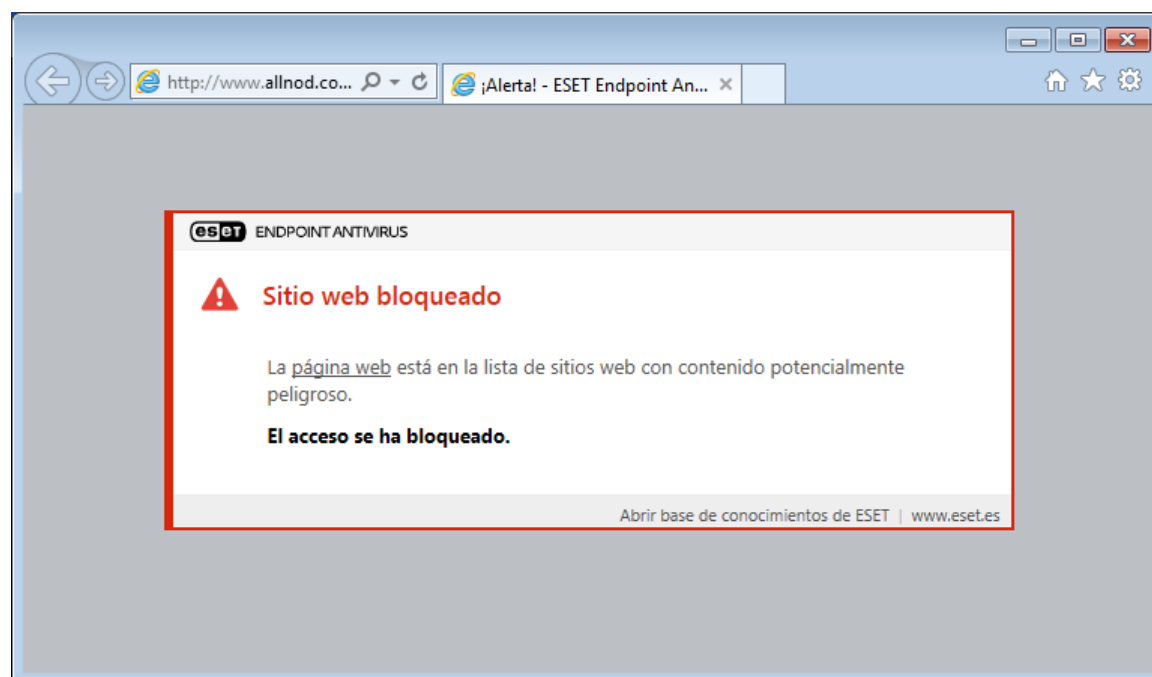
La conectividad de Internet es una característica estándar de cualquier ordenador personal. Lamentablemente, también se ha convertido en el principal medio de transferencia de código malicioso. La protección del tráfico de Internet funciona supervisando la comunicación entre navegadores web y servidores remotos, y cumple con las reglas HTTP (Protocolo de transferencia de hipertexto) y HTTPS (comunicación cifrada).

El acceso a las páginas web que se sabe que contienen código malicioso se bloquea antes de descargar contenido. El motor de análisis ThreatSense analiza todas las demás páginas web cuando se cargan y bloquean en caso de detección de contenido malicioso. La protección del tráfico de Internet ofrece dos niveles de protección: bloqueo por lista negra y bloqueo por contenido.

Le recomendamos encarecidamente que active la opción de protección del tráfico de Internet. Se puede acceder a esta opción desde la ventana principal de ESET Endpoint Antivirus accediendo a **Configuración > Protección de Internet > Protección del tráfico de Internet**.



Protección de acceso a la web mostrará el siguiente mensaje en su navegador cuando el sitio web esté bloqueado:



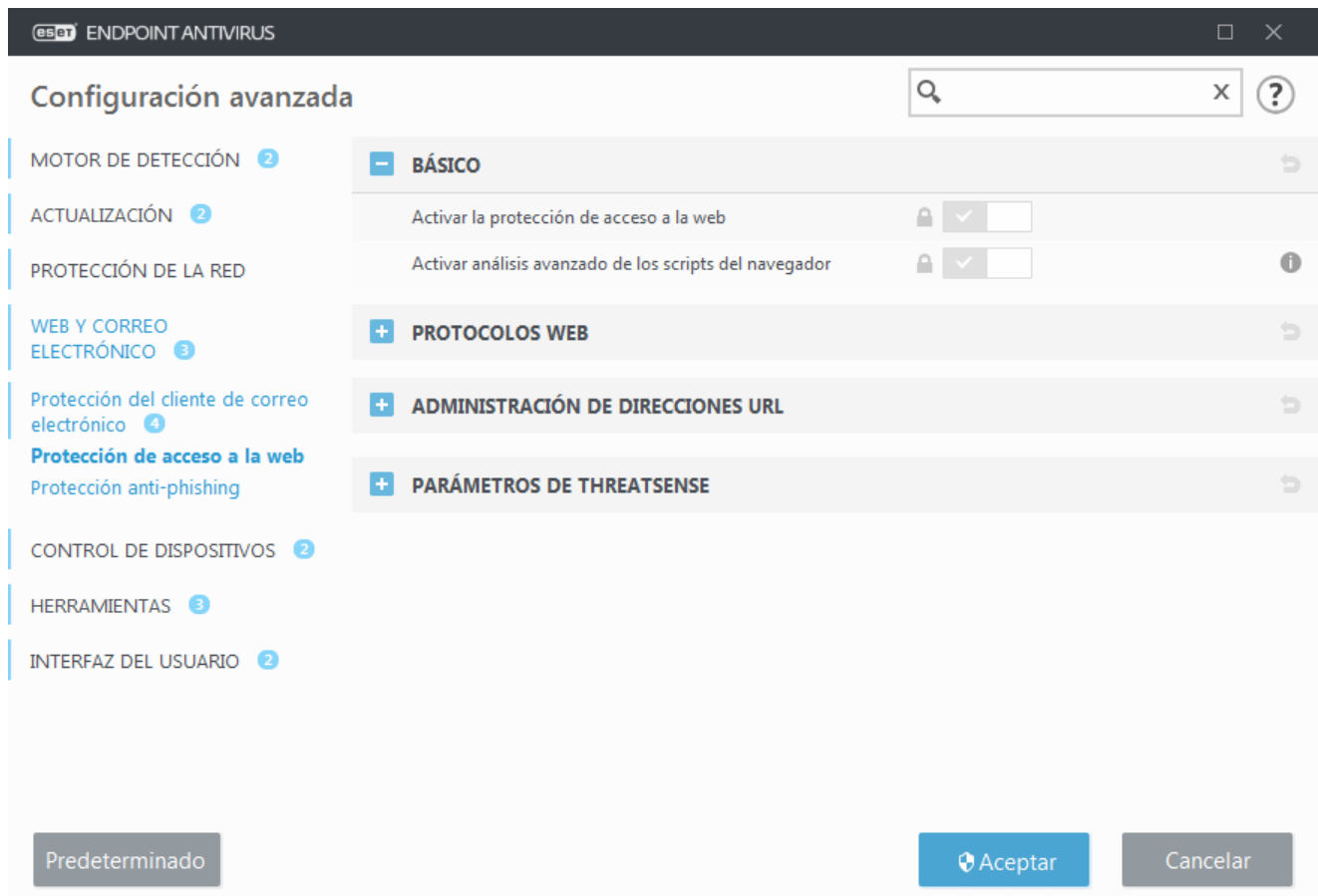
Instrucciones con ilustraciones

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](#)
- [Unblock a safe website on an endpoint using ESET Security Management Center](#)

Las opciones siguientes están disponibles en **Configuración avanzada (F5) > Web y correo electrónico > Protección del tráfico de Internet:**

- **Básico:** para activar o desactivar esta característica desde Configuración avanzada.
- **Protocolos web:** le permite configurar la supervisión de estos protocolos estándar que utilizan la mayoría de los navegadores de Internet.
- **Gestión de direcciones URL:** le permite especificar las direcciones URL que desea bloquear, permitir o excluir del análisis.
- **Parámetros de ThreatSense:** la configuración avanzada del análisis de virus le permite configurar opciones como los tipos de objetos que desea analizar (mensajes de correo electrónico, archivos comprimidos, etc.), los métodos de detección para la protección del tráfico de Internet, etc.



Configuración avanzada de la protección de acceso a la web

Las siguientes opciones están disponibles en **Configuración avanzada** (F5) > **Web y correo electrónico** > **Protección de acceso a la web** > **Básico**:

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](#).

Activar análisis avanzado de los scripts del navegador: cuando esta opción está activada, el motor de detección comprueba todos los programas JavaScript ejecutados por los navegadores.



Nota

Le recomendamos encarecidamente que mantenga activada la opción **Protección del acceso a la Web**.

Protocolos web

De forma predeterminada, ESET Endpoint Antivirus está configurado para supervisar el protocolo HTTP que utilizan la mayoría de los navegadores de Internet.

Configuración del análisis de HTTP

El tráfico HTTP se supervisa siempre en todos los puertos y para todas las aplicaciones.

Configuración del análisis de HTTPS

ESET Endpoint Antivirus admite también la comprobación del protocolo HTTPS. La comunicación 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 (443, 0-65535) definidos en **Puertos utilizados por el protocolo HTTPS**, independientemente de la versión del sistema operativo.

La comunicación cifrada se analizará de forma predeterminada. Para ver la configuración del análisis, vaya a

[SSL/TLS](#) en la sección Configuración avanzada, haga clic en **Web y correo electrónico > SSL/TLS** y active la opción **Activar el filtrado del protocolo SSL/TLS**.

Gestión de direcciones URL

La sección de gestión de direcciones URL le permite especificar las direcciones HTTP que desea bloquear, permitir o excluir del análisis de contenido.

Debe seleccionar **Activar el filtrado del protocolo SSL/TLS** si desea filtrar las direcciones HTTPS, además de las páginas web 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. Tenga especial cuidado 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**.



Bloquear o permitir extensiones de archivo concretas

La gestión de direcciones URL también permite bloquear o permitir la apertura de tipos de archivos específicos durante la navegación en Internet. Por ejemplo, si no desea que se abran archivos ejecutables, seleccione la lista en la que desee bloquear estos archivos del menú desplegable y, a continuación, introduzca la máscara "**.exe".



Dominios de confianza

No se filtrarán las direcciones si ha activado el ajuste **Web y correo electrónico > SSL/TLS > Excluir la comunicación con los dominios de confianza** y el dominio se considera de confianza.

Lista de direcciones

?

Q

Nombre de la lista	Tipos de direcciones	Descripción de la lista
Lista de direcciones permitidas	Permitido	
Lista de direcciones bloqueadas	Bloqueado	
Lista de direcciones excluidas del análisis de contenido	Se ha ignorado el malwa...	

Agregar

Editar

Eliminar

Agregue un comodín (*) a la lista de direcciones bloqueadas para bloquear todas las URL excepto aquellas incluidas en una lista de direcciones permitidas.

Aceptar

Cancelar

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 URL

En esta sección podrá indicar las listas de direcciones HTTP 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**.

Lista de direcciones

?

Nombre de la lista

Tipos de direcciones

Descripción de la lista

Lista de direcciones permitidas	Permitido	
Lista de direcciones bloqueadas	Bloqueado	
Lista de direcciones excluidas del análisis de contenido	Se ha ignorado el malwa...	

Agregar

Editar

Eliminar

Agregue un comodín (*) a la lista de direcciones bloqueadas para bloquear todas las URL excepto aquellas incluidas en una lista de direcciones permitidas.

Aceptar

Cancelar



Instrucciones con ilustraciones

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](#)
- [Unblock a safe website on an endpoint using ESET Security Management Center](#)

Si desea obtener más información, consulte [Administración de direcciones URL](#).

Creación de nueva lista de direcciones URL

En esta sección podrá indicar las listas de máscaras o direcciones URL que desea bloquear, permitir o excluir del análisis.

Cuando se crea una lista nueva, se pueden configurar las siguientes opciones:

Tipo de lista de direcciones: están disponibles tres tipos de listas predefinidas:

- **Excluido de la comprobación:** no se comprobará la existencia de código malicioso en ninguna de las direcciones agregadas a esta lista.
- **Bloqueado:** el usuario no tendrá acceso a las direcciones especificadas en la lista.
- **Permitido:** si se configura la política para utilizar esta característica y el valor de comodín (*) se agrega a esta lista, podrá acceder a las direcciones de esta lista aunque dichas direcciones también aparezcan en la lista bloqueada.

Nombre de la lista: especifique el nombre de la lista. Este campo no estará disponible si edita una de las tres listas predefinidas.

Descripción de la lista: escriba una breve descripción de la lista (opcional). Este campo no estará disponible si edita una de las tres listas predefinidas.

Lista activa: seleccione la barra deslizante para activar la lista.

Notificar al aplicar: seleccione la barra deslizante si desea recibir una notificación cuando se utilice esta lista para evaluar un sitio HTTP que haya visitado. Por ejemplo, se emitirá una notificación cuando un sitio web se bloquee o admita porque se ha incluido en la lista de direcciones bloqueadas o permitidas. La notificación mostrará el nombre para de la lista que especifique el sitio web.

Registro de severidad: seleccione el registro de severidad en el menú desplegable. El administrador remoto puede recopilar los registros con detalle de advertencia.

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. Solo se puede utilizar con direcciones que se hayan creado con la opción **Agregar**.

Quitar: elimina las direcciones existentes de la lista. Solo se puede utilizar con direcciones que se hayan creado con la opción **Agregar**.

Importar: importe un archivo con direcciones URL separadas por un salto de línea (por ejemplo, un archivo *.txt con codificación UTF-8).

Cómo agregar una máscara URL

Consulte las instrucciones de este cuadro de diálogo antes de especificar la dirección/máscara de dominio que desea.

ESET Endpoint Antivirus permite al usuario bloquear el acceso a determinados sitios web para evitar que el navegador de Internet muestre su contenido. Además, permite 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.).

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 *.dominio.com no coincidirá con <http://cualquierdominio.com/cualquierruta#.dominio.com> (este sufijo se puede añadir a cualquier URL sin que la descarga se vea afectada). En segundo lugar, la secuencia "*" también corresponde 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 *.dominio.com también coincide con <http://dominio.com>. No sería correcto utilizar *dominio.com, ya que esta cadena también detectaría <http://otrodominio.com>.

Protección Anti-Phishing

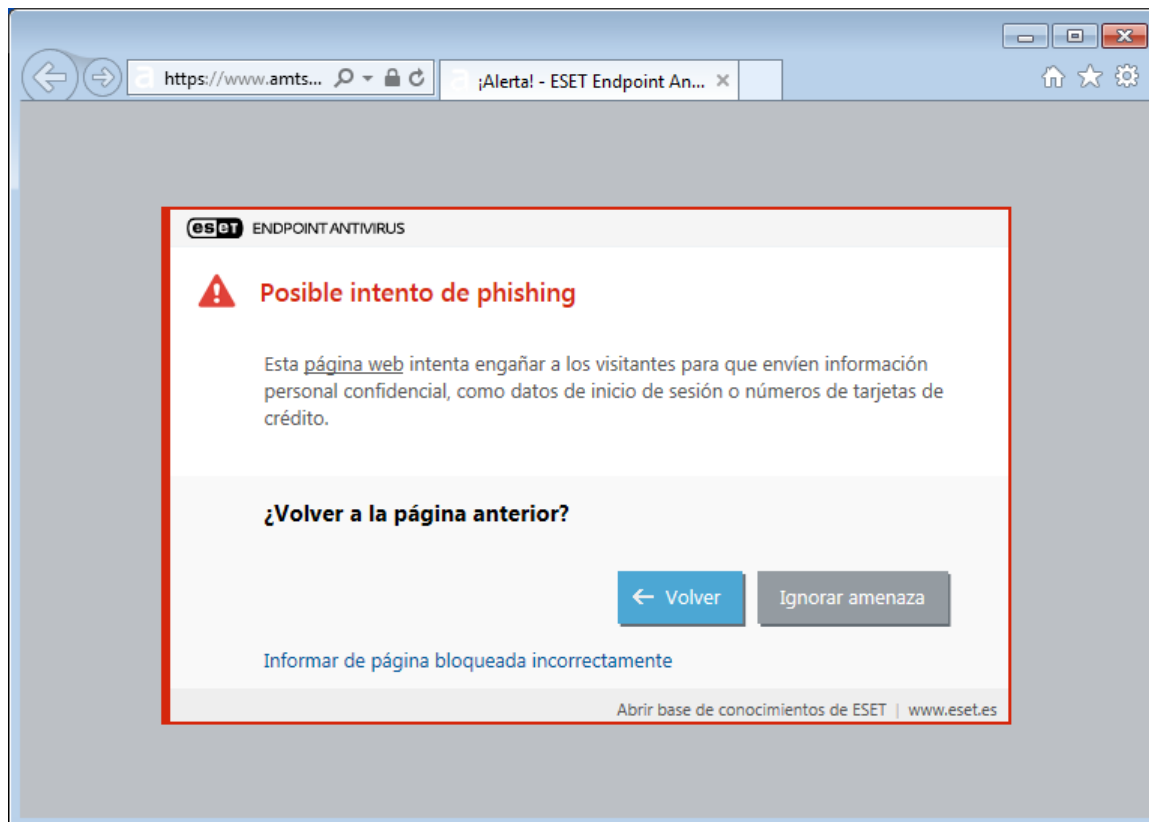
El término phishing, o suplantación de la identidad, define una actividad delictiva que usa técnicas de ingeniería social (manipulación de los usuarios para obtener información confidencial). Su objetivo con frecuencia es acceder a datos confidenciales como, por ejemplo, números de cuentas bancarias, códigos PIN, etc. Puede obtener más información sobre esta actividad en el [glosario](#). ESET Endpoint Antivirus incluye protección frente al phishing que bloquea páginas web conocidas por distribuir este tipo de contenido.

Recomendamos encarecidamente que active la protección Anti-Phishing en ESET Endpoint Antivirus. Para ello, abra **Configuración avanzada** (F5) y acceda a **Web y correo electrónico > Protección Anti-Phishing**.

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

Cuando entre en un sitio web de phishing reconocido se mostrará el siguiente cuadro de diálogo en su navegador web. Si aun así quiere acceder al sitio web, haga clic en **Ir al sitio** (no recomendado).



Nota

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** (F5), despliegue **Web y correo electrónico > Protección del tráfico de Internet > Gestión de direcciones URL > Lista de direcciones**, haga clic en **Modificar** y agregue a la lista el sitio web que desee modificar.

Cómo informar de sitios de phishing

El enlace [Informar](#) le permite informar de un sitio web de phishing o malicioso para que ESET lo analice.



Nota

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 un falso positivo de phishing](#).

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.).

Actualización del programa

La mejor manera de disfrutar del máximo nivel de seguridad en el ordenador es actualizar ESET Endpoint Antivirus de forma periódica. El módulo Actualización garantiza que el programa está siempre actualizado de dos maneras: actualizando el motor de detección y los componentes del sistema. Cuando se activa el programa, las actualizaciones están activadas de forma predeterminada.

