

ESET PROTECT

Guía para pequeñas y medianas empresas

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

Copyright ©2023 de ESET, spol. s r.o.

ESET PROTECT está desarrollado por ESET, spol. s r.o.

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

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

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

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

REV. 19/03/2023

1	Acerca de la ayuda	1
2	Introducción	2
	2.1 Productos ESET Endpoint que se pueden administrar	2
	2.2 Nuevas funciones de ESET PROTECT 9.0	2
3	Componentes y arquitectura de ESET PROTECT	3
4	Requisitos del sistema	5
	4.1 Hardware	5
	4.2 Sistema operativo	6
	4.3 Red	8
	4.4 Software	8
5	Instalar ESET PROTECT Server	9
	5.1 Instalación todo en uno de ESET PROTECT Server	10
6	Pasos posteriores a la instalación	23
7	Implementación de ESET Management Agent y el producto ESET Endpoint	24
	7.1 Creación del paquete de implementación	25
	7.2 Instalación del paquete de implementación	28
	7.3 Otros métodos de implementación	31
	7.4 ESET Remote Deployment Tool	32
8	ESET PROTECT Web Console	35
	8.1 Asistente de inicio	37
	8.2 Consola	38
	8.3 Ordenadores	40
	8.4 Grupos	41
	8.5 Detecciones	43
	8.6 Informes	44
	8.7 Tareas	45
	8.8 Políticas	46
	8.9 Notificaciones	47
	8.10 Resumen del estado	49
	8.11 Cuarentena	50
	8.12 Administración de licencias	51
	8.13 Conjuntos de permisos y usuarios	52
	8.14 Certificados	53
9	Ayuda y asistencia técnica	54
10	Acuerdo de licencia para el usuario final	54
11	Política de privacidad	61

Acerca de la ayuda

Por motivos de coherencia y para evitar confusiones, la terminología que se usa en esta guía está basada en los nombres de parámetro de ESET PROTECT. También usamos una serie de símbolos para destacar temas de especial interés o importancia.

 Las notas pueden contener información valiosa, como funciones específicas o un vínculo a un tema relacionado.

 Este contenido requiere su atención y no debe ignorarse. Normalmente ofrece información que no es vital, pero sí importante.

 Se trata de información vital que debe tratar con mayor cautela. Las advertencias tienen como finalidad específica evitar que cometa errores que pueden tener consecuencias negativas. Lea y comprenda el texto situado en secciones de advertencia, ya que hace referencia a ajustes del sistema muy delicados o a cuestiones que pueden suponer un riesgo.

 Se trata de una situación de ejemplo que describe un caso de uso pertinente para el tema en el que se incluye. Los ejemplos se usan para detallar temas más complicados.

Convención	Significado
Negrita	Nombres de elementos de la interfaz, como recuadros y botones de opciones.
<i>Cursiva</i>	Marcadores de posición de información que facilita. Por ejemplo, nombre de archivo o ruta de acceso significa que se debe escribir la ruta de acceso o el nombre de un archivo.
Courier New	Ejemplos de código o comandos.
Hipervínculo	Ofrece un acceso rápido y sencillo a temas como referencia cruzada o a sitios web externos. Los hipervínculos aparecen resaltados en azul y pueden estar subrayados.
%ProgramFiles%	El directorio del sistema operativo Windows en el que se almacenan los programas instalados de Windows y de otras empresas.

- La [Ayuda en línea](#) es la fuente principal de contenido de ayuda. Siempre que tenga una conexión a Internet disponible, se mostrará automáticamente la versión más reciente de la Ayuda en línea. Las páginas de la Ayuda en línea de ESET PROTECT presentan cuatro pestañas activas en el encabezado de navegación superior: [Instalación/Actualización](#), [Administración](#), [Implementación del dispositivo virtual](#) y [Guía de SMB](#).
- Los temas de esta guía están divididos en diversos capítulos y subcapítulos. Puede buscar información pertinente desde el campo Buscar situado en la parte superior.

 Cuando abra una guía del usuario desde la barra de navegación situada en la parte superior de la página, la búsqueda se limitará al contenido de dicha guía. Por ejemplo, si abre la guía Administración, no se incluirán en los resultados de la búsqueda los temas de las guías Instalación/Actualización e Implementación del dispositivo virtual.

- La [Base de conocimiento ESET](#) contiene respuestas a las preguntas más frecuentes, así como soluciones recomendadas para distintos problemas. Esta Base de conocimiento la actualizan periódicamente los especialistas técnicos de ESET, y es la herramienta más potente para resolver diversos tipos de problema.
- El [Foro de ESET](#) ofrece a los usuarios de ESET una forma sencilla de obtener ayuda y de ayudar a otras personas. Puede publicar cualquier problema o pregunta que tenga con respecto a sus productos ESET.

Introducción

Esta guía está pensada para una pyme que gestiona hasta 250 productos ESET para puntos de acceso Windows con ESET PROTECT 9.

En ella se explican conceptos básicos importantes para la implementación y el uso de los productos de seguridad de ESET.

ESET PROTECT 9

ESET PROTECT 9 (anteriormente ESMC) es una aplicación que le permite gestionar los productos de ESET en estaciones de trabajo cliente, servidores y dispositivos móviles en un entorno de red desde una ubicación central.

El sistema de administración de tareas integrado en ESET PROTECT le permite instalar soluciones de seguridad de ESET en ordenadores remotos y responder rápidamente a nuevos problemas y detecciones.

ESET PROTECT no ofrece protección frente a código malicioso por sí mismo. La protección del entorno depende de la presencia en las estaciones de trabajo de una solución de seguridad de ESET, como ESET Endpoint.

Productos ESET Endpoint que se pueden administrar

Los productos ESET Endpoint están diseñados principalmente para utilizarlos en estaciones de trabajo dentro de un entorno de pequeña o gran empresa, y se pueden utilizar con ESET PROTECT.

ESET PROTECT 9 puede implementar, activar o administrar los siguientes productos de ESET Endpoint:

Administrable desde ESET PROTECT 9	Versión del producto
ESET Endpoint Security para Windows	6.5+, 7.x, 8.x, 9.x
ESET Endpoint Antivirus para Windows	6.5+, 7.x, 8.x, 9.x
ESET Endpoint Security para macOS	6.8+
ESET Endpoint Antivirus para macOS	6.8+
ESET Endpoint Security para Android	2.x

Consulte también la [lista completa de los productos de seguridad de ESET que se pueden administrar](#).

Nuevas funciones de ESET PROTECT 9.0

Acceso a información detallada con un solo clic

Nunca ha sido más fácil ver rápidamente detalles del ordenador o detalles de la detección y acceder a ellos. Solo tiene que hacer clic en el nombre del ordenador en la sección **Ordenadores**, y aparecerá un panel lateral con detalles. [Más información](#) También hemos usado el mismo enfoque para la sección **Detecciones** al hacer clic en un tipo de detección. [Más información](#)

Nuevo panel principal de información general para EDTD

Hemos introducido un nuevo panel en el que encontrará información y estadísticas útiles relacionadas con ESET Dynamic Threat Defense. [Más información](#)

Actualizaciones automáticas del producto

Para facilitarle la vida, vamos a introducir actualizaciones automáticas de nuestros productos de seguridad (productos para equipos Windows por ahora) con activación preconfigurada en el próximo ESET Endpoint Security/Antivirus v9, que se desplegará en noviembre. Con las actualizaciones automáticas puede mantener siempre actualizados los productos de ESET de su red. [Más información](#)

Gestión de la protección contra ataques de fuerza bruta

En la versión 9 de los productos para equipos Windows, implementamos una nueva función de seguridad que protege los dispositivos frente a los intentos de adivinar las credenciales y establecer una conexión remota. Puede configurar fácilmente esta función mediante una política directamente desde la consola y crear exclusiones desde la sección **Detecciones** cuando se bloquee un elemento que no deba bloquearse.

Mejoras en ESET Full Disk Encryption

Ahora puede ahorrar un valioso tiempo al automatizar fácilmente las actualizaciones de los módulos de ESET Full Disk Encryption. También hemos agregado la opción de implementar un instalador con una contraseña predefinida y un mapa del teclado para iniciar el cifrado. Por último, hemos mejorado la interfaz de usuario para mostrar los módulos de ESET Full Disk Encryption que están instalados.

Otras mejoras y cambios para facilitar el uso

Puede ver más detalles en [el registro de cambios](#).