Haga clic en **Actualizar** en la ventana principal del programa para comprobar el estado de la actualización, la fecha y la hora de la última actualización, y si es necesario actualizar el programa. También puede hacer clic en el vínculo **Mostrar todos los módulos** para abrir la lista de módulos instalados y comprobar tanto la versión como la última actualización de un módulo.

También tiene a su disposición la opción **Buscar actualizaciones** para iniciar el proceso de actualización de forma manual. La actualización del motor de detección de virus y la actualización de los componentes del programa son partes importantes a la hora de mantener una protección completa frente a código malicioso. Preste especial atención a su configuración y funcionamiento. Si no especificó los datos de la licencia durante la instalación, puede introducir la clave de licencia haciendo clic en **Activar producto** cuando realice la actualización para acceder a los servidores de actualización de ESET.

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.



Nota

ESET le facilita la clave de licencia tras la compra de ESET Endpoint Antivirus.

La imagen muestra la interfaz de usuario de ESET Endpoint Antivirus. En la parte superior, el título de la ventana es "eset ENDPOINT ANTIVIRUS". A la izquierda hay un menú de navegación con íconos y texto: "ESTADO DE LA PROTECCIÓN", "ANÁLISIS DEL ORDENADOR", "ACTUALIZACIÓN" (destacado), "CONFIGURACIÓN", "HERRAMIENTAS" y "AYUDA Y ASISTENCIA TÉCNICA". El área principal de la derecha está titulada "Actualización" y contiene una lista de estado de las actualizaciones. La primera fila muestra "ESET Endpoint Antivirus" con una marca de verificación verde y "Versión actual: 7.2.2055.0". La segunda fila muestra "Última actualización correcta: 8. 11. 2019 11:24:50" y "Última búsqueda de actualizaciones realizada correctamente: 8. 11. 2019 13:26:00", también con una marca de verificación verde. Debajo de esto hay un enlace azul "Mostrar todos los módulos". En la parte inferior de la ventana, hay dos botones: "Buscar actualizaciones" y "Cambiar frecuencia de actualización".

Actualización	
✓ ESET Endpoint Antivirus	
Versión actual:	7.2.2055.0
✓ Última actualización correcta:	8. 11. 2019 11:24:50
Última búsqueda de actualizaciones realizada correctamente:	8. 11. 2019 13:26:00
Mostrar todos los módulos	

ENJOY SAFER TECHNOLOGY™

Buscar actualizaciones Cambiar frecuencia de actualización

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

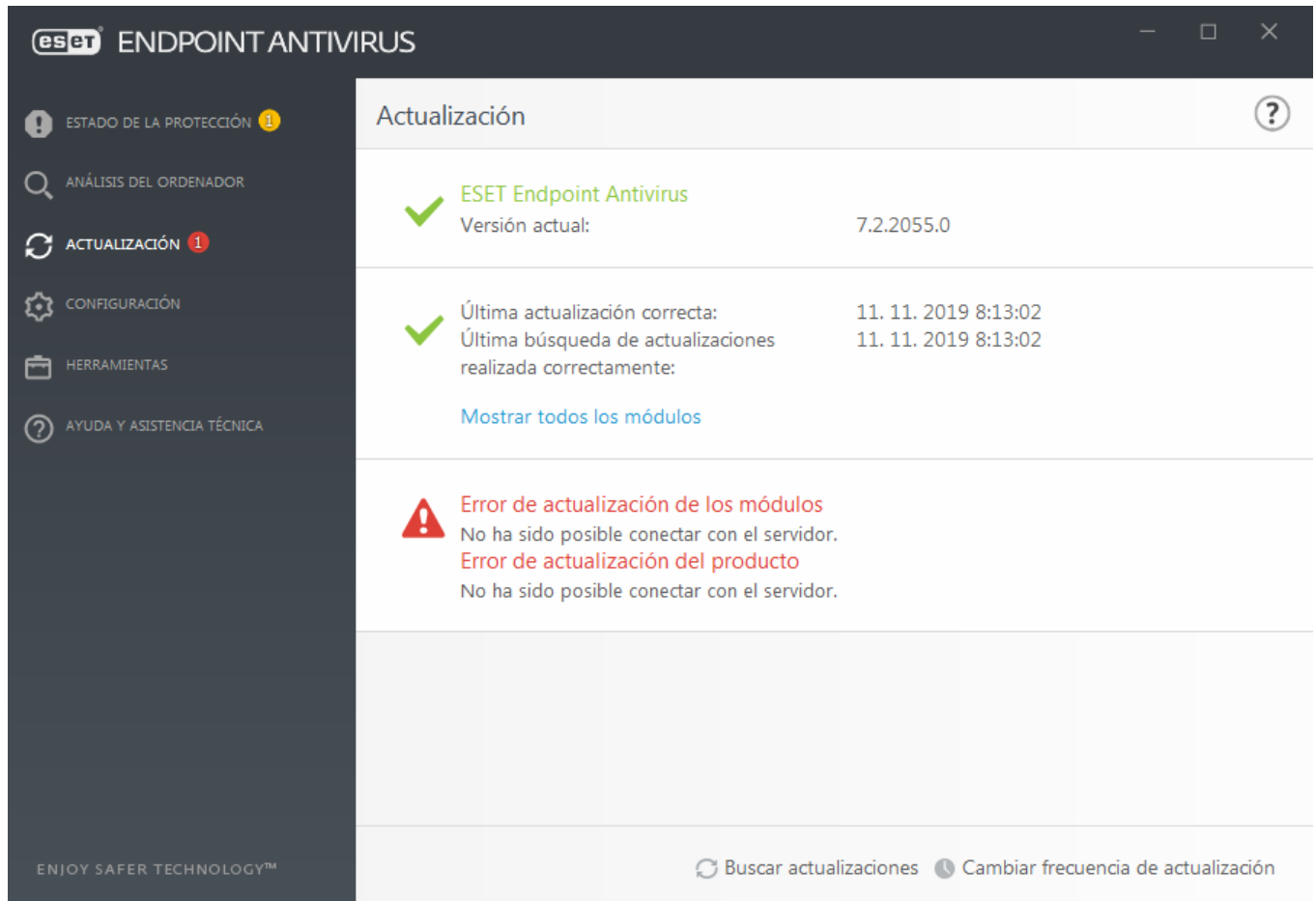
Última actualización correcta: fecha y hora de la última actualización correcta. Asegúrese de que hace referencia a una fecha reciente, lo que significa que el motor de detección está actualizado.

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**.



The screenshot shows the 'Actualización' (Update) window of ESET Endpoint Antivirus. The left sidebar contains navigation options: ESTADO DE LA PROTECCIÓN, ANÁLISIS DEL ORDENADOR, ACTUALIZACIÓN (highlighted with a red '1'), CONFIGURACIÓN, HERRAMIENTAS, and AYUDA Y ASISTENCIA TÉCNICA. The main area displays the following information:

- ESET Endpoint Antivirus**
Versión actual: 7.2.2055.0
- Última actualización correcta: 11. 11. 2019 8:13:02
Última búsqueda de actualizaciones realizada correctamente: 11. 11. 2019 8:13:02
[Mostrar todos los módulos](#)
- Error de actualización de los módulos**
No ha sido posible conectar con el servidor.
Error de actualización del producto
No ha sido posible conectar con el servidor.

At the bottom, there are buttons for 'Buscar actualizaciones' and 'Cambiar frecuencia de actualización'.



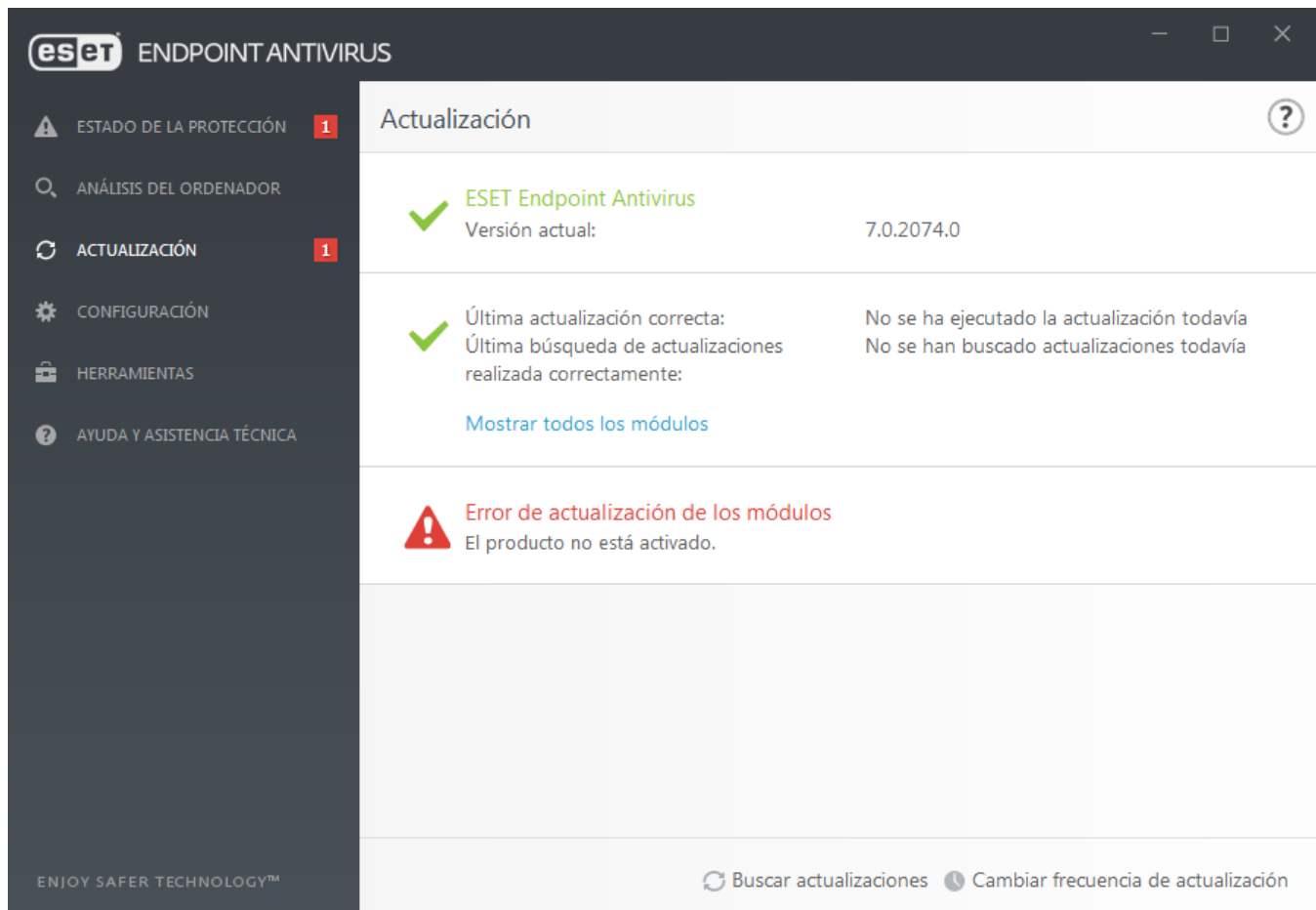
Importante

En circunstancias normales, los módulos se actualizan varias veces al día. En caso contrario, el programa no estará actualizado y será más vulnerable a la infección. Actualice los módulos lo antes posible.

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:** la clave de licencia se ha introducido en la configuración de actualización de forma incorrecta. Recomendamos que compruebe sus datos de autenticación. La ventana Configuración avanzada (haga clic en **Configuración** en el menú principal y, a continuación, en **Configuración avanzada**, o pulse F5 en el teclado) ofrece más opciones de actualización. 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. Consulte a su proveedor de servicios de Internet (ISP) si no tiene una conexión activa a Internet.



Nota
consulte este artículo de la [base de conocimiento de ESET](#) para obtener más información.

Configuración de actualizaciones

Las opciones de configuración de actualizaciones están disponibles en el árbol **Configuración avanzada** (F5), en **Actualización**. En esta sección se especifica la información del origen de la actualización, como los servidores de actualización utilizados y sus datos de autenticación.



Ajuste correcto de la configuración de las actualizaciones

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).

— Básico

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 (antes **Seleccionar notificaciones de actualización recibidas**): haga clic en **Editar** para seleccionar las [notificaciones de aplicaciones](#) que desee que se muestren. Puede elegir para las notificaciones **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**

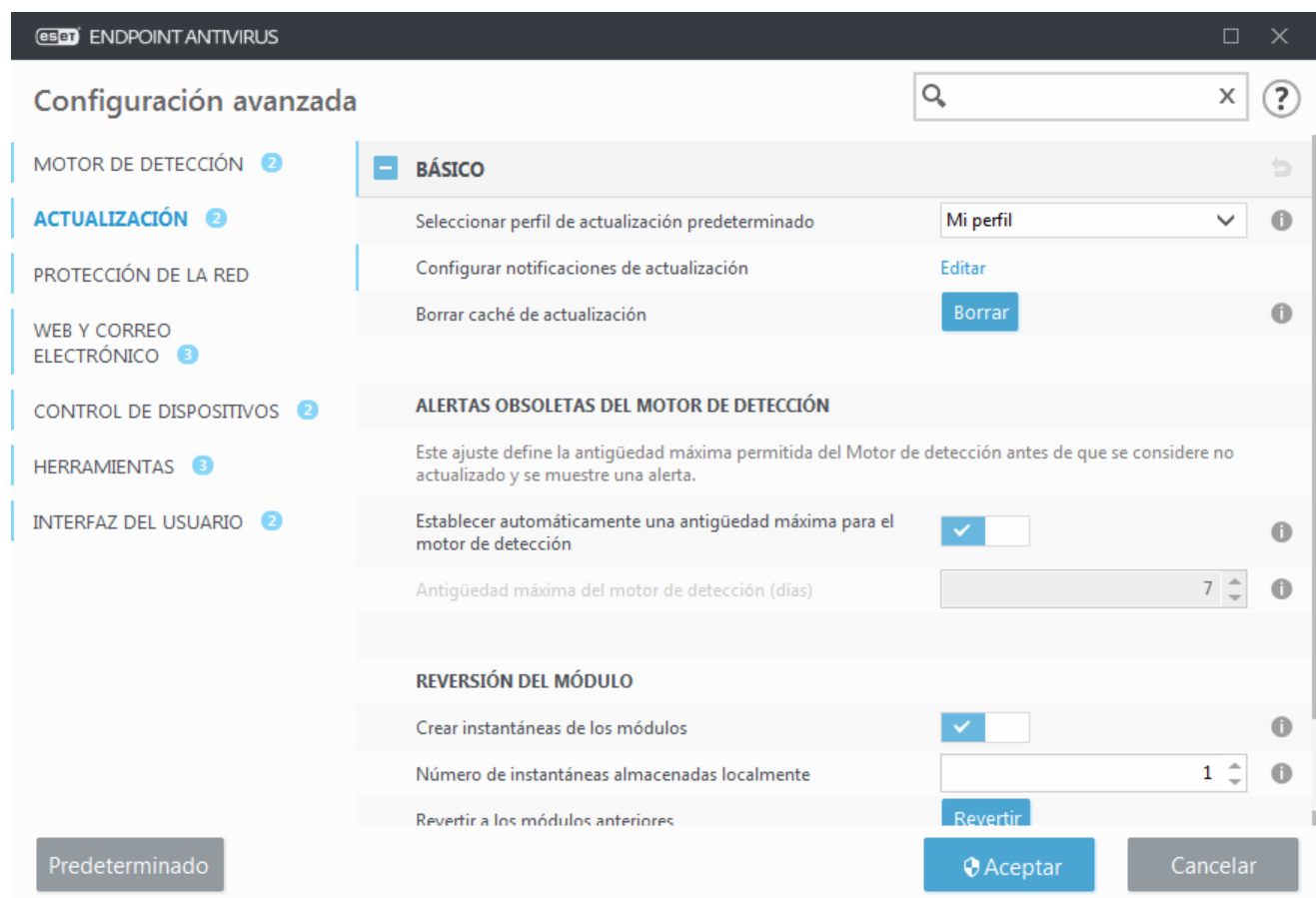
actualización para borrar la memoria caché/los archivos de actualización temporales.

Alertas de Motor de detección obsoleto

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**.

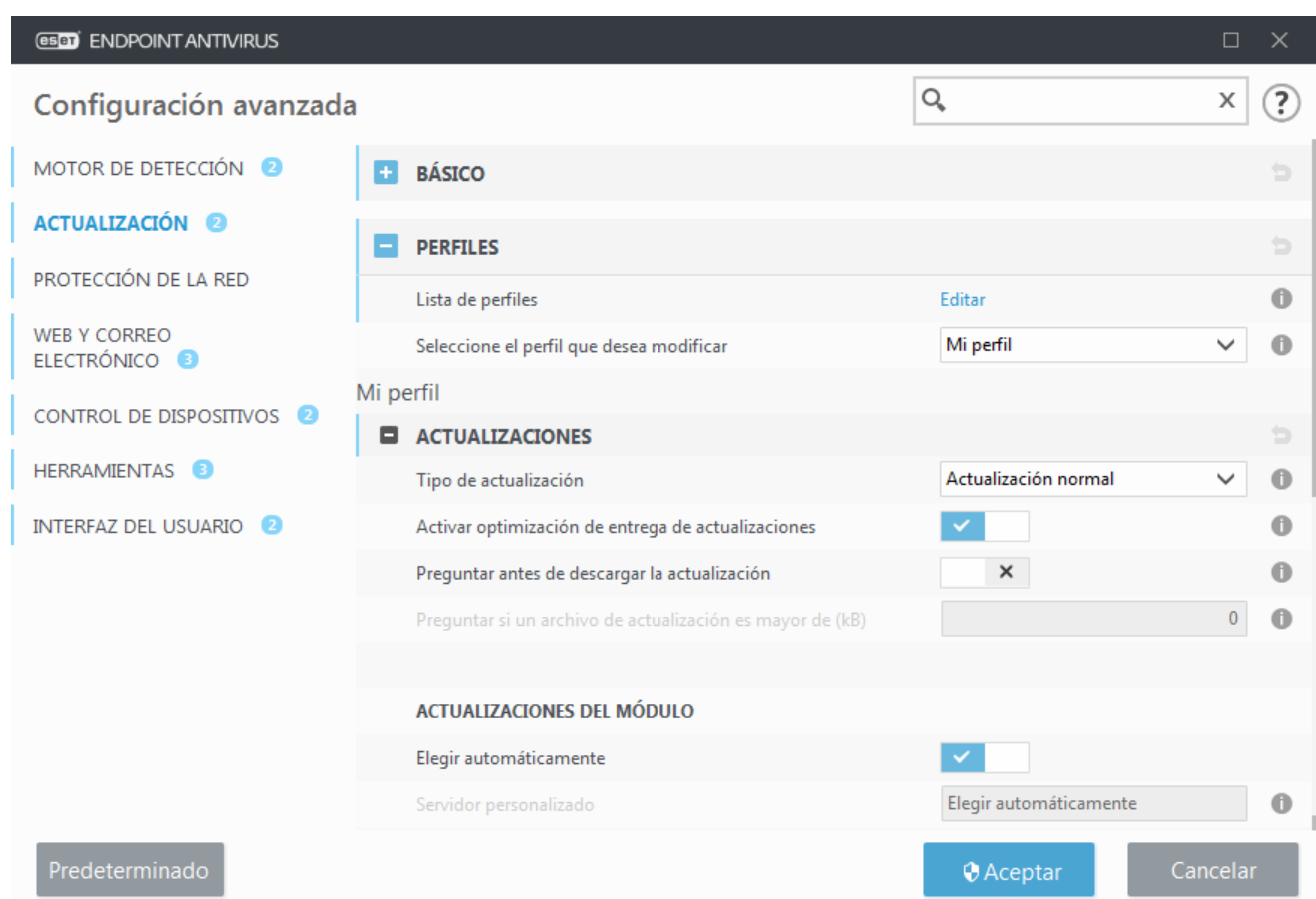
Actualizaciones

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`



HTTP número de puerto del servidor

Número de puerto del servidor HTTP especificado en los ejemplos anteriores depende del puerto en el que su servidor HTTP/HTTPS recibe las conexiones.