Componentes y arquitectura de ESET PROTECT

Para realizar una implementación completa de la cartera de soluciones de seguridad de ESET, se deben instalar los siguientes componentes:

- ESET PROTECT Server (controla la comunicación con los ordenadores cliente)
- ESET PROTECT Web Console (interfaz de usuario basada en navegador de ESET PROTECT Server)
- ESET Management Agent (se implementa en los ordenadores cliente, se comunica con ESET PROTECT Server)

Los siguientes componentes complementarios son opcionales, pero se recomienda instalarlos para un mejor rendimiento de la aplicación en la red:

- Proxy HTTP Apache
- RD Sensor (puede detectar ordenadores no administrados en la red)

Servidor

ESET PROTECT Server es la aplicación que procesa todos los datos recibidos de los clientes que se conectan al servidor (a través de ESET Management Agent).

Agente

ESET Management Agent es una parte fundamental de ESET PROTECT. Los ordenadores cliente no se comunican con el servidor directamente, sino que el agente facilita esta comunicación. El agente recopila información del cliente y la envía a ESET PROTECT Server. Si ESET PROTECT Server envía una tarea al cliente, esta se envía al agente que la envía, a su vez, al producto ESET Endpoint que se ejecuta en el cliente.

Web Console

ESET PROTECT Web Console es una interfaz de usuario basada en navegador que le permite administrar las soluciones de seguridad de ESET en su entorno. Muestra información general del estado de los clientes en la red y se puede utilizar para implementar de forma remota soluciones de ESET en ordenadores no administrados. Si decide hacer que el servidor web sea accesible desde Internet, puede utilizar ESET PROTECT desde prácticamente cualquier lugar o dispositivo.

Proxy HTTP Apache

El proxy HTTP Apache es un servicio que puede usarse junto con ESET PROTECT 9 para distribuir los paquetes de instalación y las actualizaciones a los ordenadores cliente. Actúa como un proxy transparente, lo que significa que almacena en caché los archivos que ya se han descargado para minimizar el tráfico de Internet en la red.

El uso del proxy HTTP Apache ofrece las siguientes ventajas:

- Descarga y almacena en caché lo siguiente:

- o Actualizaciones del motor de detección

- o Tareas de activación, incluida la comunicación con servidores de activación y almacenamiento en la caché de solicitudes de licencia.

- o Datos del repositorio de ESET PROTECT

- o Actualizaciones de componentes del producto: el proxy Apache almacena en caché y distribuye las actualizaciones a los puntos de acceso clientes de su red.

- Minimiza el tráfico de Internet en la red.

Rogue Detection Sensor

Rogue Detection Sensor (RD Sensor) busca en la red ordenadores no registrados en ESET PROTECT. Este componente puede localizar ordenadores nuevos y agregarlos en ESET PROTECT automáticamente.

Los equipos recién detectados se muestran en un [informe predefinido](#) que facilita la tarea de implementar ESET Management Agent en ellos, asignarlos a grupos estáticos concretos y administrarlos mediante [tareas](#) y [políticas](#).

Requisitos del sistema

Antes de instalar ESET PROTECT, asegúrese de que se cumplan todos los requisitos de [hardware](#), [sistema operativo](#), [red](#) y [software](#).

Hardware

El equipo de ESET PROTECT Server debe cumplir las siguientes recomendaciones de hardware incluidas en la tabla a continuación.

Número de clientes	ESET PROTECT Server + Servidor de bases de datos SQL				
	Núcleos de la CPU	Velocidad de reloj de la CPU (GHz)	RAM (GB)	Unidad de disco ¹	ESPS ² en disco
Hasta 1.000	4	2.1	4	Única	500
5.000	8	2.1	8		1.000
10.000 ³	4	2.1	16	Independiente	2.000
20.000	4	2.1	16		4.000
50.000	8	2.1	32		10.000
100.000	16	2.1	64 o superior		20.000

1 Disco individual/independiente: se recomienda instalar la [base de datos](#) en una unidad independiente para sistemas con más de 10.000 clientes.

2 IOPS (total de operaciones de E/S por segundo): valor mínimo necesario.

- Se recomienda contar con aproximadamente 0,2 IOPS por cliente conectado, pero con un mínimo de 500.
- Puede comprobar el IOPS de la unidad con la herramienta [diskspd](#); utilice el siguiente comando:

Número de clientes	Comando
Hasta 5.000 clientes	<code>diskspd.exe -c1000M -b4K -d120 -Sh -r -z -w50 C:\testfile.dat</code>
Más de 5.000 clientes	<code>diskspd.exe -c10000M -b4K -d600 -Sh -r -z -w50 C:\testfile.dat</code>

3 Consulte el [caso de ejemplo](#) para un entorno de 10.000 clientes.

Recomendaciones de unidad de disco

La unidad de disco es el factor crítico que influye en el rendimiento de ESET PROTECT.

- La instancia de SQL Server puede compartir recursos con ESET PROTECT Server para maximizar la utilización y minimizar la latencia. Ejecute ESET PROTECT Server y el servidor de bases de datos en un solo equipo para aumentar el rendimiento de ESET PROTECT.

- El rendimiento de un servidor SQL mejorará si coloca la los archivos de base de datos y de registro de transacciones en unidades independientes, a ser posible en unidades SSD físicas independientes.
- Si tiene una sola unidad de disco, le recomendamos utilizar una unidad SSD.
- Le recomendamos que utilice una arquitectura íntegramente con memoria flash. Los discos de estado sólido (SSD) son mucho más rápidos que la unidad de disco duro estándar.
- Si cuenta con una alta capacidad de RAM, una configuración SAS con R5 será suficiente. La configuración probada: Diez discos SAS de 1,2 TB en R5: dos grupos de paridad en 4+1 sin almacenamiento en caché adicional.
- El rendimiento no mejora cuando se utiliza un SSD empresarial con un alto número de IOPS.
- Una capacidad de 100 GB es suficiente para cualquier cantidad de clientes. Puede que necesite mayor capacidad si realiza copias de seguridad de la base de datos con frecuencia.
- No utilice una unidad de red, ya que su rendimiento ralentizará ESET PROTECT.
- Si trabaja con una infraestructura de almacenamiento de varios niveles que permite la migración al almacenamiento en línea, le recomendamos que empiece por niveles compartidos más lentos y supervise el rendimiento de ESET PROTECT. Si observa que la latencia de lectura/escritura supera los 20 ms, puede realizar un traslado sin interrupciones de la capa de almacenamiento a un nivel más rápido para utilizar el backend más rentable. Puede hacer lo mismo en un hipervisor (si utiliza ESET PROTECT como máquina virtual).

Recomendaciones de dimensionamiento para distintos recuentos de clientes

A continuación puede ver los resultados de rendimiento de un entorno virtual con un número de clientes definido en ejecución durante un año.

i La base de datos de y ESET PROTECT se están ejecutando en máquinas virtuales independientes con configuraciones de hardware idénticas.

Núcleos de la CPU	Velocidad de reloj de la CPU (GHz)	RAM (GB)	Rendimiento		
			10.000 clientes	20.000 clientes	40.000 clientes
8	2.1	64	Alta	Alta	Normal
8	2.1	32	Normal	Normal	Normal
4	2.1	32	Normal	Normal	Baja
2	2.1	16	Baja	Baja	Insuficiente
2	2.1	8	Muy bajo (no recomendado)	Muy bajo (no recomendado)	Insuficiente

Sistema operativo

En la siguiente tabla se muestran los sistemas operativos Windows compatibles con cada componente de ESET PROTECT. Consulte también una [lista completa de sistemas operativos compatibles](#).

Sistema operativo	Servidor	Agente	RD Sensor	MDM
Windows Server 2008 R2 x64 SP1 con KB4474419 y KB4490628 instalado		✓	✓	
Windows Server 2008 R2 CORE x64 con KB4474419 y KB4490628 instalado		✓	✓	
Windows Storage Server 2008 R2 x64 con KB4474419 y KB4490628 instalado		✓	✓	
Microsoft SBS 2011 Standard x64		✓	✓	
Microsoft SBS 2011 Essentials x64		✓	✓	
Windows Server 2012 x64	✓	✓	✓	✓
Windows Server 2012 CORE x64	✓	✓	✓	✓
Windows Server 2012 R2 x64	✓	✓	✓	✓
Windows Server 2012 R2 CORE x64	✓	✓	✓	✓
Windows Storage Server 2012 R2 x64	✓	✓	✓	✓
Windows Server 2016 x64	✓	✓	✓	✓
Windows Storage Server 2016 x64	✓	✓	✓	✓
Windows Server 2019 x64	✓	✓	✓	✓
Windows Server 2022 x64	✓	✓	✓	✓

Sistema operativo	Servidor	Agente	RD Sensor	MDM
Windows 7 x86 SP1 con las actualizaciones de Windows más recientes (KB4474419 y KB4490628 como mínimo)		✓	✓	
Windows 7 x64 SP1 con las actualizaciones de Windows más recientes (KB4474419 y KB4490628 como mínimo)		✓	✓	
Windows 8 x86		✓	✓	
Windows 8 x64	?	✓	✓	?
Windows 8.1 x86		✓	✓	
Windows 8.1 x64	?	✓	✓	?
Windows 10 x86		✓	✓	
Windows 10 x64 (todas las versiones oficiales)	?	✓	✓	?
Windows 10 en ARM		✓		

Sistema operativo	Servidor	Agente	RD Sensor	MDM
Windows 11 x64	?	✓	✓	?