Actualización de componentes del programa

Consulte [Actualización de componentes del programa](#).

Mirror de actualización

Consulte [Mirror de actualización](#).

Reversión de actualización

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. 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 activado el conmutador **Crear instantáneas de los módulos**. El campo **Número de instantáneas almacenadas localmente** define el número de instantáneas del motor de detección anteriores almacenadas.

Si hace clic en **Revertir (Configuración avanzada [F5] > Actualización > Básico > Reversión del módulo)**, deberá seleccionar un intervalo de tiempo en el menú desplegable que represente el periodo de tiempo durante el que estarán en pausa las actualizaciones del motor de detección y del módulo del programa.

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.

La versión del motor de detección se degrada a la más antigua disponible y se almacena como instantánea en el sistema de archivos del ordenador local.



Nota

Supongamos que el número 19959 es la versión más reciente del motor de detección. Se almacenan 19958 y 19956 como instantáneas del motor de detección. Observe que 19957 no está disponible porque, por ejemplo, el ordenador estuvo apagado y había disponible una actualización más reciente antes de que se descargara 19957. Si se ha definido 2 en el campo **Número de instantáneas almacenadas localmente** y hace clic en **Revertir**, el motor de detección (incluidos los módulos del programa) se restaurará a la versión número 19956. Este proceso puede tardar un tiempo. Compruebe si la versión del motor de detección se ha degradado en la ventana principal del programa de ESET Endpoint Antivirus en la sección [Actualización](#).

Actualización de componentes del programa

La sección **Actualización de componentes del programa** contiene opciones relacionadas con la actualización de componentes del programa. El programa le permite predefinir su comportamiento cuando está disponible una nueva actualización de componentes del programa.

Las actualizaciones de componentes del programa 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 la instalación de una actualización de componentes del programa, puede que sea necesario reiniciar el ordenador.

En el menú desplegable **Modo de actualización** hay tres opciones disponibles:

- **Preguntar antes de actualizar:** esta es la opción predeterminada. Se le solicitará que confirme o rechace las actualizaciones de componentes del programa cuando estén disponibles.
- **Actualizar automáticamente:** se descargará e instalará una actualización de componentes del programa de manera automática. Recuerde que es posible que tenga que reiniciar el ordenador.
- **No actualizar nunca:** las actualizaciones de componentes del programa no se realizarán. Esta opción es adecuada para las instalaciones de servidores, dado que normalmente los servidores solo se pueden reiniciar cuando se realizan tareas de mantenimiento en ellos.

De forma predeterminado, las actualizaciones de componentes del programa 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 de componentes del programa.

[Definición de un servidor personalizado para las actualizaciones de componentes del programa](#)

1. Defina la ruta de acceso a la actualización de componentes del programa 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 pruebe la presencia de una actualización de componentes del programa con una actualización de ESET Endpoint Antivirus estándar.



Nota

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 estaciones de trabajo y servidores; por ejemplo, el reinicio automático del servidor tras una actualización del programa podría causar daños graves.

Opciones de conexión

Para acceder a las opciones de configuración del servidor proxy de un perfil de actualización concreto, haga clic en **Actualización** en el árbol **Configuración avanzada** (F5) y, a continuación, haga clic en **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 las opciones de configuración del servidor proxy ya especificadas en la sección **Herramientas > Servidor proxy** del árbol de configuración avanzada.

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 Internet Explorer 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.



Advertencia

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.

Mirror de actualización

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 Repositorio local y, después, se distribuyen a todas las estaciones de trabajo para así evitar el riesgo de sobrecargar el tráfico de red. La actualización de estaciones de trabajo cliente desde un servidor Mirror optimiza el equilibrio de carga de la red y ahorra ancho de banda de la conexión a Internet.

Las opciones de configuración del servidor Mirror local están en Configuración avanzada, en **Actualización**. Para acceder a esta sección, pulse **F5** para acceder a Configuración avanzada, haga clic en **Actualización > Perfiles y seleccione la ficha Mirror de actualización**.

Configuración avanzada

- MOTOR DE DETECCIÓN 1
- ACTUALIZACIÓN 4**
- PROTECCIÓN DE LA RED
- WEB Y CORREO ELECTRÓNICO 3
- CONTROL DE DISPOSITIVOS 1
- HERRAMIENTAS 2
- INTERFAZ DEL USUARIO 1

Crear mirror de actualización

☒

ACCESO A LOS ARCHIVOS DE ACTUALIZACIÓN

Carpeta de almacenamiento

C:\ProgramData\ESET\ESET Smart Security Premium\mirror

Borrar

Activar servidor HTTP

☒

Nombre de usuario

Contraseña

ACTUALIZACIÓN DE COMPONENTES DEL PROGRAMA

Archivos

Editar

Actualizar componentes automáticamente

☒

Actualizar componentes ahora

Actualizar

☒ SERVIDOR HTTP

☒ OPCIONES DE CONEXIÓN

Predeterminado

Aceptar

Cancelar

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 y la contraseña deben introducirse con el formato *Dominio/Usuario* o *Grupo de trabajo/Usuario*. No olvide que debe introducir las contraseñas correspondientes.

Actualización de componentes del programa

Archivos: durante la configuración del servidor Mirror puede especificar las versiones de idioma de las actualizaciones que desea descargar. Los idiomas seleccionados deben ser compatibles con el servidor Mirror configurado por el usuario.

Actualizar componentes automáticamente: permite instalar características nuevas y actualizaciones de las

características existentes. La actualización se puede realizar de manera automática, sin la intervención del usuario, o configurar de modo que este reciba una notificación. Después de instalar una actualización de componentes del programa, puede que sea necesario reiniciar el ordenador.

Actualizar componentes ahora: actualiza los componentes del programa a la versión más reciente.

Servidor HTTP

Puerto de servidor: el puerto de servidor predeterminado es el 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 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.



Nota

los datos de autenticación, como el **nombre de usuario** y la **contraseña** sirven para acceder al servidor Proxy. Rellene estos campos únicamente si es necesario introducir un nombre de usuario y una contraseña. Tenga en cuenta que en estos campos no debe introducir su contraseña y nombre de usuario de ESET Endpoint Antivirus, que únicamente debe proporcionar si sabe que es necesaria una contraseña para acceder a Internet a través de un servidor Proxy.

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.

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** y seleccione **Crear mirror de actualización**.

En la sección **Servidor HTTP** de la ficha **Mirror**, puede especificar el **Puerto del servidor** donde el servidor HTTP estará a la escucha, así como el tipo de **autenticación** que utiliza el servidor HTTP. El valor predeterminado del puerto del servidor es **2221**. La opción **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.



Advertencia

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.

SSL para el servidor HTTP

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: **PEM**, **PFX** y **ASN**. 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 en **Integrada** de forma predeterminada, lo que significa que la clave privada forma parte del archivo de cadena de certificados seleccionado.



Nota

Si se realizan varios intentos sin éxito de actualizar el motor de detección 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** 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:

- **Acceda a Configuración avanzada** (F5) y haga clic en **Actualización > Perfiles > Básico**.
- Desactive **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** desactivando **Proporcionar archivos de actualización mediante el servidor HTTP interno**. 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 ESET Endpoint Antivirus **Configuración avanzada** (F5) y haga clic en **Actualización > Perfiles > 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 ESET Endpoint Antivirus y haga clic en **Actualización > Perfiles > Actualizaciones**.
2. Desactive **Elegir automáticamente** junto a **Actualizaciones del módulo** y escriba un nuevo servidor en el campo **Servidor de actualización** con el formato \\UNC\PATH.



Nota

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 ESMC 7 desde el Mirror, establezca el [Servidor de actualizaciones](#) en (según la ubicación raíz de su servidor HTTP):

http://your_server_address/mirror/eset_upd/era6

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 **Actualización de componentes del programa** está activada, no es necesario hacer clic en **Actualizar** porque los archivos se copian en el servidor Repositorio local automáticamente cuando se encuentran disponibles. Consulte [Tipo de actualización](#) para obtener más información acerca de las actualizaciones de los componentes del programa.

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.

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 están activadas de forma predeterminada en ESET Endpoint Antivirus:

- **Actualización automática de rutina**
- **Actualización automática al detectar la conexión por módem**
- **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 [Planificador de tareas](#).

Herramientas

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

Este menú incluye las herramientas siguientes:

- [Archivos de registro](#)
- [Informe de seguridad](#)
- [Procesos en ejecución](#) (si ESET LiveGrid® se ha activado en ESET Endpoint Antivirus)
- [Observar actividad](#)
- [Tareas programadas](#)
- [ESET SysInspector](#)
- [ESET SysRescue Live](#): le redirige al sitio web de ESET SysRescue Live, del que puede descargar la imagen .iso del CD/DVD de ESET SysRescue Live.
- [Cuarentena](#)
- [Enviar muestra para su análisis](#): le permite enviar un archivo sospechoso para que lo analicen en el laboratorio de investigación de ESET. La ventana de diálogo mostrada al hacer clic en esta opción se describe en esta sección.



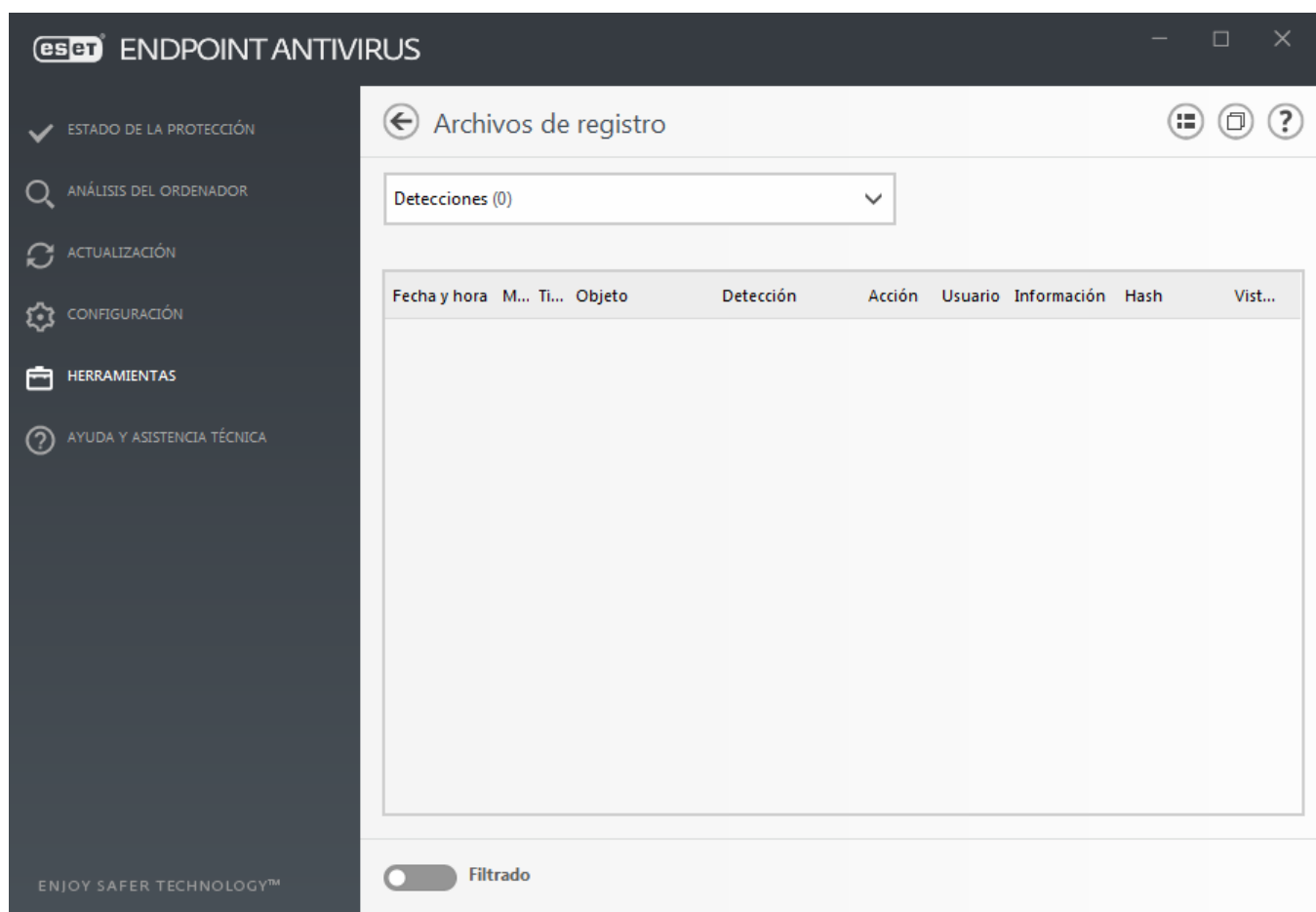
Archivos de registro

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 **Registro**, 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 que estaban bloqueados y a los que no fue posible acceder. 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.
- **Archivos enviados:** contiene registros de archivos enviados a ESET LiveGrid® o [ESET Dynamic Threat Defense](#) 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 [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 del cortafuegos puede ayudarle a detectar a tiempo amenazas del sistema, para así poder evitar el acceso no autorizado al sistema. Para obtener más información sobre ataques de red concretos, 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 que la [Protección del tráfico de Internet](#) ha bloqueado. 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.).
- **Filtrar/Buscar:** después de hacer clic en esta opción, la [ventana Filtrado de registros](#) le permitirá definir los criterios de filtrado para entradas de registro específicas.
- **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.
- **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, la ventana Filtrado de registros le permitirá definir los criterios de filtrado para entradas de registro específicas.
- **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.

Registro de configuración

La configuración de registros de ESET Endpoint Antivirus está disponible en la ventana principal del programa. Haga clic en **Configuración > 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".
- **Crítico:** registra únicamente los errores graves (errores al iniciar la protección antivirus, etc.).



Nota

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. Se eliminan todas las entradas vacías del registro para mejorar el rendimiento y aumentar la velocidad del proceso de 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 Log Collector

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 conocimientos de ESET](#).

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 a partir de ESET Endpoint Antivirus versión 7.1, y es una solución 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.

Archivos de registro

Registros de auditoría (351)

Fecha y hora	Tipo	Descripción	Fuente	Usuario
8.11.2019...	Característica m...	Se ha cambiado el estado de Actualización de...	SISTEMA	NT AUTHORITY\SYSTEM
8.11.2019...	Característica m...	Se ha cambiado el estado de Botnet de Inacti...	SISTEMA	NT AUTHORITY\SYSTEM
8.11.2019...	Característica m...	Se ha cambiado el estado de Protección contr...	SISTEMA	NT AUTHORITY\SYSTEM
8.11.2019...	Característica m...	Se ha cambiado el estado de Control de disp...	SISTEMA	NT AUTHORITY\SYSTEM
8.11.2019...	Característica m...	Se ha cambiado el estado de Anti-Phishing d...	SISTEMA	NT AUTHORITY\SYSTEM
8.11.2019...	Característica m...	Se ha cambiado el estado de Control de disp...	SISTEMA	NT AUTHORITY\SYSTEM
8.11.2019...	Característica m...	Se ha cambiado el estado de Actualización de...	SISTEMA	NT AUTHORITY\SYSTEM
8.11.2019...	Característica m...	Se ha cambiado el estado de Protección de d...	SISTEMA	NT AUTHORITY\SYSTEM
8.11.2019...	Característica m...	Se ha cambiado el estado de Protección del si...	SISTEMA	NT AUTHORITY\SYSTEM
8.11.2019...	Característica m...	Se ha cambiado el estado de Antirransomwar...	SISTEMA	NT AUTHORITY\SYSTEM
8.11.2019...	Característica m...	Se ha cambiado el estado de Bloqueador de ...	SISTEMA	NT AUTHORITY\SYSTEM
8.11.2019...	Característica m...	Se ha cambiado el estado de Análisis avanzad...	SISTEMA	NT AUTHORITY\SYSTEM
8.11.2019...	Característica m...	Se ha cambiado el estado de HIPS de Inactivo ...	SISTEMA	NT AUTHORITY\SYSTEM
8.11.2019...	Característica m...	Se ha cambiado el estado de Botnet de Inacti...	SISTEMA	NT AUTHORITY\SYSTEM
8.11.2019...	Característica m...	Se ha cambiado el estado de Actualización de...	SISTEMA	NT AUTHORITY\SYSTEM
8.11.2019...	Característica m...	Se ha cambiado el estado de Protección contr...	SISTEMA	NT AUTHORITY\SYSTEM

☐ Filtrado

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 ESMC). 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.