* Es posible que la instalación de componentes de ESET PROTECT en un SO cliente no cumpla con la política de concesión de licencias de Microsoft. Consulte la política de concesión de licencias de Microsoft o póngase en contacto con su proveedor de software para obtener más información. En los entornos de redes de pequeño tamaño/pequeñas y medianas empresas, le recomendamos que realice una instalación de ESET PROTECT para Linux o utilice un [dispositivo virtual](#) cuando corresponda.

Sistemas MS Windows más antiguos:

- Instale siempre el Service Pack más reciente, sobre todo en sistemas más antiguos, como Server 2008 y Windows 7.

- ESET PROTECT no admite la administración de ordenadores que ejecutan Windows 7 (sin SP) Windows Vista y Windows XP.



- A partir del 24 de marzo de 2020, ESET dejará de ser compatible oficialmente o proporcionará soporte técnico para ESET PROTECT (Server y MDM) instalado en los siguientes sistemas operativos Microsoft Windows: Windows 7 Windows Server 2008 (todas las versiones).

No se admiten sistemas operativos ilegales o pirateados.



Desde enero de 2019, las actualizaciones públicas de Oracle JAVA SE 8 para uso empresarial, comercial o de producción requieren una licencia comercial. Si no compra una suscripción de JAVA SE, puede optar por la transición a una alternativa sin coste siguiendo esta guía. Consulte las [versiones compatibles de JDK](#).



Puede ejecutar ESET PROTECT en un sistema operativo que no sea de servidor y sin necesidad de ESXi.

Instalar [VMware Player](#) en un sistema operativo de escritorio e implementar el dispositivo virtual [ESET PROTECT](#).

Red

Es fundamental que tanto ESET PROTECT Server como los ordenadores cliente administrados por ESET PROTECT tengan una conexión a Internet válida para poder llegar a los servidores de activación y al repositorio de ESET. Si prefiere que los clientes no se conecten directamente a Internet, puede utilizar un servidor proxy (distinto del proxy HTTP Apache) para facilitar la comunicación con su red e Internet.

Los ordenadores administrados a través de ESET PROTECT deben conectarse a la misma red local o deben estar en el mismo dominio de Active Directory que ESET PROTECT Server. Los ordenadores cliente deben poder ver el ESET PROTECT Server. Además, los ordenadores cliente deben poder comunicarse con su ESET PROTECT Server para utilizar la implementación remota y la función [Llamada de activación](#).

Puertos utilizados

Si su red utiliza un cortafuegos, consulte nuestra lista de posibles [puertos de comunicación de red](#) utilizados cuando ESET PROTECT y sus componentes están instalados en su infraestructura.

Software

Se deben cumplir los siguientes requisitos para instalar ESET PROTECT Server en Windows:

- Debe disponer de una [licencia](#) válida.
- Se debe instalar Microsoft .NET Framework 4; puede instalarlo con el **Asistente para agregar roles y características**.
- ESET PROTECT Web Console requiere Java/OpenJDK (64 bits).



Desde enero de 2019, las actualizaciones públicas de Oracle JAVA SE 8 para uso empresarial, comercial o de producción requieren una licencia comercial. Si no compra una suscripción de JAVA SE, puede optar por la transición a una alternativa sin coste siguiendo esta guía. Consulte las [versiones compatibles de JDK](#).

- ESET PROTECT es compatible con dos tipos de servidores de bases de datos: MS SQL y MySQL. Le recomendamos que utilice Microsoft SQL Server Express 2019, que se incluye en el Instalador todo en uno de ESET PROTECT para Windows. Si ya tiene un servidor de base de datos y desea utilizarlo para ESET PROTECT, asegúrese de que cumple los [requisitos de bases de datos](#).

- ESET PROTECT Web Console se puede ejecutar en los siguientes navegadores web:

Mozilla Firefox

Microsoft Edge

Google Chrome

Safari

Opera



Para disfrutar de la mejor experiencia con la Consola web de ESET PROTECT, le recomendamos que mantenga actualizados los navegadores web.

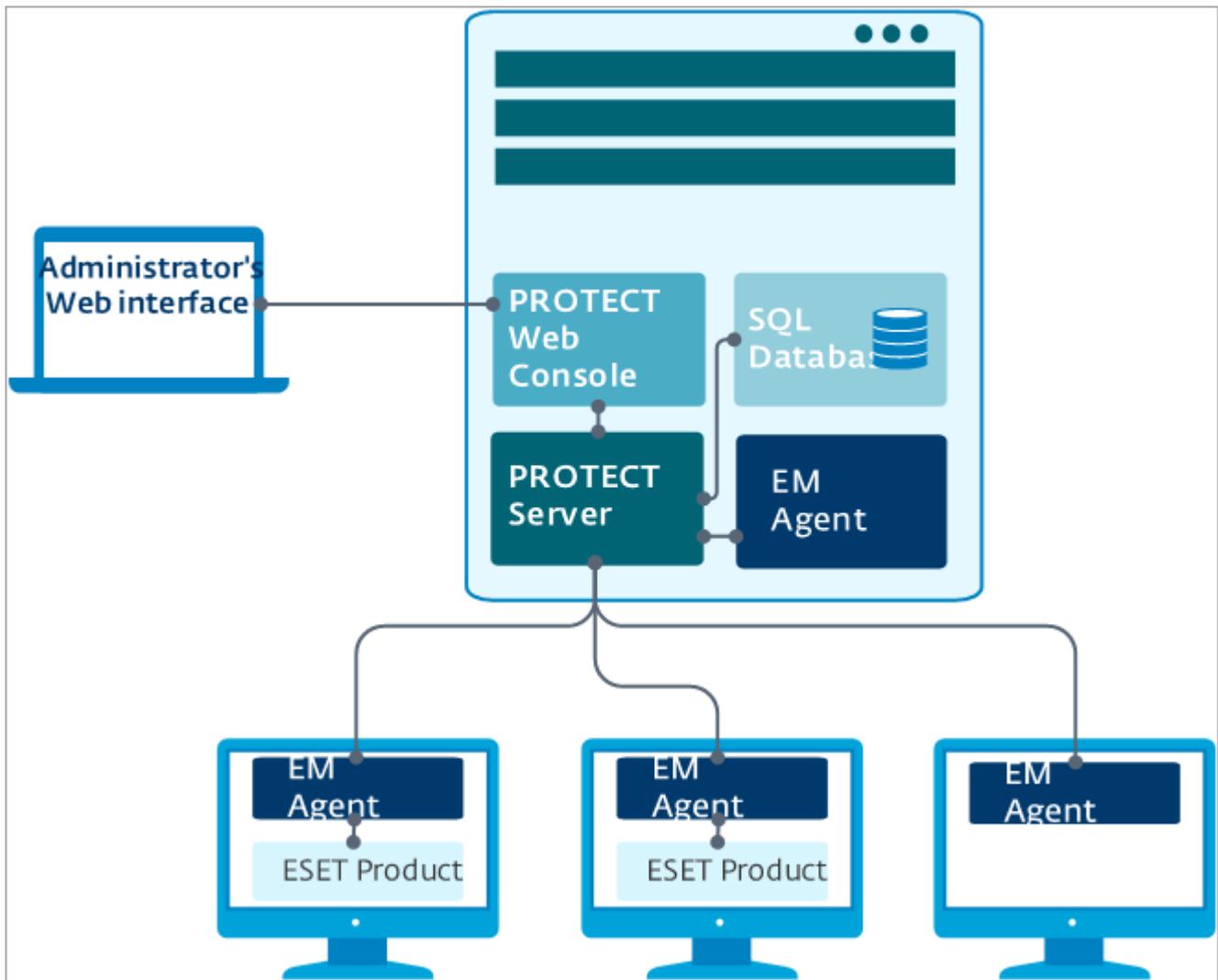
Si utiliza Internet Explorer, ESET PROTECT Web Console le avisará de que está utilizando un navegador web no compatible.