Planificador de tareas

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

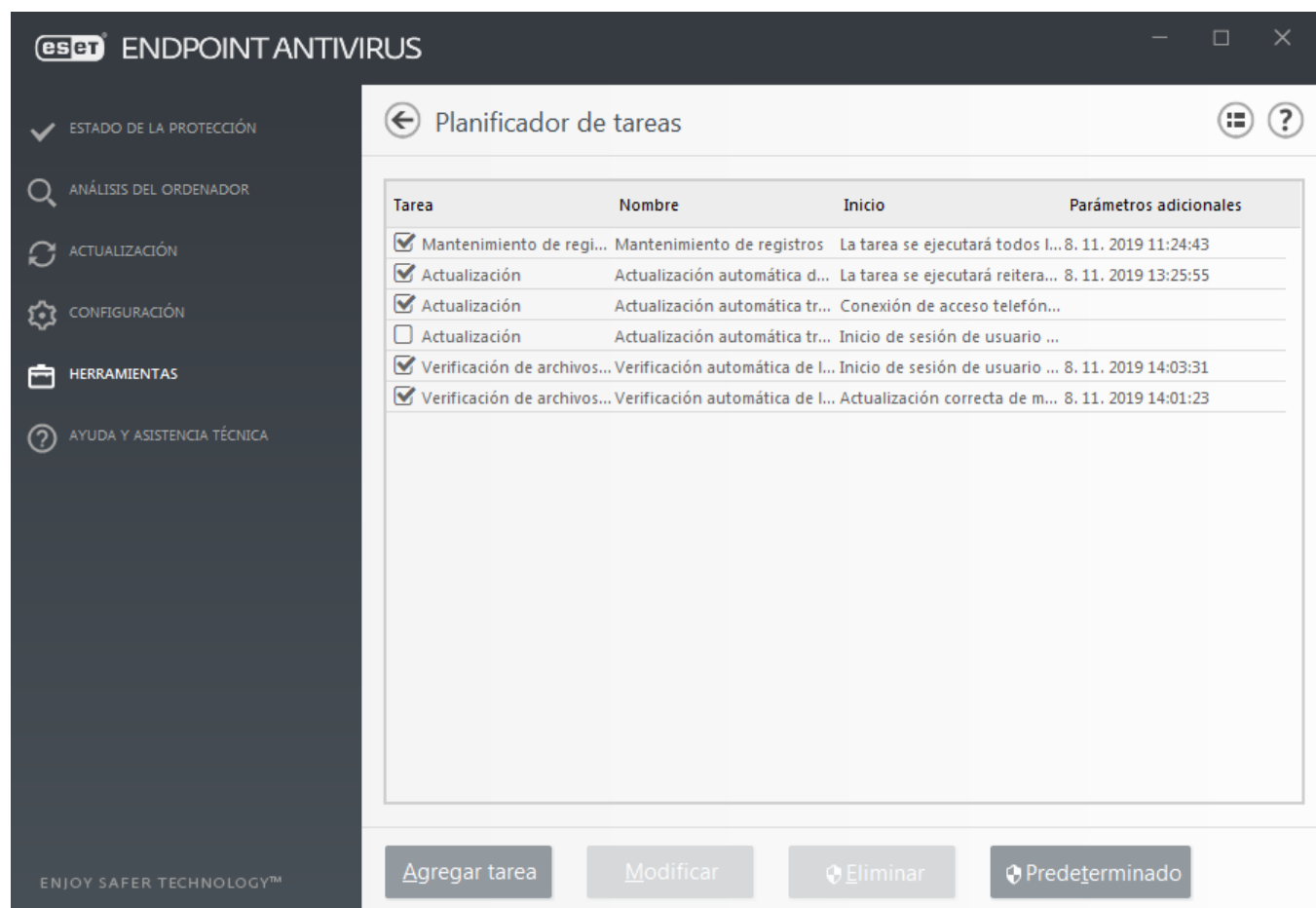
Se puede acceder al Planificador de tareas desde la ventana principal del programa de ESET Endpoint Antivirus haciendo clic en **Herramientas > Planificador de tareas**. El **Planificador de tareas** contiene una lista de todas las tareas programadas y sus propiedades de configuración, como la fecha, 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)

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.Introduzca un nombre para 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 una instantánea de estado del equipo:** crea una instantánea del ordenador de ESET SysInspector, recopila información detallada sobre los componentes del sistema (por ejemplo, controladores y 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**)

Si desea revisar la tarea programada, haga clic con el botón derecho del ratón y, después, haga clic en **Mostrar detalles de la tarea**.

Nombre de tarea

Actualización automática tras el registro del usuario

Tipo de tarea

Actualización

Ejecutar la tarea

El usuario inicie la sesión (una vez cada hora como máximo)

Acción a realizar si la tarea no pudo ser completada en el tiempo especificado

En la siguiente hora programada

Aceptar

Estadísticas de protección

Para ver un gráfico de datos estadísticos relacionados con los módulos de protección de ESET Endpoint Antivirus, haga clic en **Herramientas > Estadísticas de protección**. Seleccione el módulo de protección aplicable en el menú desplegable **Estadísticas** para ver el gráfico y la leyenda correspondientes. Si pasa el ratón por encima de un elemento de la leyenda, solo aparecerán en el gráfico los datos de ese elemento.

Desde ESET Endpoint Antivirus versión 7.1 se ha introducido un nuevo tipo de informe: [Informe de seguridad](#). La sección Estadísticas de protección ya no estará disponible.

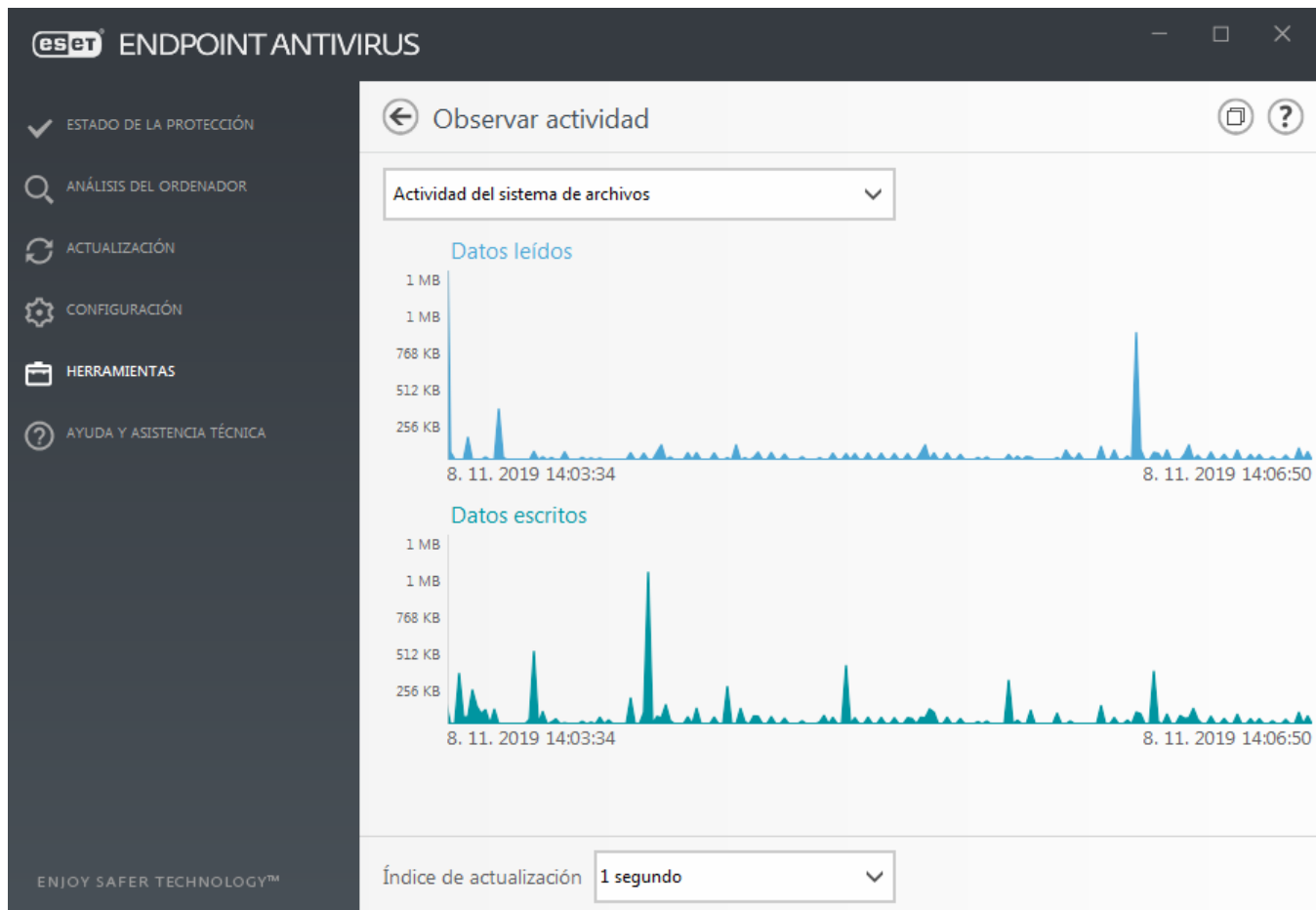
Están disponibles los siguientes gráficos de estadísticas:

- **Protección antivirus y antiespía:** muestra el número de objetos infectados y no infectados
- **Protección del sistema de archivos:** solo muestra objetos que se leyeron o escribieron en el sistema de archivos.
- **Protección del cliente de correo electrónico:** solo muestra objetos que fueron enviados o recibidos por clientes de correo electrónico.
- **Protección del tráfico de Internet y Anti-Phishing:** solo muestra objetos descargados por los navegadores web.

Junto a los gráficos de estadísticas, se muestra el número de objetos analizados, de objetos infectados, de objetos desinfectados y de objetos limpios. Haga clic **Restablecer** para borrar los datos estadísticos o haga clic en **Restablecer todo** para borrar y eliminar todos los datos disponibles.

Observar actividad

Para ver la **Actividad del sistema de archivos** actual en un gráfico, haga clic en **Herramientas > Observar actividad**. En la parte inferior del gráfico hay una línea cronológica que registra la actividad del sistema de archivos en tiempo real en el intervalo de tiempo seleccionado. Si desea cambiar el intervalo de tiempo, realice la selección en el menú desplegable **Índice de actualización**.



Están disponibles las opciones siguientes:

- **Pasar 1 segundo:** el gráfico se actualiza cada segundo y la línea cronológica abarca los últimos 10 minutos.
- **Pasar 1 minuto (últimas 24 horas):** el gráfico se actualiza cada minuto y la línea cronológica abarca las últimas 24 horas.
- **Pasar 1 hora (último mes):** el gráfico se actualiza cada hora y la línea cronológica abarca el último mes.
- **Pasar 1 hora (mes seleccionado):** el gráfico se actualiza cada hora y la línea cronológica abarca los últimos X meses seleccionados.

El eje vertical del **Gráfico de actividad del sistema de archivos** representa la cantidad de datos leídos (color azul) y escritos (color turquesa). Ambos valores se ofrecen en KB (kilobytes), MB o GB. Si pasa el ratón por encima de los datos leídos o escritos en la leyenda disponible debajo del gráfico, el gráfico solo mostrará los datos de ese tipo de actividad.

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 malware. [Consulte también la guía del usuario en línea de ESET SysInspector.](#)

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

- **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 creado. También puede hacer clic con el botón derecho del ratón sobre un archivo de registro determinado y seleccionar **Mostrar** en el menú contextual.
- **Comparar:** compara dos registros existentes.
- **Crear...:** crea un registro nuevo. Espere hasta que ESET SysInspector finalice (el estado del registro se mostrará como Creado) antes de intentar acceder al registro.
- **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).
- **Comparar:** compara dos registros existentes.
- **Crear...:** crea un registro nuevo. Espere hasta que ESET SysInspector finalice (el estado del registro se mostrará como Creado) antes de intentar acceder al registro.
- **Eliminar:** elimina el registro seleccionado.
- **Eliminar todos:** elimina todos los registros.
- **Exportar:** exporta el registro a un archivo .xml o .xml comprimido.

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 en estado salvaje, 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.

Existen tres opciones:

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 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.



Información relacionada

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®, pulse **F5** para acceder a la Configuración avanzada y despliegue **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.

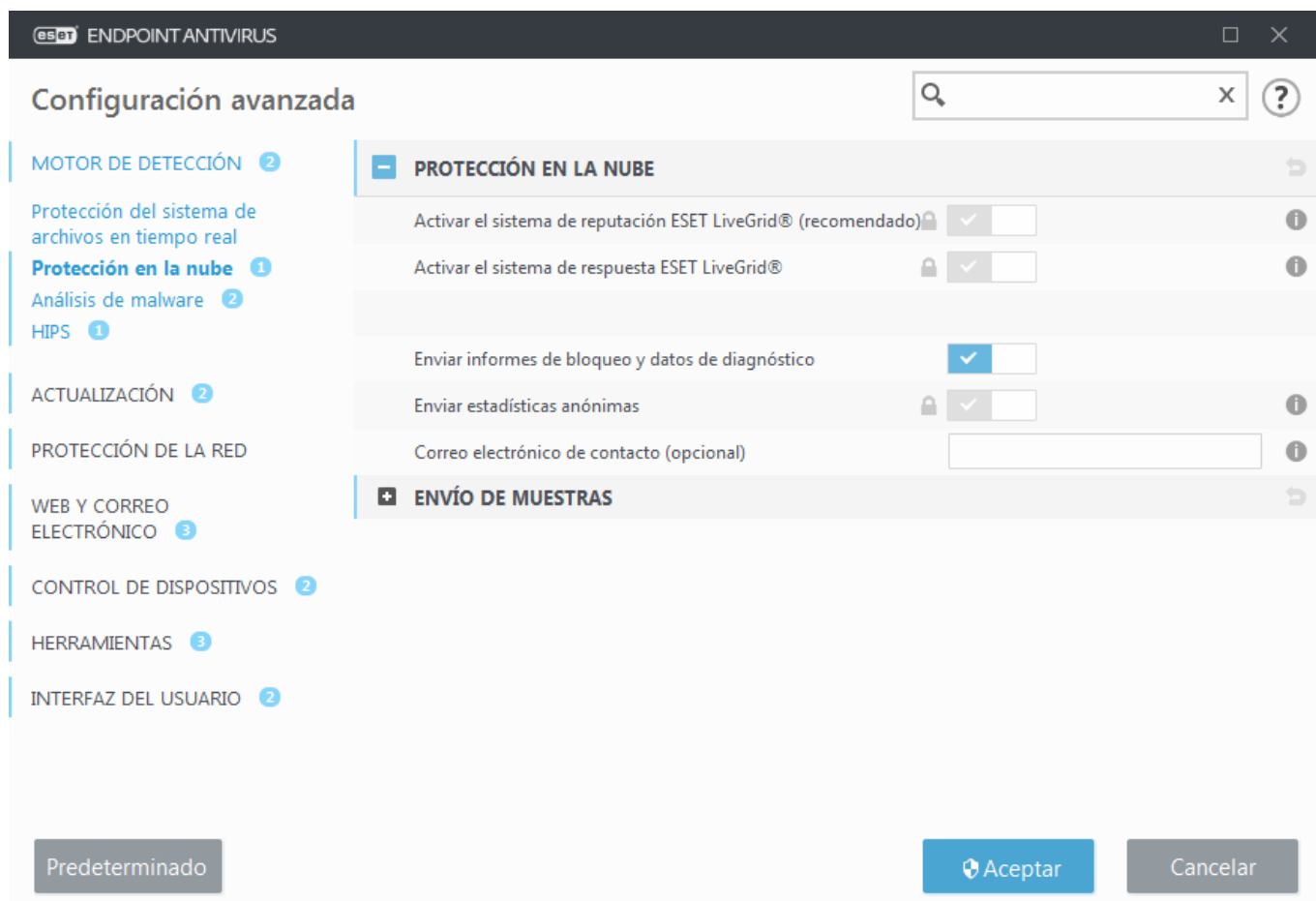
Activar el sistema de respuesta ESET LiveGrid®: envía los datos de envío pertinentes (descritos en la sección **Envío de muestras** a continuación) junto con informes de bloqueo y estadísticas al laboratorio de investigación de ESET para su análisis.

Activar ESET Dynamic Threat Defense (no visible en ESET Endpoint Antivirus): ESET Dynamic Threat Defense es un servicio de pago proporcionado 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. Tenga en cuenta que no recibirá una respuesta de ESET, a no ser que sea necesaria más información.



Envío de muestras

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 en caso de que el motor de detección no las detecte. 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 determinados 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.

ESET Dynamic Threat Defense

Para activar el servicio ESET Dynamic Threat Defense en una máquina cliente con ESMC Web Console, consulte [Configuración de EDTD para ESET Endpoint Antivirus](#).

Si utilizó ESET LiveGrid® anteriormente pero lo desactivó, 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 a los laboratorios de ESET para su análisis, aunque contengan código sospechoso. Los tipos de archivo más habituales (como .doc, etc.) se excluyen de forma predeterminada.



Nota

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

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.

ENDPOINT ANTIVIRUS

ESTADO DE LA PROTECCIÓN

ANÁLISIS DEL ORDENADOR

ACTUALIZACIÓN

CONFIGURACIÓN

HERRAMIENTAS

AYUDA Y ASISTENCIA TÉCNICA

Procesos en ejecución

En esta ventana se muestra una lista de los archivos seleccionados con información adicional de ESET LiveGrid®. Se indica la reputación de cada uno, junto con el número de usuarios y la hora de la primera detección.

Reputación	Proceso	PID	Número de us...	Hora de det...	Nombre de la aplicación
	smss.exe	248		hace 6 meses	Microsoft® Windows® Op...
	csrss.exe	332		hace 7 años	Microsoft® Windows® Op...
	wininit.exe	384		hace 7 años	Microsoft® Windows® Op...
	winlogon.exe	420		hace 7 años	Microsoft® Windows® Op...
	services.exe	476		hace 7 años	Microsoft® Windows® Op...
	lsass.exe	492		hace 6 meses	Microsoft® Windows® Op...
	lsm.exe	508		hace 7 años	Microsoft® Windows® Op...
	svchost.exe	596		hace 7 años	Microsoft® Windows® Op...
	vboxservice.exe	680		hace 6 meses	Oracle VM VirtualBox Guest...

Ruta:
Tamaño:
Descripción:
Empresa:
Versión:
Producto:
Fecha de creación:
Fecha de modificación:

c:\windows\system32\smss.exe
68,0 KB
Windows Session Manager
Microsoft Corporation
6.1.7600.16385 (win7_rtm.090713-1255)
Microsoft® Windows® Operating System
10. 5. 2019 11:09:48
21. 2. 2019 4:34:07

Ocultar detalles

Reputación: generalmente, ESET Endpoint Antivirus y la tecnología ESET LiveGrid® asignan un nivel de riesgo a los objetos (archivos, procesos, claves del registro, etc.). Para ello, utilizan una serie de reglas heurísticas que examinan las características de cada objeto y, después, ponderan el potencial de 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.



Nota

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.



Nota

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.

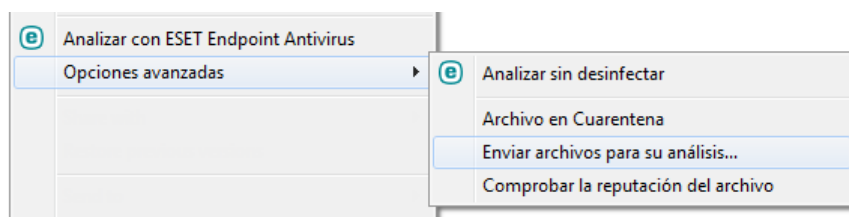
Al hacer clic en una aplicación en la parte inferior, se mostrará la siguiente información en la parte inferior de la ventana:

- **Ruta:** ubicación de una aplicación en el ordenador.
- **Tamaño:** tamaño del archivo en KB (kilobytes) o MB (megabytes).
- **Descripción:** características del archivo de acuerdo con la descripción del sistema operativo.
- **Empresa:** nombre del proveedor o el proceso de la aplicación.
- **Versión:** información sobre el editor de la aplicación.
- **Producto:** nombre de la aplicación o nombre comercial.
- **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.



Nota

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 comprobados: 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.