Instalar ESET PROTECT Server

Estructura de los componentes de ESET PROTECT

Para administrar redes de tamaño pequeño a mediano (1.000 clientes o menos), suele ser suficiente una sola máquina con ESET PROTECT Server y todos sus componentes (servidor web suministrado, base de datos, entre otros) instalados. Puede pensar en él como en un solo servidor o una instalación independiente. Todos los clientes administrados se conectan directamente a ESET PROTECT Server a través de ESET Management Agent. El administrador puede conectarse a ESET PROTECT Web Console a través de un navegador web desde cualquier

ordenador de la red o ejecutar Web Console directamente desde ESET PROTECT Server.



Instalación

Los instaladores de ESET PROTECT están disponibles en diferentes formatos para admitir diversos métodos de instalación:

- ESET recomienda el [Instalador todo en uno](#) para pequeñas implementaciones en Windows.
- ESET recomienda implementar un [dispositivo virtual de ESET PROTECT](#) preconfigurado (que se ejecute en CentOS Linux) si usa un hipervisor. Su implementación es rápida y más directa que la instalación en Windows.

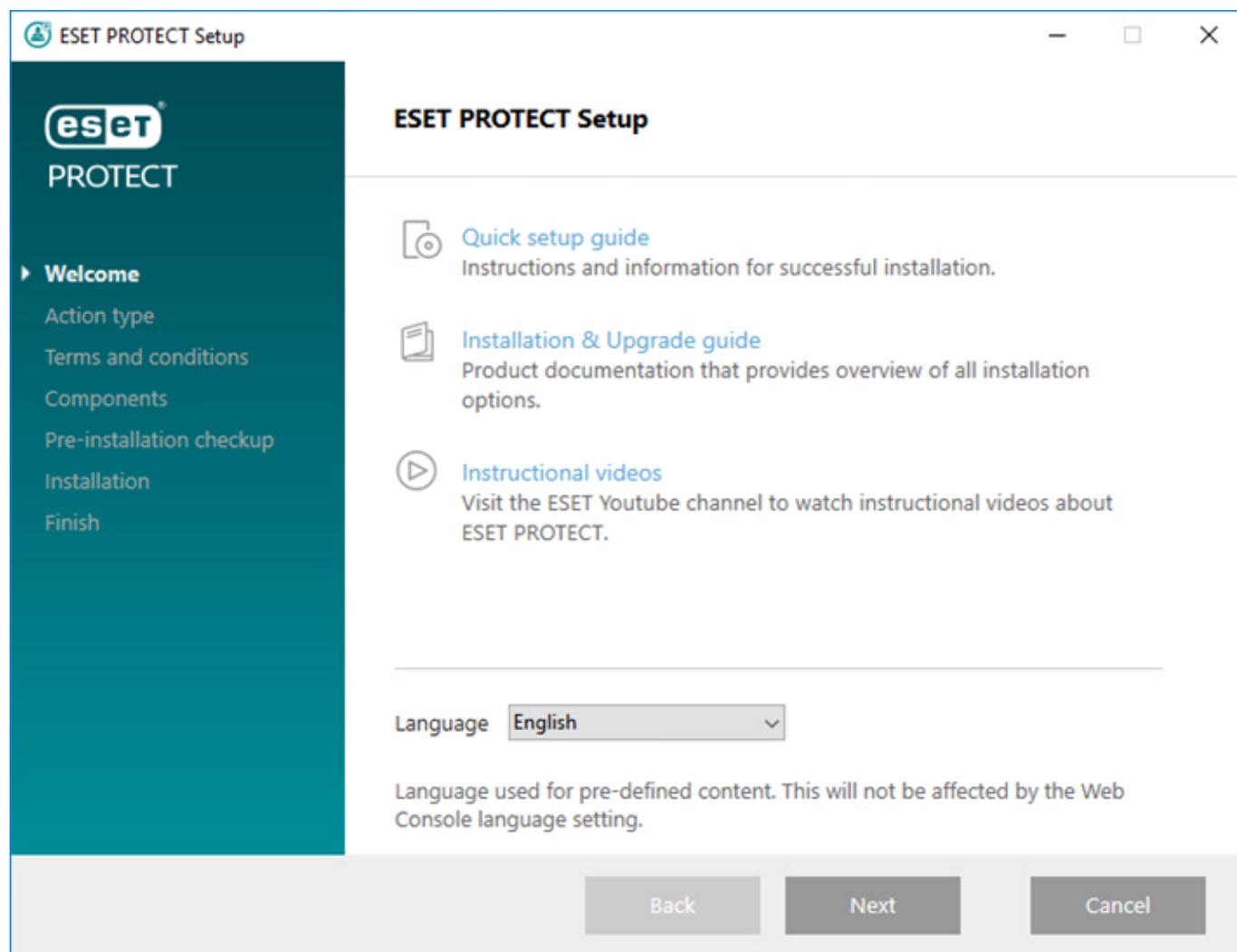
i Si está actualizando desde una versión anterior de ESET PROTECT o ESMC 7.x, siga [estas instrucciones](#).