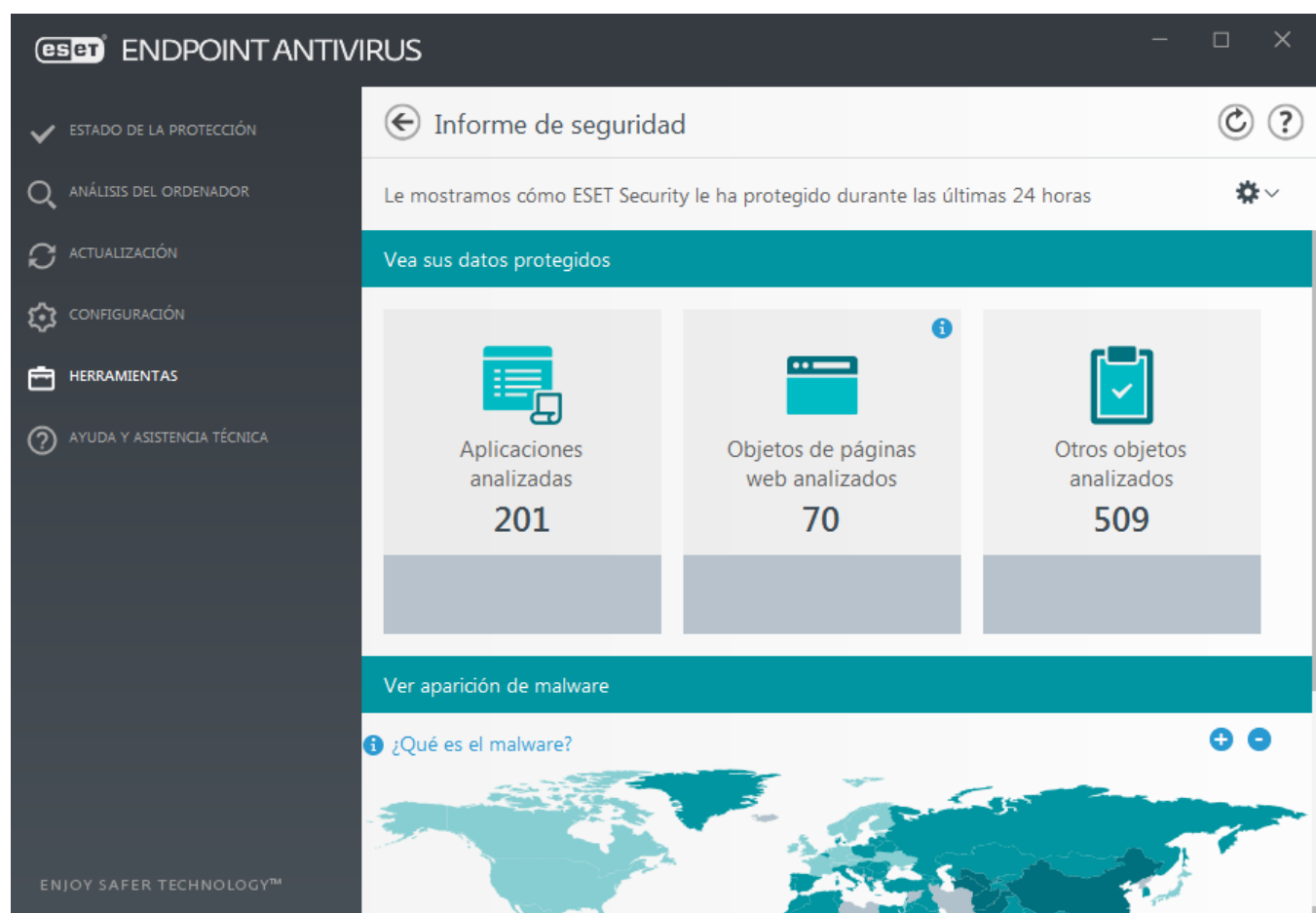
Objetos de página web analizados: muestra el número de objetos de página web analizados.

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.

Debajo de las categorías puede ver la situación de virus real en el mapa del mundo. La presencia de virus en cada país se indica mediante colores (cuanto más oscuro es el color, más alto es el número). Los países de los que no hay datos aparecen atenuados. Coloque el cursor del ratón sobre el país para mostrar datos del país seleccionado. Puede seleccionar un continente y se aplicará zoom automáticamente.

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 anula la selección de la opción **Preguntar antes de restablecer las estadísticas** en **Configuración avanzada > Interfaz de usuario > Cuadros de alertas y mensajes > Mensajes de confirmación**.

ESET SysRescue Live

ESET SysRescue Live es una utilidad gratuita que le permite crear un CD/DVD o una unidad USB de rescate de arranque. Podrá arrancar un ordenador infectado desde un soporte de rescate para analizarlo en busca de malware y limpiar los archivos infectados.

La principal ventaja de ESET SysRescue Live es que se ejecuta de forma independiente del sistema operativo host, pero tiene acceso directo al disco y al sistema de archivos. Gracias a esto, es posible eliminar amenazas que quizá no se podrían suprimir en condiciones de funcionamiento normales (por ejemplo, cuando el sistema operativo se está ejecutando, etc.).

- [Ayuda en línea de ESET SysRescue Live](#)

Envío de muestras para el análisis

Si encuentra un archivo que se comporta de manera sospechosa en su ordenador o un sitio sospechoso en Internet, puede enviarlos al laboratorio de investigación de ESET para que los analicen.



Antes de enviar muestras a ESET

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. Cómo 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: esta dirección de correo electrónico de contacto se envía a ESET junto con los archivos sospechosos y se puede utilizar para contactar con usted en caso de que sea necesaria 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.



Puede que no reciba ninguna respuesta de ESET.

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.



Nota

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 llegó 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.



Nota

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 archivo 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.

Notificaciones

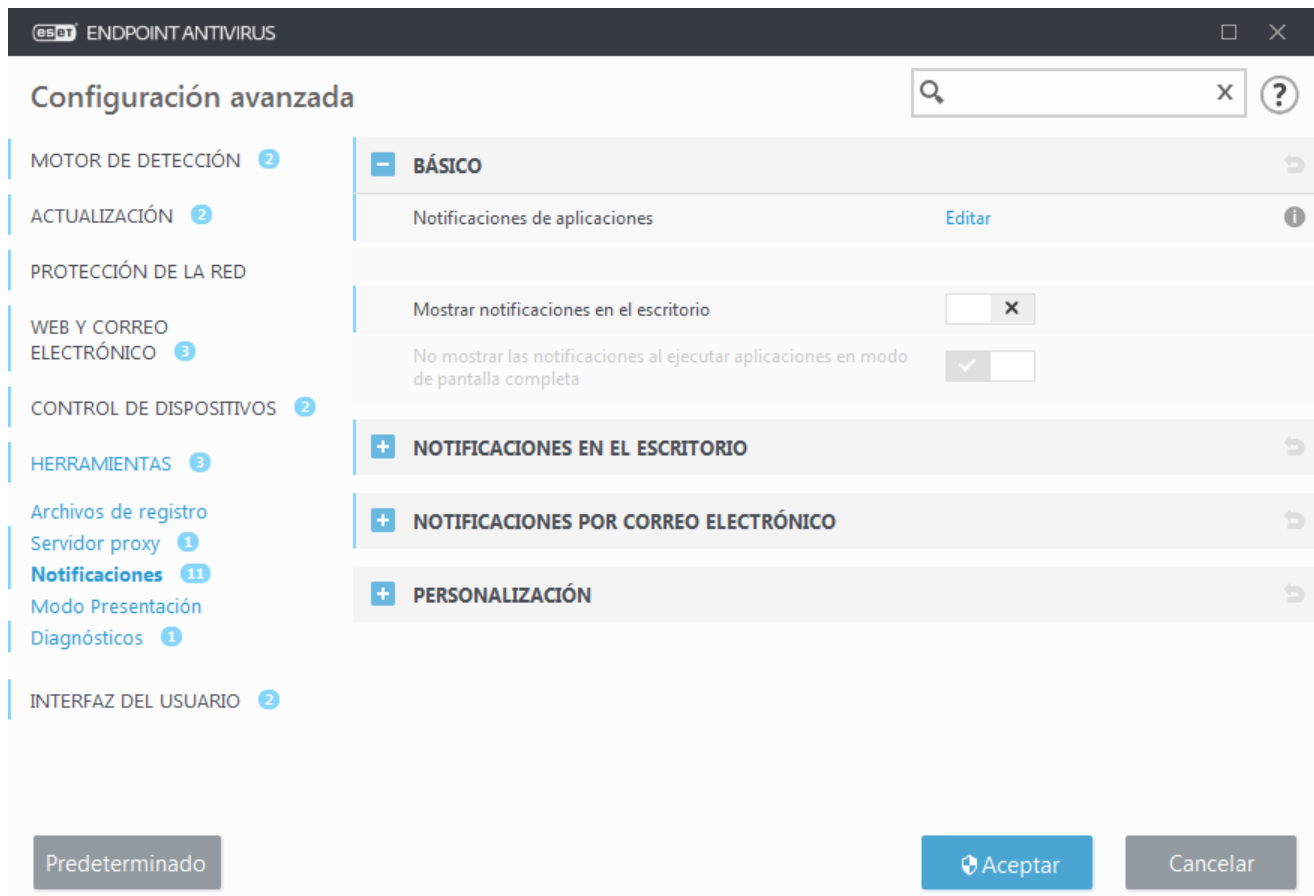
Para controlar la forma en la que ESET Endpoint Antivirus comunica los sucesos al usuario, diríjase a **Configuración avanzada (F5) > Herramientas > Notificaciones**. Esta ventana de configuración le permite configurar los siguientes tipos de notificaciones:

- [Notificaciones de aplicaciones](#): se muestran directamente en la ventana principal del programa.
- [Notificaciones en el escritorio](#): una notificación en el escritorio mostrada como una pequeña ventana emergente junto a la barra de tareas del sistema.
- [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.

Utilice los modificadores correspondientes en la sección **Básico** para ajustar lo siguiente:

Modificador	Predeterminado	Descripción
Mostrar notificaciones en el escritorio	<input checked="" type="checkbox"/>	Desactívelo para ocultar las notificaciones emergentes junto a la barra de tareas del sistema. Se recomienda mantener esta opción activada, para que el producto pueda informarle cuando tiene lugar un suceso nuevo.
No mostrar las notificaciones al...	<input checked="" type="checkbox"/>	Mantenga No mostrar las notificaciones al ejecutar aplicaciones en modo de pantalla completa activado para suprimir todas las notificaciones no interactivas.
Mostrar notificaciones del informe de seguridad	<input type="checkbox"/>	Actívelo para recibir una notificación cuando se genere una versión nueva del Informe de seguridad .
Mostrar notificación de actualización correcta	<input type="checkbox"/>	Actívelo para recibir una notificación cuando el producto actualiza sus componentes y los módulos del motor de detección.
Enviar notificación de suceso por correo electrónico	<input type="checkbox"/>	Actívelo para activar Notificaciones por correo electrónico .

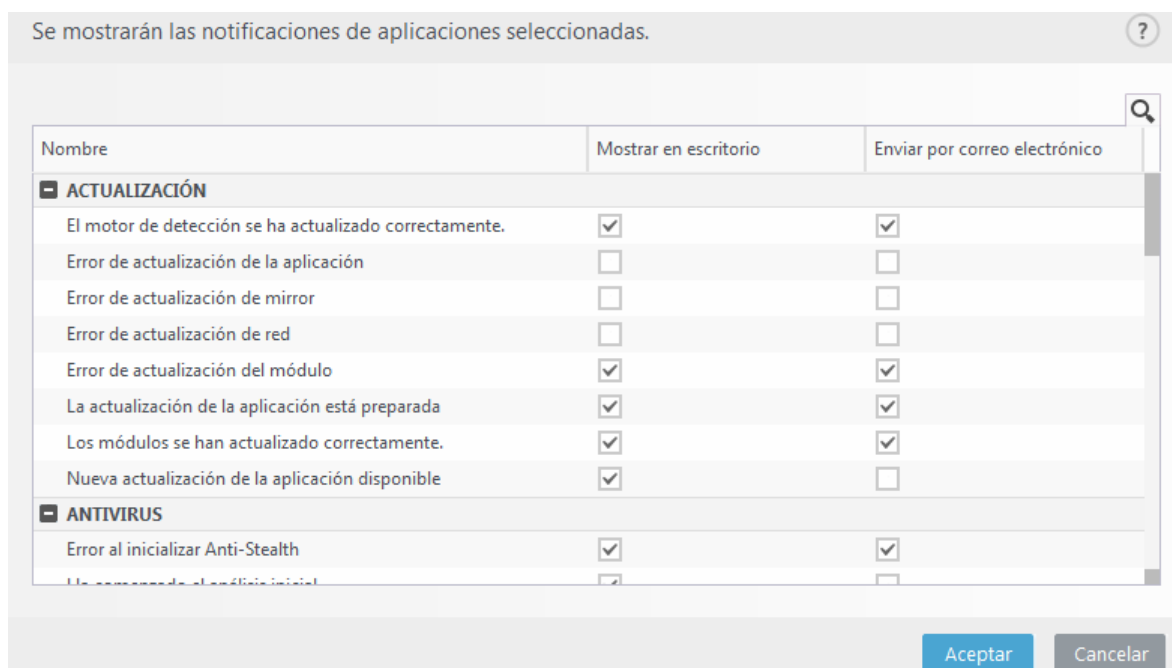
Para activar o desactivar [Notificaciones de aplicaciones](#) concretas, haga clic en **Modificar** junto a **Notificaciones de aplicaciones**.



Notificaciones de aplicaciones

Para ajustar la visibilidad de las notificaciones de la aplicación (mostradas en la esquina inferior derecha de la pantalla), diríjase a **Herramientas > Notificaciones > Básico > Notificaciones de aplicaciones** en el árbol de configuración avanzada de ESET Endpoint Antivirus.

La lista de notificaciones se divide en tres columnas. Los nombres de las notificaciones se ordenan por categoría en la primera columna. Para cambiar la forma en la que el producto notifica de nuevos sucesos en la aplicación, marque las casillas de las columnas correspondientes **Mostrar en el escritorio** y **Enviar por correo electrónico**.



Para configurar los ajustes generales de las notificaciones en el escritorio, por ejemplo durante cuánto tiempo se mostrará un mensaje o el nivel de detalle mínimo de los sucesos que se deben mostrar, consulte [Notificaciones en el escritorio](#) en **Configuración avanzada > Herramientas > Notificaciones**.

Para configurar el formato de los mensajes de correo electrónico y configurar los ajustes del servidor SMTP, consulte [Notificaciones por correo electrónico](#) en **Configuración avanzada > Herramientas > Notificaciones**.

Notificaciones en el escritorio

La notificación en el escritorio se representa mediante una pequeña ventana emergente 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.

La sección **Notificaciones en el escritorio** le permite personalizar el comportamiento de las notificaciones emergentes. Se pueden configurar los siguientes atributos:

Duración: define durante cuánto tiempo se muestra el mensaje de notificación. El valor debe oscilar entre 3 y 30 segundos.

Transparencia: establece la transparencia del mensaje de notificación en porcentaje. El intervalo admitido es desde 0 (sin transparencia) hasta 80 (transparencia muy alta).

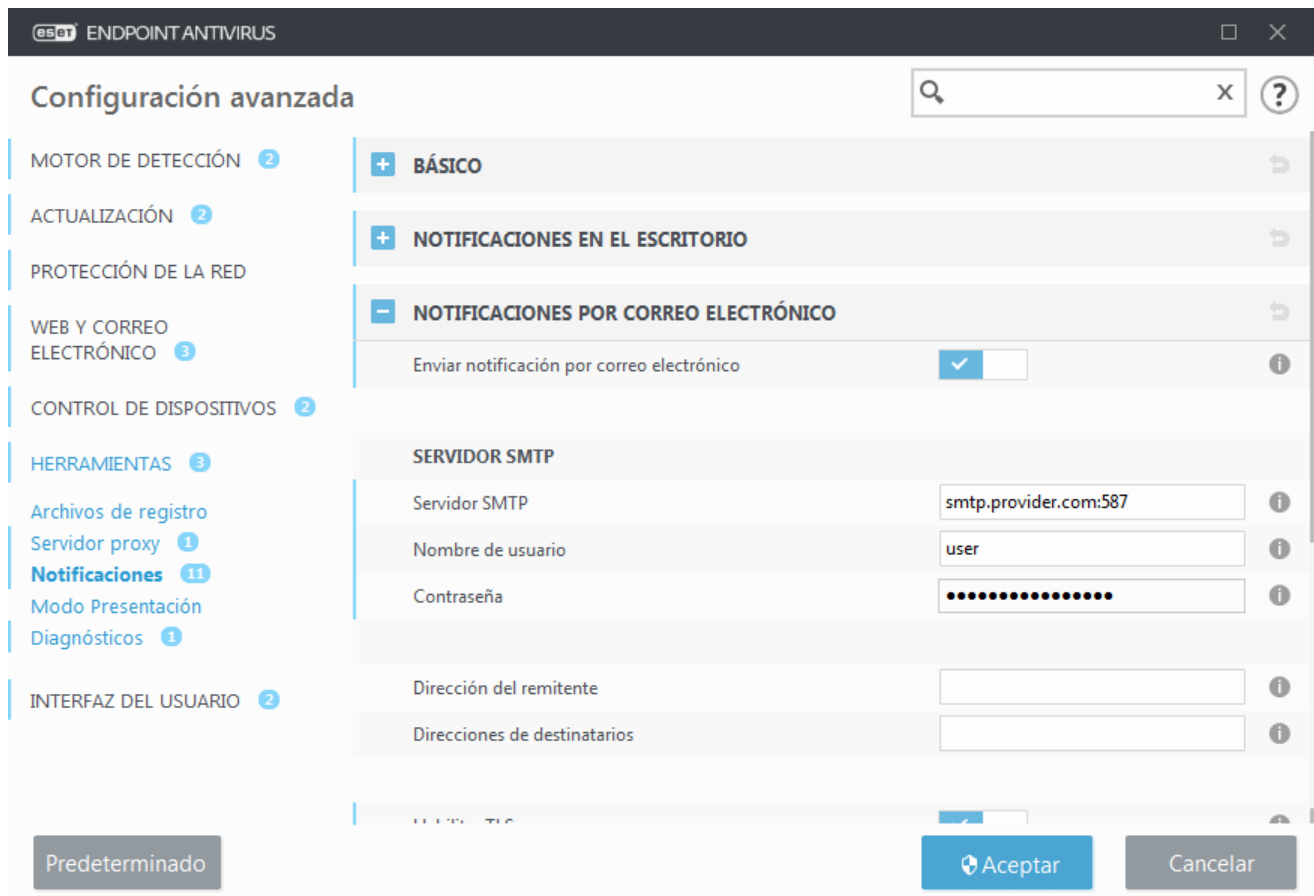
Nivel mínimo de detalle de los sucesos a mostrar: en el menú desplegable puede seleccionar el nivel de gravedad inicial de las notificaciones que se mostrarán:

- **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 los errores graves y los mensajes de advertencia (la tecnología Anti-Stealth no está funcionando adecuadamente o el proceso de actualización ha fallado).
- **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: escriba el nombre completo de las cuentas de los usuarios que podrán recibir notificaciones en el escritorio. Por ejemplo, si usa el ordenador con una cuenta que no sea la de administrador y quiere seguir recibiendo información sobre nuevos sucesos del producto.

Notificaciones por correo electrónico

ESET Endpoint Antivirus puede enviar correos electrónicos de forma automática si se produce un suceso con el nivel de detalle seleccionado. Active **Enviar notificaciones de sucesos por correo electrónico** en la sección [Básico](#) para activar las notificaciones por correo electrónico.



Servidor SMTP

Servidor SMTP: el servidor SMTP que se utiliza para enviar notificaciones (por ejemplo, *smtp.provider.com:587*, el puerto predeterminado es 25).



Nota

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.

Configuración de 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 los errores graves y los mensajes de advertencia (la tecnología Anti-Stealth no está funcionando adecuadamente o el proceso de actualización ha fallado).
- **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).

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 numerosos 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.

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.

Para alertar sobre amenazas: los mensajes de notificación y alerta de amenazas tienen un formato predefinido de forma predeterminada. 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 puede 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.

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.

Amenazas

Active **No cerrar las notificaciones de malware automáticamente** para mantener las notificaciones de malware en pantalla hasta que se cierren manualmente.

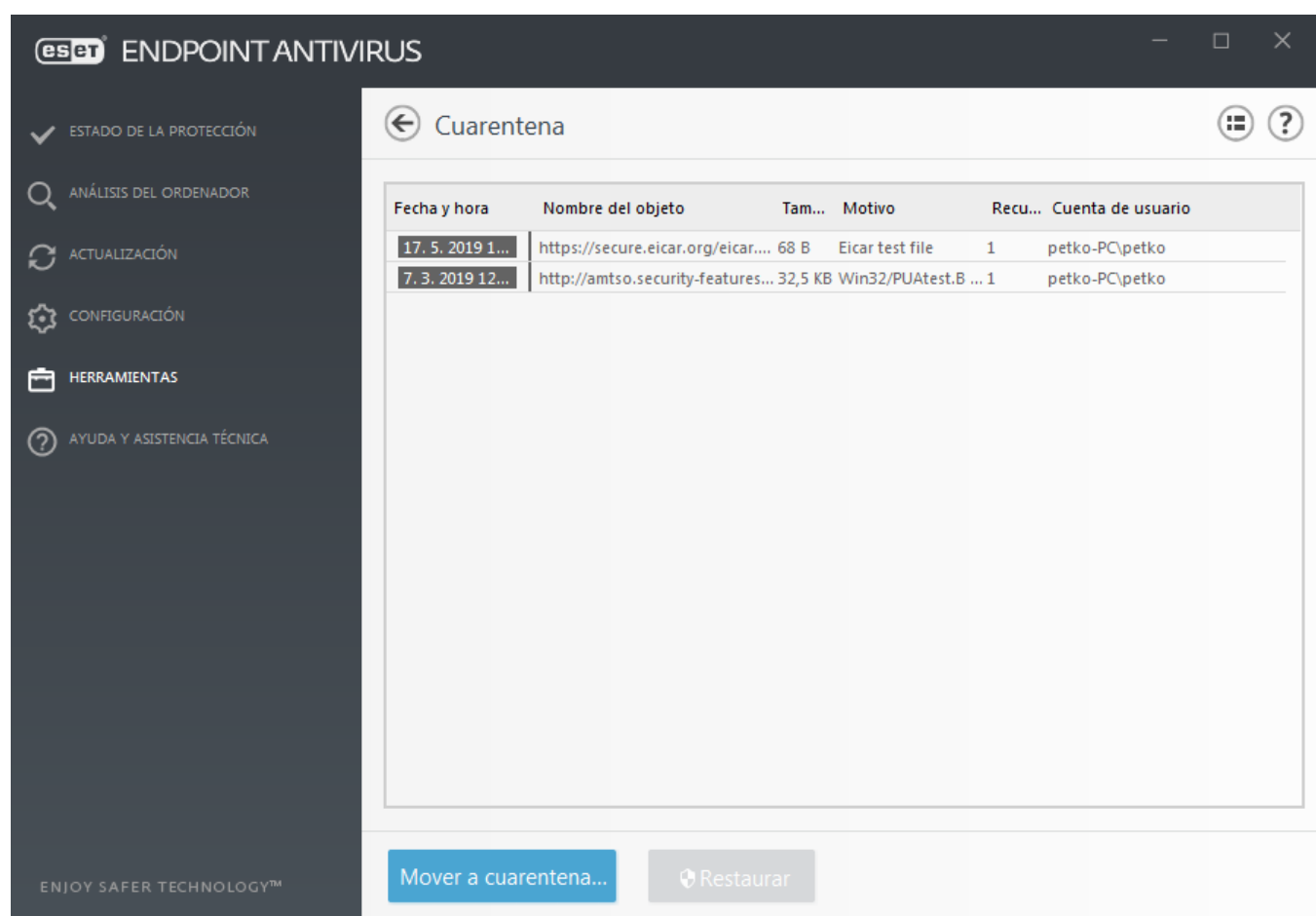
Desactive **Usar mensaje predeterminado** e introduzca su propio mensaje en el campo **Mensaje de notificación de amenaza** para utilizar mensajes de notificación personalizados.

Cuarentena

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

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

Puede poner en cuarentena cualquier archivo, o también puede utilizar la función de arrastrar y colocar para poner en cuarentena un archivo manualmente si hace clic en el archivo, desplaza el cursor del ratón hasta la zona marcada mientras mantiene pulsado el botón del ratón y, a continuación, lo suelta. Así, la aplicación pasa al primer plano. Esto es recomendable si el comportamiento de un archivo es sospechoso, pero el escáner antivirus no detecta dicho archivo. Los archivos en cuarentena se pueden enviar al laboratorio de investigación de ESET para su análisis.



Los archivos almacenados en la carpeta de cuarentena se pueden ver en una tabla que muestra la fecha y la hora en las que se pusieron en cuarentena, la ruta de acceso de la ubicación original del archivo infectado, su tamaño en bytes, el motivo (por ejemplo, objeto agregado por el usuario) y el número de amenazas detectadas.

Poner archivos en cuarentena

ESET Endpoint Antivirus pone los archivos eliminados en cuarentena automáticamente (si no ha desactivado esta opción en la ventana de alerta). Si lo desea, puede poner en cuarentena cualquier archivo sospechoso de forma manual haciendo clic en **Mover a cuarentena**. El archivo original se quitará de su ubicación original. El menú contextual también se puede utilizar con este fin: haga clic con el botón derecho en la ventana **Cuarentena** y seleccione **Archivo en cuarentena**.

Restauración de archivos de cuarentena

Los archivos puestos en cuarentena se pueden restaurar a su ubicación original. Si desea restaurar un archivo puesto en cuarentena, haga clic en él con el botón derecho del ratón en la ventana Cuarentena y seleccione **Restaurar** en el menú contextual. Si el archivo está marcado como [aplicación potencialmente no deseada](#), también estará disponible la opción **Restaurar y excluir del análisis**. El menú contextual también contiene la opción **Restaurar a...**, que le permite restaurar archivos en una ubicación distinta a la original de la cual se eliminaron.

Eliminación de la 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. Es posible seleccionar varios elementos y eliminarlos al mismo tiempo.



Nota

Si el programa ha puesto en cuarentena un archivo no dañino por error, [excluya el archivo del análisis](#) después de restaurarlo y envíelo al servicio de soporte técnico de ESET.

Envío de un archivo de cuarentena

Si ha copiado en cuarentena un archivo sospechoso que el programa no ha detectado o si se ha evaluado incorrectamente un archivo como amenaza y, consecuentemente, se ha copiado a cuarentena, envíe el archivo al laboratorio de virus de ESET. Para enviar un archivo de cuarentena, haga clic con el botón derecho del ratón en el archivo y seleccione **Enviar para su análisis** en el menú contextual.

Servidor Proxy

En las redes LAN de gran tamaño, un servidor proxy puede mediar en la comunicación entre el ordenador e Internet. Si se usa esta configuración se deberán definir los siguientes parámetros. De lo contrario, el programa no se podrá actualizar de manera automática. En ESET Endpoint Antivirus, el servidor proxy se puede configurar en dos secciones diferentes del árbol de Configuración avanzada.

En primer lugar, se puede configurar en **Configuración avanzada**, bajo **Herramientas > 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 del servidor proxy en este nivel, seleccione **Usar servidor proxy** y especifique la dirección del servidor proxy en el campo **Servidor proxy** y su número de **Puerto**.

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. Se copiarán los parámetros especificados en las opciones de Internet de Internet Explorer o Google Chrome.



Nota

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 de actualizaciones (**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 al perfil de actualización dado y se recomienda para ordenadores portátiles que suelen recibir actualizaciones del motor de detección de ubicaciones remotas. Para obtener más información sobre este ajuste,

consulte [Configuración avanzada de actualizaciones](#).

Configuración avanzada

MOTOR DE DETECCIÓN 1

ACTUALIZACIÓN 4

PROTECCIÓN DE LA RED

WEB Y CORREO ELECTRÓNICO 3

CONTROL DE DISPOSITIVOS 1

HERRAMIENTAS 3

Archivos de registro

Servidor proxy 1

Notificaciones por correo electrónico 3

Modo de presentación

Diagnósticos

INTERFAZ DEL USUARIO 1

SERVIDOR PROXY

Usar servidor proxy

Servidor proxy

Puerto

El servidor proxy requiere autenticación

Nombre de usuario

Contraseña

Detectar el servidor proxy

Usar conexión directa si el proxy no está disponible

3128

Detectar

Predeterminado

Aceptar

Cancelar

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.

Intervalos de tiempo

Nombre

Descripción

Work time

Weekdays 8:00-17:00

Off-work

Evenings & weekends

Agregar

Editar

Eliminar

Aceptar

Cancelar

152

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 Editor de reglas de control de dispositivos](#).

Microsoft Windows Update

La característica Windows Update es un componente importante de protección de 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.

Intervalo de comprobación de la licencia

ESET Endpoint Antivirus necesita conectarse a los servidores de ESET de manera automática. Para cambiar este ajuste, diríjase a **Configuración avanzada (F5) > Herramientas > Licencia**. De forma predeterminada, **Intervalo de comprobación** se ajusta en **Automático** y el servidor de licencias de ESET comprueba el producto varias veces cada hora. Si el tráfico de red aumenta, cambie el ajuste 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.



Importante

Si el ajuste **Intervalo de comprobación** está ajustado en **Limitado**, todos los cambios relacionados con la licencia efectuados mediante ESET Business Account/ESET MSP Administrator pueden tardar hasta un día en aplicarse a la configuración de ESET Endpoint Antivirus.

Interfaz de usuario

En la sección **Interfaz de usuario** es posible configurar el comportamiento de la interfaz gráfica de usuario (GUI) del programa.

La herramienta [Elementos de la interfaz del usuario](#) le permite ajustar el aspecto visual del programa y los efectos utilizados.

Si desea disponer del máximo nivel de seguridad del software de seguridad, utilice la herramienta [Configuración de acceso](#) para impedir los cambios no autorizados.

Configurando [Alertas y cuadros de mensajes](#) y [Notificaciones](#) puede cambiar el comportamiento de las alertas de detección y de las notificaciones del sistema. Pueden personalizarse según sus necesidades.

Si elige la opción de no mostrar algunas notificaciones, estas se mostrarán en el área **Elementos de la interfaz del usuario > Estados de la aplicación**. Aquí puede comprobar su estado o, si lo desea, impedir la visualización de estas notificaciones.

La opción [Integración en el menú contextual](#) aparece al hacer clic con el botón derecho en el objeto seleccionado. Utilice esta herramienta para integrar elementos de control de ESET Endpoint Antivirus en el menú contextual.

[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 **Interfaz de usuario > Elementos de la interfaz del usuario** del árbol de configuración avanzada de ESET Endpoint Antivirus.

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.



Nota

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 Security Management Center utilizando una directiva.

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.

Estados

Estados de la aplicación: haga clic en el botón **Editar** para administrar (desactivar) los estados que se muestran en el menú **Estado de protección** del menú principal.

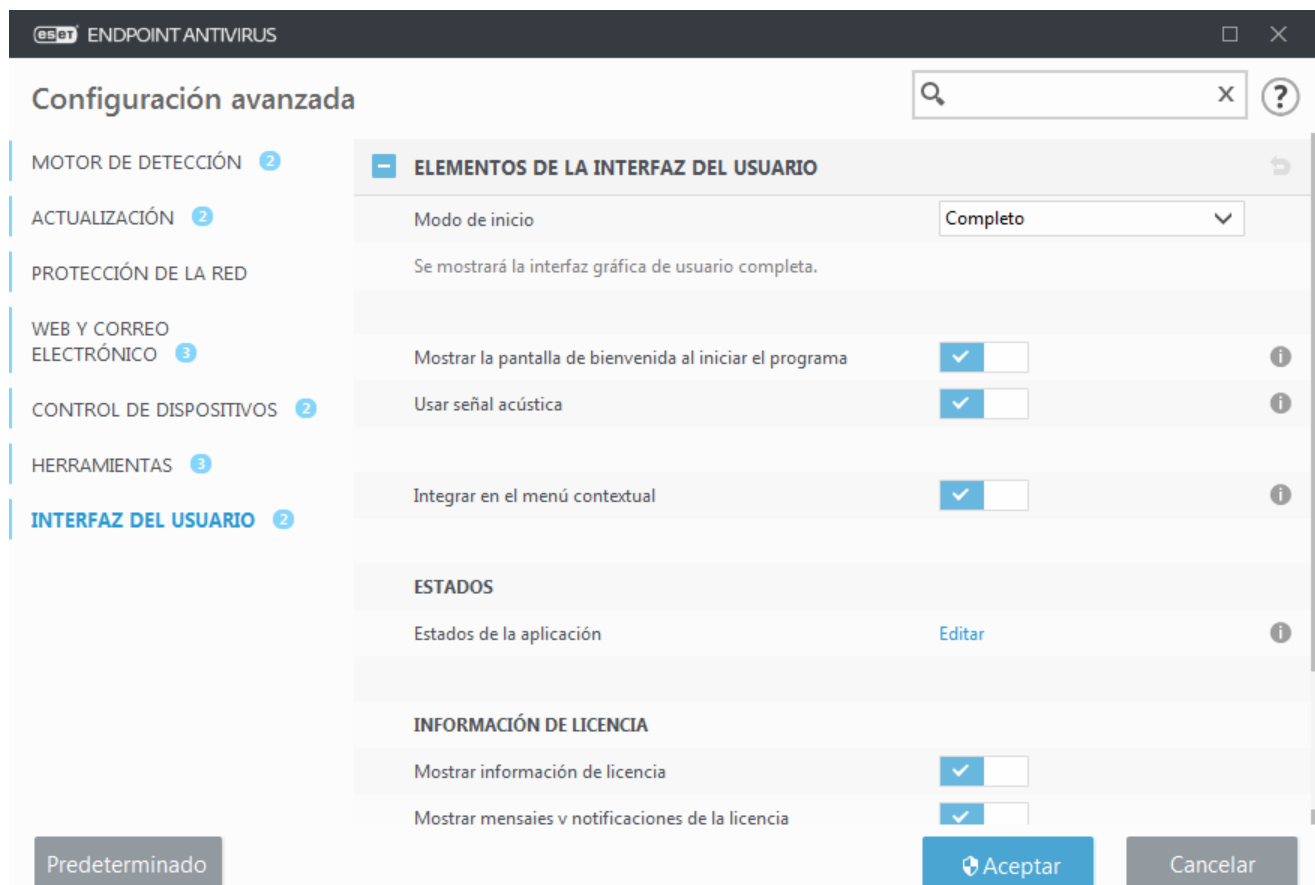
Información de licencia

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**.

Mostrar mensajes y notificaciones de la licencia: cuando esta opción está desactivada, las notificaciones y los mensajes solo se mostrarán cuando la licencia caduque.



Nota
en las instancias de ESET Endpoint Antivirus activadas con licencia MSP, los ajustes de información de la licencia se aplican pero no son accesibles.



Estados de la aplicación

Para ajustar los estados en el producto en el primer panel de ESET Endpoint Antivirus, diríjase a **Interfaz de usuario > Elementos de la interfaz de usuario > Estados de la aplicación** en el árbol de configuración avanzada de ESET Endpoint Antivirus.

Se mostrarán los estados de aplicación seleccionados ?

Q

Nombre	Mostrar
ACTUALIZACIÓN	
Actualización disponible	<input checked="" type="checkbox"/>
Configuración de actualización incorrecta	<input checked="" type="checkbox"/>
El Motor de detección no está actualizado	<input checked="" type="checkbox"/>
Error de actualización de los módulos	<input checked="" type="checkbox"/>
Error de actualización de los módulos (problema de conexión)	<input checked="" type="checkbox"/>
La actualización del módulo se ha suspendido temporalmente	<input checked="" type="checkbox"/>
No hay actualizaciones regulares programadas	<input checked="" type="checkbox"/>
ANTIVIRUS	
Anti-Stealth está desactivado	<input checked="" type="checkbox"/>
Anti-Stealth no está operativo	<input checked="" type="checkbox"/>
La protección antivirus no está operativa	<input checked="" type="checkbox"/>

Aceptar
Cancelar

Active o desactive los estados de aplicación que se mostrarán o no. Por ejemplo, cuando pone en pausa la protección antivirus y antiespía o cuando activa el modo de presentación. El estado de una aplicación también se muestra cuando no se ha activado el producto o si la licencia ha caducado. Este ajuste puede modificarse a través de [Políticas de ESET Security Management Center](#).

Configuración de acceso

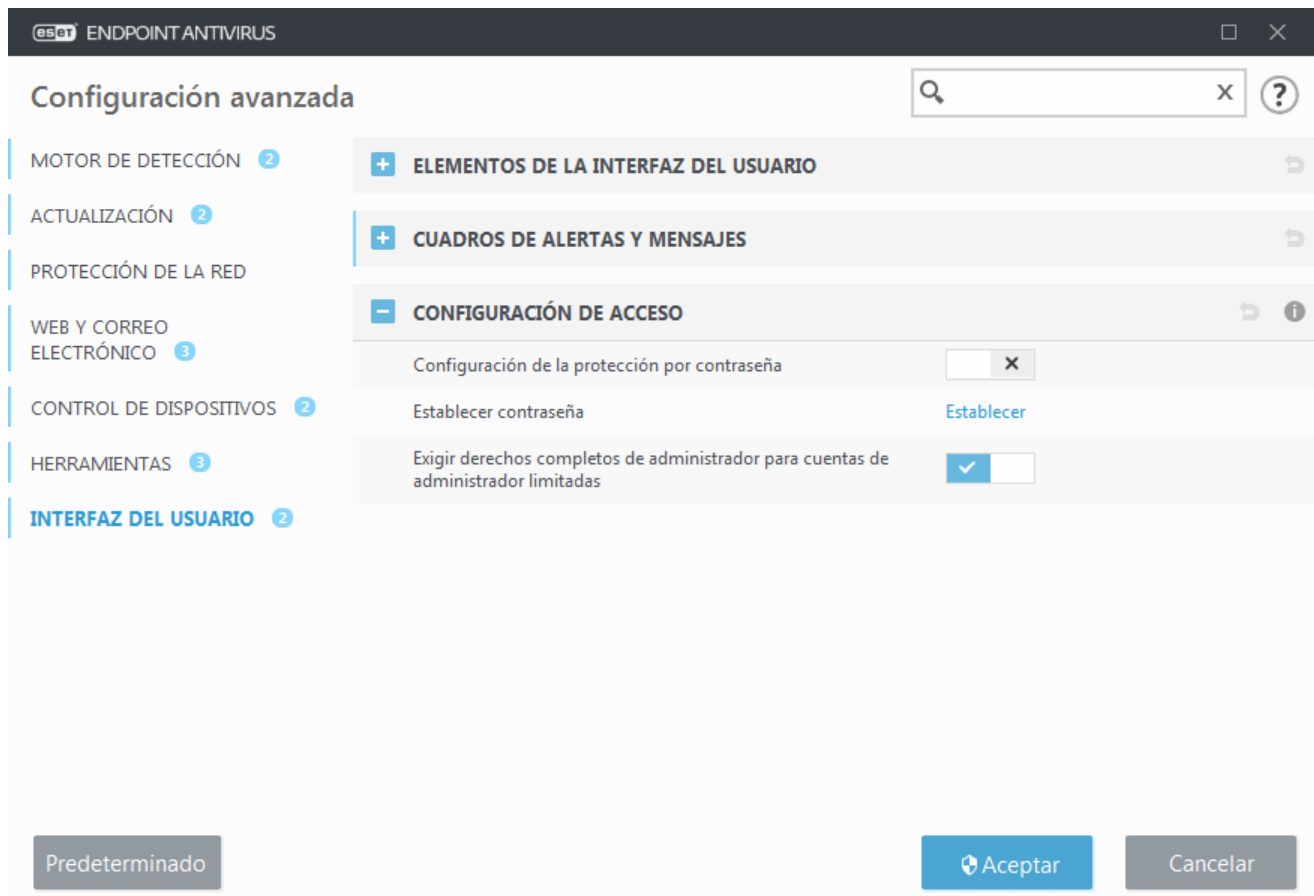
Para ofrecer la máxima seguridad a su sistema, es esencial que ESET Endpoint Antivirus se haya configurado correctamente. Una configuración incorrecta puede provocar la pérdida de datos importantes. Para evitar modificaciones no autorizadas, los parámetros de configuración de ESET Endpoint Antivirus se pueden proteger mediante 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](#).

No administrado

La configuración para la protección con contraseña se encuentra en **Configuración avanzada** (F5) en **Interfaz del usuario > Configuración del acceso**.



Configuración de la protección por contraseña: indique la configuración de la contraseña. Haga clic para abrir la ventana de configuración de contraseña.

Para configurar o cambiar una contraseña para proteger los parámetros de configuración, haga clic en **Definir**.

Exigir derechos completos de administrador para cuentas de administrador limitadas: mantenga esta opción activa para solicitar al usuario actual (si no tiene derechos de administrador) que introduzca el nombre de usuario y la contraseña de administrador al modificar determinados parámetros del sistema (parecido al UAC en Windows Vista). Estas modificaciones incluyen la desactivación de los módulos de protección.

Solo para Windows XP:

Exigir derechos de administrador (sistema sin soporte UAC): active esta opción para que ESET Endpoint Antivirus solicite las credenciales de administrador.

Contraseña de Configuración avanzada

Debe definir una nueva contraseña para proteger los parámetros de configuración de ESET Endpoint Antivirus con el fin de evitar modificaciones no autorizadas.

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 olvida su contraseña, puede restaurar el acceso a la configuración avanzada.

- [Restaurar con el método "Restaurar contraseña" \(versión 7.1 y posteriores\)](#)
- [Restaurar con la herramienta de desbloqueo de ESET \(versión 7.0 y anteriores\)](#)

[Haga clic aquí si ha olvidado su clave de licencia emitida por ESET](#), la fecha de caducidad de su licencia o cualquier otra información de la licencia de ESET Endpoint Antivirus.

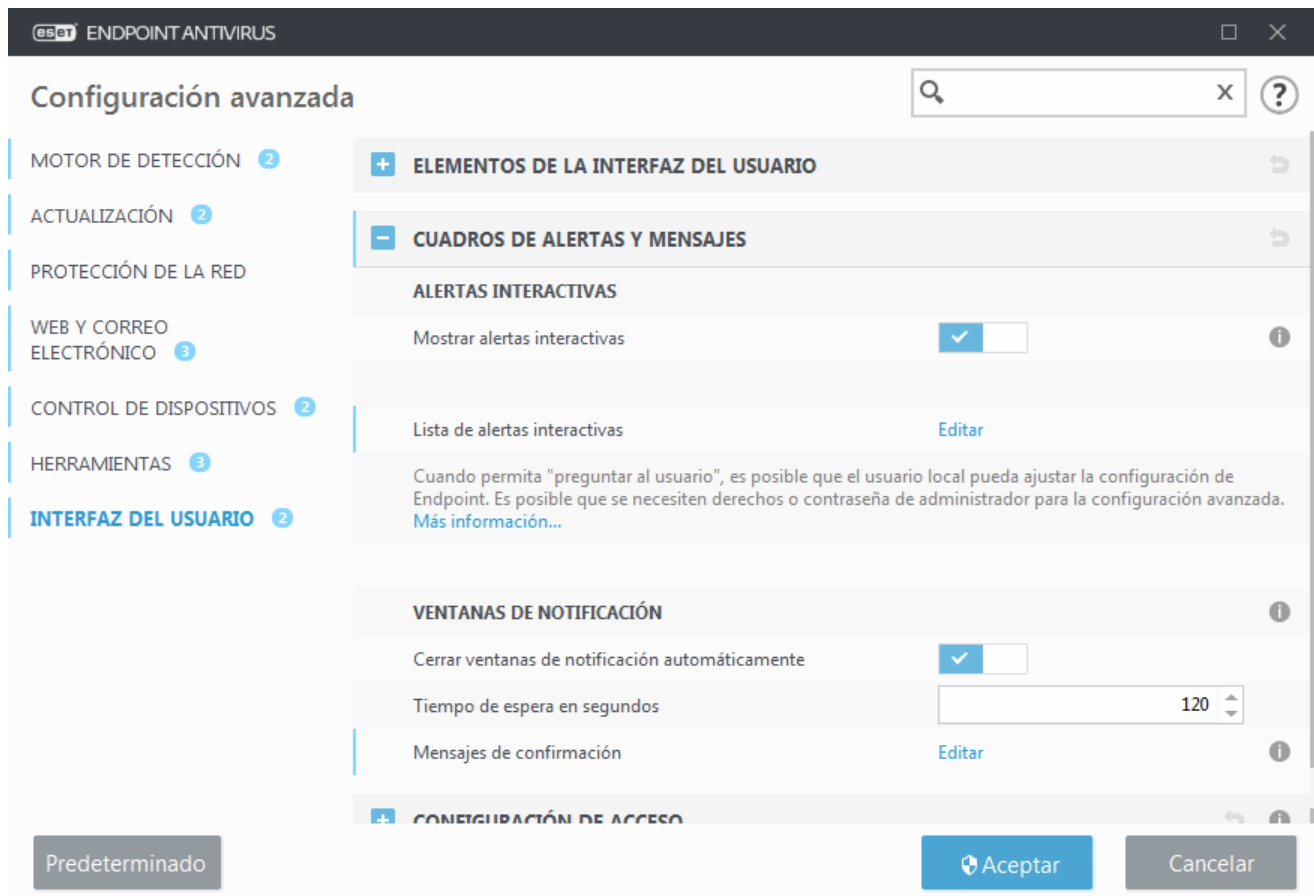
Cuadros de alertas y mensajes



¿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](#)

La sección **Cuadros de alertas y mensajes** (antes **Alertas y notificaciones**) de **Interfaz de usuario** le permite configurar cómo gestiona ESET Endpoint Antivirus las detecciones cuando un usuario debe tomar una decisión (por ejemplo, sitios web que pueden ser de phishing).



Alertas interactivas

Cuando se encuentra una detección o se requiere la intervención del usuario, se muestran ventanas de alerta interactiva.

Mostrar alertas interactivas

ESET Endpoint Antivirus versión 7.2 y posteriores:

- 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](#).

Si se desactiva **Mostrar alertas interactivas**, se ocultarán todas las ventanas de alerta y los cuadros de diálogo del navegador. Se seleccionará automáticamente una acción predeterminada predefinida (por ejemplo, los "sitios web que pueden ser de phishing" se bloquearán).

ESET Endpoint Antivirus versión 7.1 y anteriores:

El nombre de este ajuste es **Mostrar alertas** y no es posible personalizar acciones predefinidas para ventanas específicas de alertas interactivas.

Notificaciones en el escritorio

Las [notificaciones del escritorio](#) y los globos de sugerencias son solo informativos y no requieren interacción del usuario. La sección **Notificaciones en el escritorio** se movió a **Herramientas > Notificaciones** en Configuración avanzada (versión 7.1 y posteriores).

Cuadros de mensajes

Para cerrar las ventanas emergentes automáticamente después de un período de tiempo determinado, seleccione la opción **Cerrar ventanas de notificación automáticamente**. Si no se cierran de forma manual, las ventanas

de alerta se cerrarán automáticamente cuando haya transcurrido el período de tiempo especificado.

Mensajes de confirmación: muestra una [lista de mensajes de confirmación](#) que se pueden seleccionar para que se muestren o no.

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, vaya a **Interfaz de usuario > Cuadros de alertas y mensajes > Lista de alertas interactivas** del árbol de configuración avanzada de ESET Endpoint Antivirus y haga clic en **Editar**.



Objetivo

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 también los [estados de la aplicación](#) en el producto.

Selecciónar qué alerta interactiva se mostrará

Nombre	Preguntar al usuario	Acción aplicada cuando no se muestra
Medios extraíbles		
Se detectó un nuevo dispositivo	<input checked="" type="checkbox"/>	Mostrar las opciones de análisis
Protección de la red		
Acceso a la red bloqueado	<input checked="" type="checkbox"/>	Ninguno
Comunicación de red bloqueada	<input checked="" type="checkbox"/>	Bloquear
Amenaza de red bloqueada	<input checked="" type="checkbox"/>	Bloquear
Alertas del navegador web		
Se encontró contenido potencialmente indeseable	<input checked="" type="checkbox"/>	Bloquear
Sitio web bloqueado debido a phishing	<input checked="" type="checkbox"/>	Bloquear

Aceptar Cancelar

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 ESMC.
- [Comunicación de red bloqueada](#)
- [Amenaza de red bloqueada](#)

Alertas del navegador web

- [Se encontró contenido potencialmente indeseable](#)
- [Sitio web bloqueado debido a phishing](#)

Ordenador

La presencia de estas alertas cambiará la interfaz de usuario a naranja:

- [Reiniciar el ordenador \(obligatorio\)](#)
- [Reiniciar el ordenador \(recomendado\)](#)



Limitaciones

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, diríjase a **Interfaz de usuario > Alertas y cuadros de mensajes > Mensajes de confirmación** en el árbol de configuración avanzada de ESET Endpoint Antivirus y haga clic en **Editar**.

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.

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.



Importante

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

Si las máquinas del punto de conexión reciben la alerta roja "Es necesario reiniciar", puede desactivar la visualización de las alertas.

Para desactivar las alertas "Es necesario reiniciar" o "Se recomienda reiniciar", siga los pasos que se indican a continuación:

1. Pulse la tecla **F5** para acceder a Configuración avanzada y despliegue la sección **Cuadros de alertas y mensajes**.
2. Haga clic en **Editar** junto a **Lista de alertas interactivas**. En la sección **Ordenador**, desmarque las casillas de verificación situadas junto a **Reiniciar el ordenador (obligatorio)** y **Reiniciar el ordenador (recomendado)**.

Select which interactive alert will be displayed ?

Name	Ask user	Action applied when not displayed
+ Removable media		
+ Network protection		
+ Web browser alerts		
- Computer		
Restart computer (required)	<input type="checkbox"/>	None
Restart computer (recommended)	<input type="checkbox"/>	None

OK Cancel

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**.

Selected application statuses will be displayed ?

Name	Show
DEVICE CONTROL	
Device control is not fully functional	<input checked="" type="checkbox"/>
Device control is paused	<input checked="" type="checkbox"/>
GENERAL	
Computer restart recommended	<input type="checkbox"/>
Computer restart required	<input type="checkbox"/>
ESET LiveGrid® is disabled	<input checked="" type="checkbox"/>
ESET LiveGrid® is not accessible	<input checked="" type="checkbox"/>
Policy override active	<input checked="" type="checkbox"/>
Presentation mode is enabled	<input checked="" type="checkbox"/>
Settings password has to be updated	<input checked="" type="checkbox"/>
Windows updates available	<input checked="" type="checkbox"/>

OK Cancel

Se recomienda reiniciar

Si las máquinas del punto de conexión reciben la alerta amarilla "Se recomienda reiniciar", puede desactivar la visualización de las alertas.

Para desactivar las alertas "Es necesario reiniciar" o "Se recomienda reiniciar", siga los pasos que se indican a continuación:

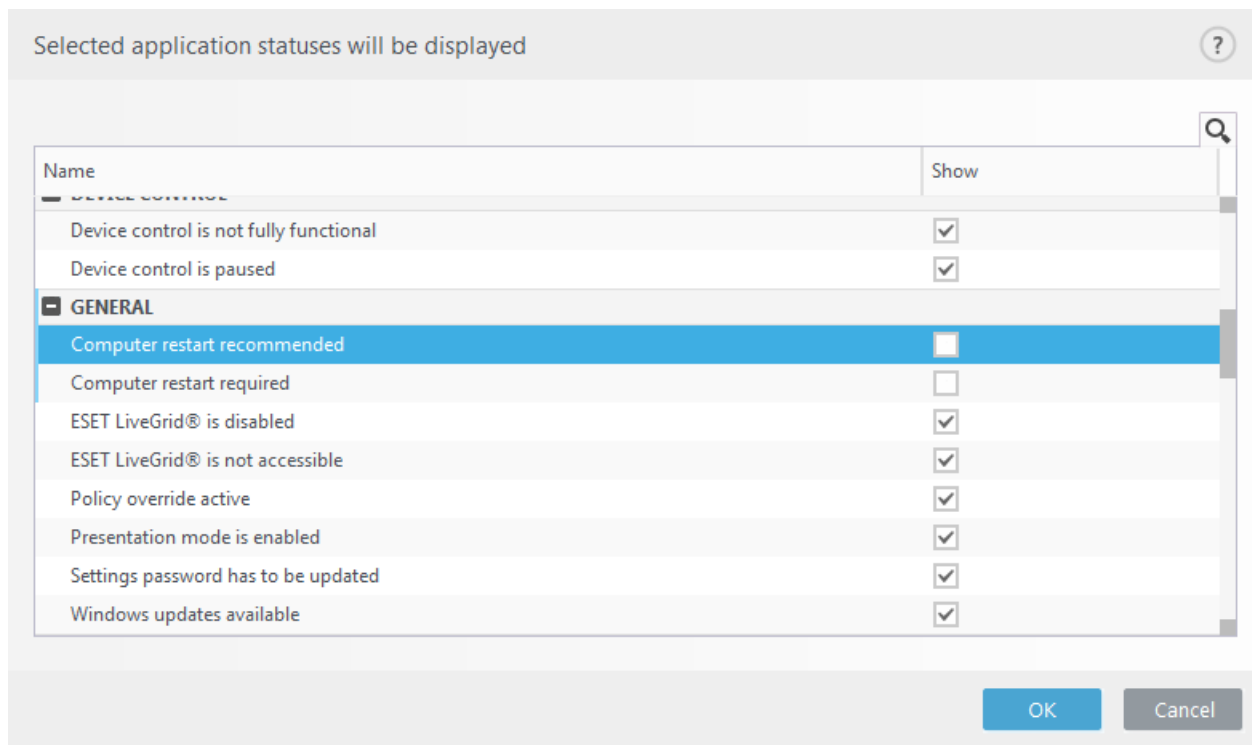
1. Pulse la tecla **F5** para acceder a Configuración avanzada y despliegue la sección **Cuadros de alertas y mensajes**.
2. Haga clic en **Editar** junto a **Lista de alertas interactivas**. En la sección **Ordenador**, desmarque las casillas de verificación situadas junto a **Reiniciar el ordenador (obligatorio)** y **Reiniciar el ordenador (recomendado)**.

Select which interactive alert will be displayed ?

Name	Ask user	Action applied when not displayed
+ Removable media		
+ Network protection		
+ Web browser alerts		
- Computer		
Restart computer (required)	<input type="checkbox"/>	None
Restart computer (recommended)	<input type="checkbox"/>	None

OK Cancel

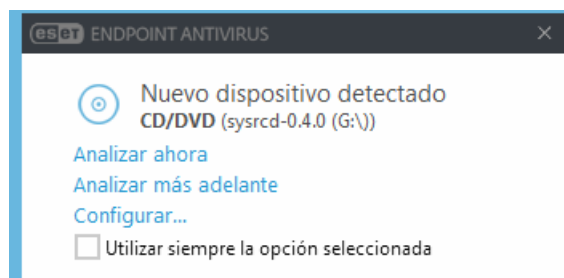
3. Haga clic en **Aceptar** para guardar sus cambios en las dos ventanas abiertas.
4. Las alertas ya no aparecerán en la máquina del punto de conexión.
5. (opcional) Para desactivar el estado de la aplicación en la ventana del programa principal de ESET Endpoint Antivirus, en la [ventana Estados de la aplicación](#), desmarque las casillas de verificación situadas junto a **Es necesario reiniciar el ordenador** y **Es recomendable reiniciar el ordenador**.



Unidades extraíbles

ESET Endpoint Antivirus permite analizar los medios extraíbles (CD, DVD, USB, etc.) de forma automática. 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 ESET Endpoint Antivirus, aparece la siguiente ventana:



Opciones de este cuadro de diálogo:

- **Analizar ahora:** activa el análisis del medio extraíble.
- **Analizar más adelante:** el análisis del medio extraíble se pospone.
- **Configuración:** abre la sección **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](#).

ESET Endpoint Antivirus 7.2 y posteriores

Para acceder a la configuración del análisis de medios extraíbles, abra Configuración avanzada (**F5**) > **Interfaz de usuario** > **Cuadros de alertas y mensajes** > **Alertas interactivas** > **Lista de alertas interactivas** > **Modificar** > **Se detectó un nuevo dispositivo**.

Si **Preguntar al usuario** no está seleccionado, seleccione la acción que desea realizar 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.
- **Mostrar las opciones de análisis:** abre la sección de configuración **Alertas interactivas**.


ESET Endpoint Antivirus 7.1 y anteriores

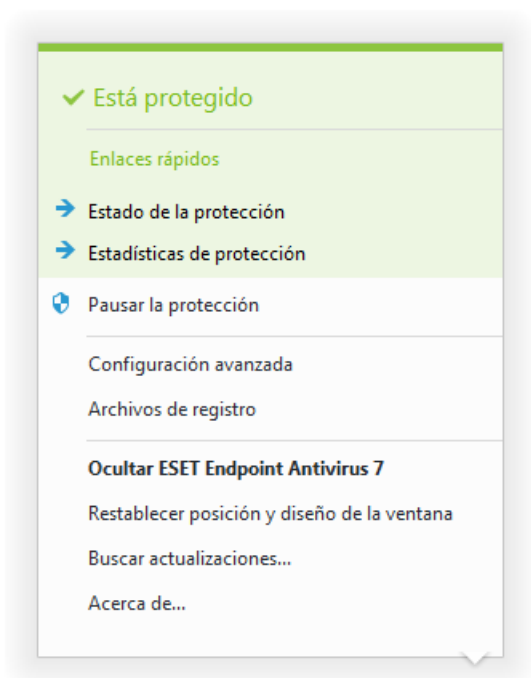
Para acceder a los ajustes para el análisis de medios extraíbles, abra Configuración avanzada (**F5**) > **Motor de detección** > **Análisis de malware** > **Medios extraíbles**.

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.
- **Mostrar las opciones de análisis:** abre la sección de configuración de **medios extraíbles**.

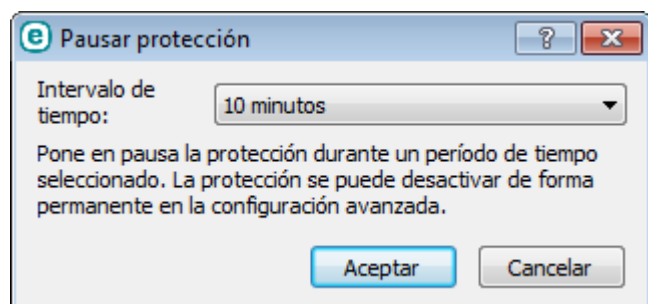
Icono en la bandeja del sistema

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 .



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** se indica el periodo de tiempo durante el que estará desactivada la protección.



Configuración avanzada: seleccione esta opción para acceder al árbol de **Configuración avanzada**. También puede acceder a Configuración mediante la tecla F5 o desde **Configuración > Configuración avanzada**.

Archivos de registro: los [archivos de registro](#) contienen información acerca de todos los sucesos importantes del programa y proporcionan información general sobre las amenazas detectadas.

Abrir ESET Endpoint Antivirus: abre la ventana principal del programa de ESET Endpoint Antivirus desde el icono de la bandeja.

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

Buscar actualizaciones....: inicia la actualización de los módulos del programa para garantizar su nivel de protección contra el código malicioso.

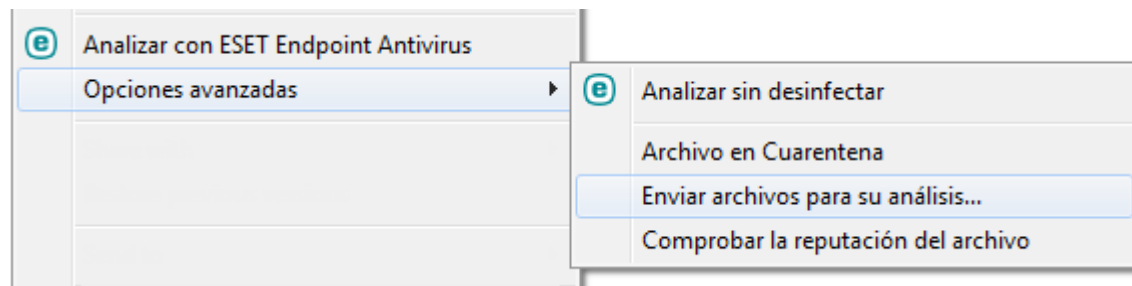
Acerca de: contiene información del sistema y detalles acerca de la versión instalada de ESET Endpoint Antivirus, así como de los módulos del programa instalados y la fecha de caducidad de la licencia. Al final de la página encontrará información sobre el sistema operativo y los recursos del sistema.

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.

Es posible integrar elementos de control de ESET Endpoint Antivirus en el menú contextual. En el árbol de configuración avanzada se proporciona una opción de configuración para esta funcionalidad, en **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.



Ayuda y asistencia técnica

ESET Endpoint Antivirus contiene herramientas de resolución de problemas e información de soporte que le

ayudará a solucionar los problemas que se encuentre.

Ayuda

Buscar en la base de conocimientos de ESET: 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.

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

Encontrar una solución rápida: haga clic en este vínculo para buscar soluciones a los problemas más frecuentes. Es recomendable que lea esta sección antes de ponerse en contacto con el equipo de soporte técnico.

Soporte técnico

Enviar una solicitud de soporte: si no encuentra respuesta a su problema, puede usar este formulario del sitio web de ESET para ponerse rápidamente en contacto con nuestro departamento de soporte técnico.

Detalles para el servicio de soporte técnico: cuando se le solicite, puede copiar y enviar información al servicio de soporte técnico de ESET (como, por ejemplo, nombre del producto, versión del producto, sistema operativo y tipo de procesador).

Herramientas de soporte

Enciclopedia de amenazas: es un enlace a la enciclopedia de amenazas de ESET, que contiene información sobre los peligros y los síntomas de diferentes tipos de amenaza.

Historial del Motor de detección: enlaces al radar de virus de ESET, que contiene información sobre cada versión de la base de detección de ESET (conocida anteriormente como "base de firmas de virus").

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.

Limpiador especializado ESET: herramientas de eliminación para infecciones por código malicioso comunes; para obtener más información, visite este [artículo de la Base de conocimiento de ESET](#).

Información del producto y la licencia

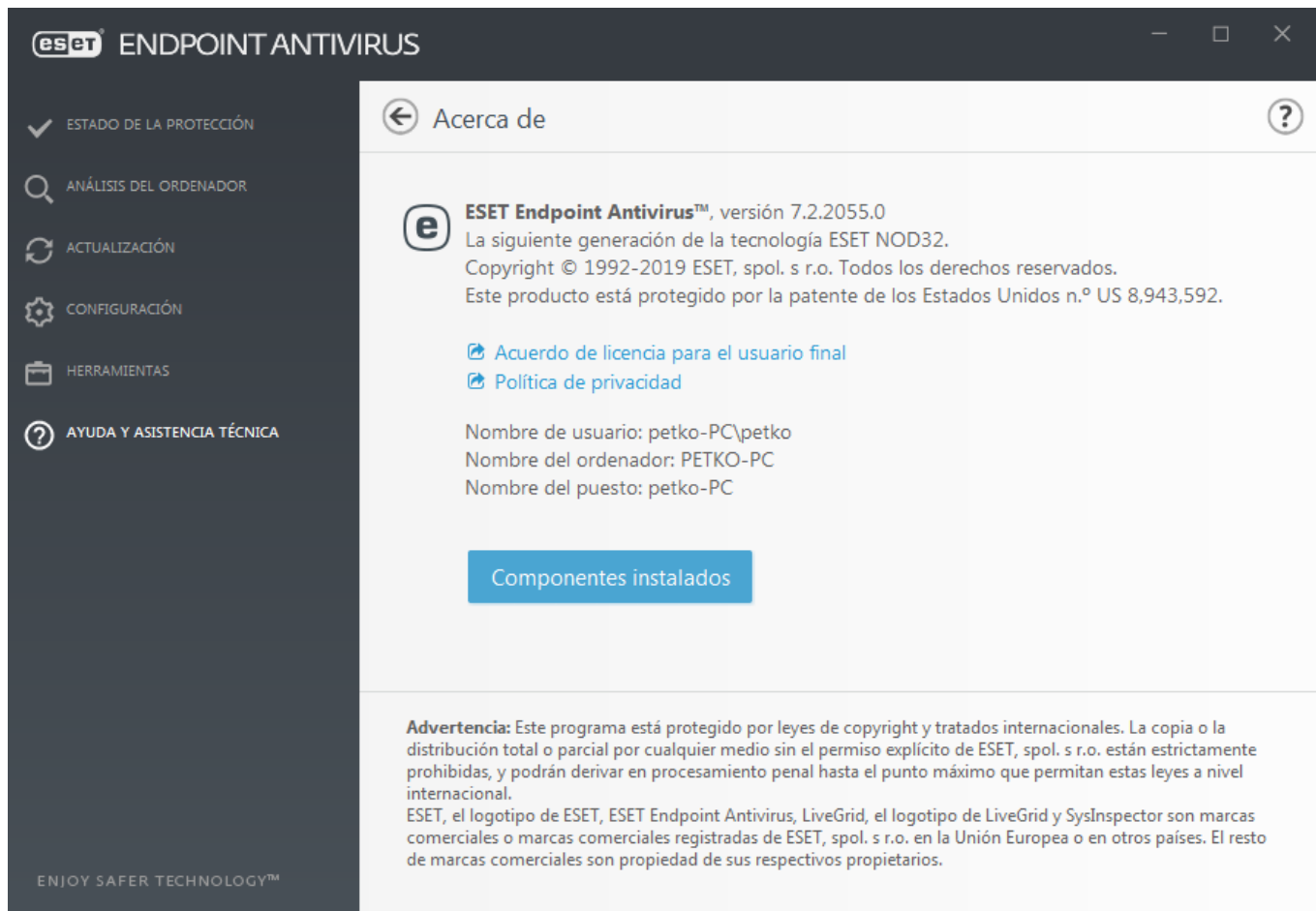
Acerca de ESET Endpoint Antivirus: muestra información sobre su copia de [ESET Endpoint Antivirus](#).

Activar producto/Cambiar licencia: haga clic para abrir la ventana de activación y activar el producto.

Acerca de ESET Endpoint Antivirus

Esta ventana contiene detalles sobre la versión instalada de ESET Endpoint Antivirus, el sistema operativo y los recursos del sistema.

Haga clic en **Componentes instalados** para ver información sobre la lista de módulos del programa instalados. Para copiar en el portapapeles información sobre los módulos, haga clic en **Copiar**. Esto puede resultarle útil durante la resolución de problemas o cuando se ponga en contacto con el servicio de soporte técnico.



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.

Al 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. Si desea enviar el formulario sin datos, haga clic en **No enviar datos** y podrá ponerse en contacto con el servicio de soporte técnico de ESET mediante el formulario de soporte en línea.

Este ajuste también puede configurarse en **Configuración avanzada > Herramientas > Diagnóstico > Soporte técnico**.



Nota

si ha optado por enviar los datos del sistema, es necesario cumplimentar y enviar el formulario web o, de lo contrario, no se creará su parte y se perderán los datos de su sistema.

Administrador de perfiles

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

Análisis del ordenador a petición

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 la ventana Configuración avanzada (F5) y haga clic en **Antivirus > Análisis del ordenador a petición** y, a continuación, en **Modificar** junto a **Lista de perfiles**. En el menú desplegable **Perfil de actualización** se muestra una lista de los perfiles de análisis disponibles. Si necesita ayuda para crear un perfil de análisis que se adecúe a sus necesidades, consulte la sección [Configuración de parámetros del motor ThreatSense](#) para ver una descripción de los diferentes parámetros de la configuración del análisis.



Nota

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 **Desinfección estricta**. 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 perfil de la sección de configuración de actualizaciones permite a los usuarios 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.

Accesos directos del teclado

Puede utilizar los siguientes accesos directos del teclado para mejorar la navegación en ESET Endpoint Antivirus:

Accesos directos del teclado	Acción realizada
F1	abre las páginas de ayuda
F5	abre la Configuración avanzada
Up/Down	navegación por los elementos del producto
TAB	mueve el cursor 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

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 que 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 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.

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 (disponible en la versión 7.2 y posteriores).

Activar registro avanzado de licencias: registrar toda la comunicación del producto con los servidores de activación de ESET y ESET Business Account.

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 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 el registro avanzado del filtrado de protocolos: registrar los datos que pasan a través del motor de filtrado de protocolos en formato PCAP. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con el filtrado de protocolos.

Habilitar el registro avanzado de exploración – Registra los problemas que tienen lugar durante la exploración de archivos y carpetas mediante la exploración del equipo o la protección del sistema de archivos en tiempo real (disponible en la versión 7.2 o posterior).

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 registro avanzado del Control web: registrar todos los sucesos que tienen lugar en Control parental. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con el Control parental.

Ubicación de los archivos de registro

Sistema operativo	Directorio de los archivos de registro
Windows Vista y posterior	C:\ProgramData\ESET\ESET Endpoint Antivirus\Diagnostics\

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 ESET:

```
ec\ls [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) utilizar el MODO desinfección para objetos infectados
/clean-mode=MODO	Están disponibles las opciones siguientes:
	• none (ninguno): no se realiza la desinfección automática.
	• standard (estándar, predeterminado): ecl.exe intenta desinfectar o eliminar automáticamente los archivos infectados.
	• strict (estricto): ecl.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): ecl.exe elimina los archivos sin intentar desinfectarlos, sea cual sea el archivo.
/quarantine	• delete (eliminar): ecl.exe elimina los archivos sin intentar desinfectarlos, pero no elimina archivos delicados como los archivos del sistema de Windows.
	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 (podrían ser amenazas)
50	amenaza detectada
100	error



Nota

los códigos de salida superiores a 100 significan que no se ha analizado el archivo y que, por lo tanto, puede estar infectado.

CMD de ESET

Se trata de una función que activa comandos de ecmd avanzados. Le permite 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.



Importante

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.



Nota

Los comandos de ecmd avanzados solo pueden ejecutarse de forma local. La ejecución de la tarea de cliente **Ejecutar comando** utilizando ESMC no funcionará correctamente.



Ejemplo

Comando para exportar configuración:

```
ecmd /getcfig
```

```
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>`.



Importante

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.



Ejemplo

Comando para firmar un archivo de configuración exportado:
`xmldsigntool /version 2 c:\config\settings.xml`

```
Administrator: C:\Windows\system32\cmd.exe

C:\Xmldsigntool>xmldsigntool /version 1 c:\config\settings.xml
Enter Advanced Setup Password:
Re-enter Password:
C:\Xmldsigntool>_
```



NOTA

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.



Advertencia

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 ESMC 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	<code>ecmd /setfeature onaccess pause</code>	<code>ecmd /setfeature onaccess enable</code>
Protección de documentos	<code>ecmd /setfeature document pause</code>	<code>ecmd /setfeature document enable</code>
Control del dispositivo	<code>ecmd /setfeature devcontrol pause</code>	<code>ecmd /setfeature devcontrol enable</code>
Modo de presentación	<code>ecmd /setfeature presentation pause</code>	<code>ecmd /setfeature presentation enable</code>
Tecnología Anti-Stealth	<code>ecmd /setfeature antistealth pause</code>	<code>ecmd /setfeature antistealth enable</code>
Cortafuegos personal	<code>ecmd /setfeature firewall pause</code>	<code>ecmd /setfeature firewall enable</code>

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 acceso a la Web	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
Protección de clientes de correo electrónico	ecmd /setfeature email pause	ecmd /setfeature email enable
Protección Antispam	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Protección Anti-Phishing	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

Detección de estado inactivo

Los ajustes de detección de estado inactivo se pueden configurar en **Configuración avanzada**, en **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](#), cuando:

- el salvapantallas se está ejecutando,
- el ordenador está bloqueado,
- un usuario cierra sesión.

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

Importar y exportar configuración

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

La importación y la exportación de un archivo 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 exportación de configuración también es de utilidad para los usuarios que desean utilizar su configuración preferida en varios sistemas, ya que les permite importar fácilmente el archivo .xml para transferir estos ajustes.

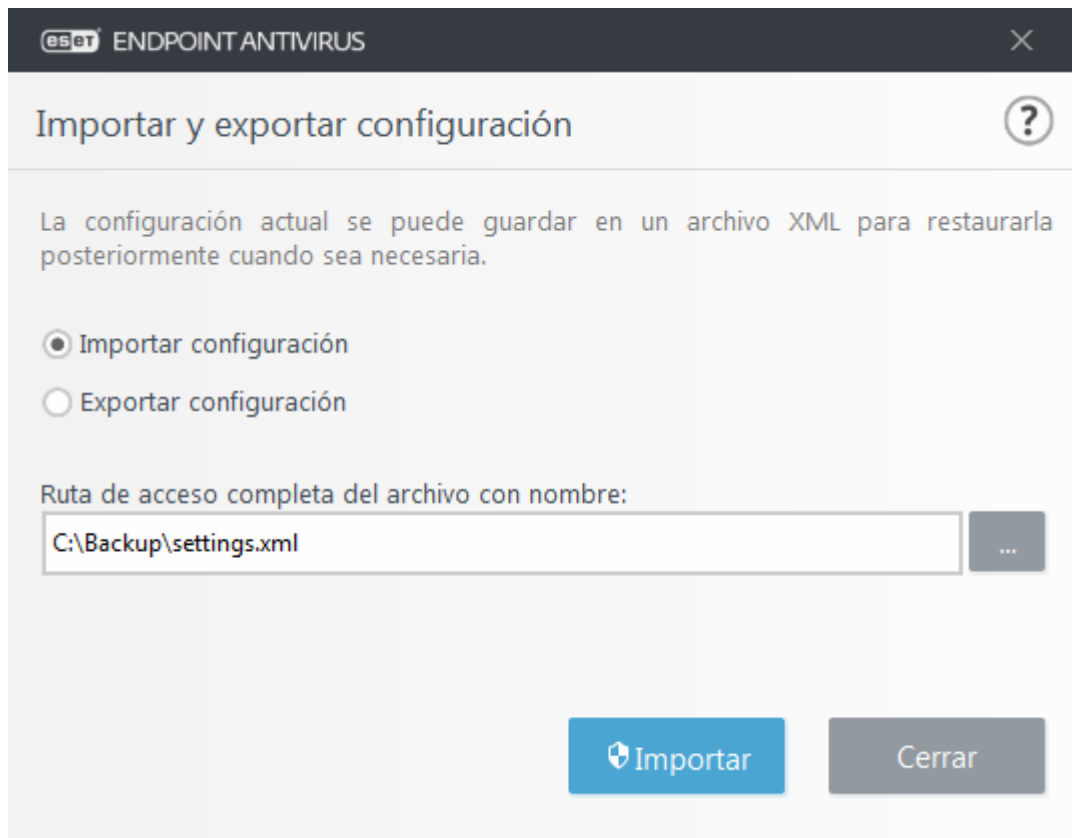
Importar la configuración es muy fácil. En la ventana principal del programa, haga clic en **Configuración > Importar/exportar configuración** y, a continuación, seleccione la opción **Importar configuración**. Introduzca el nombre del archivo de configuración o haga clic en el botón ... para buscar el archivo de configuración que desea importar.

Los pasos para exportar una configuración son muy similares. En la ventana principal del programa, haga clic en **Configuración > Importar/exportar configuración**. Seleccione **Exportar configuración** e introduzca el nombre del archivo de configuración (por ejemplo, *export.xml*). Utilice el navegador para seleccionar la ubicación del ordenador donde desee guardar el archivo de configuración.



Nota

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




Restaurar todos los valores de todas las configuraciones

Haga clic en **Predeterminado** en Configuración avanzada (F5) 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.

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