Instalación todo en uno de ESET PROTECT Server

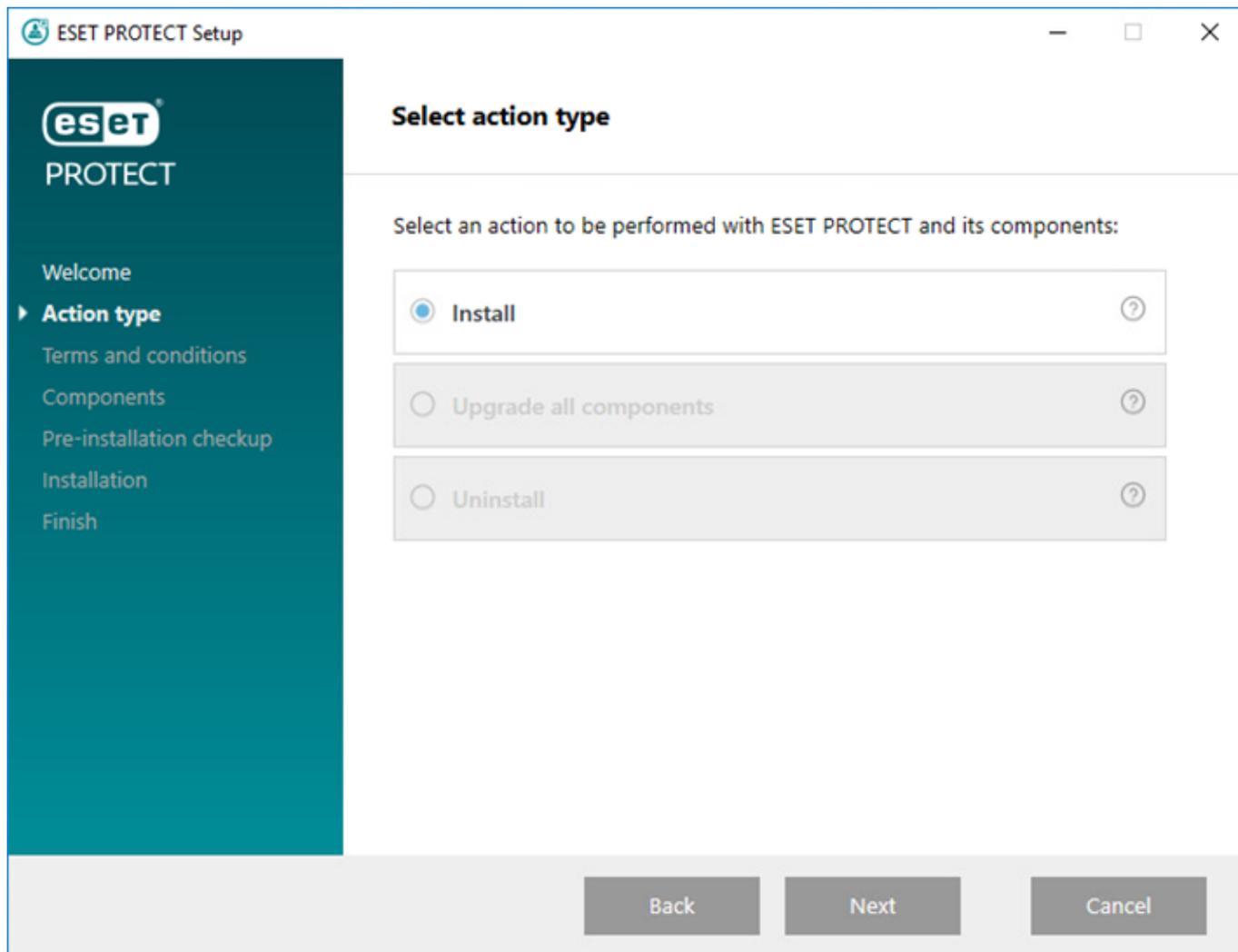
- i**
- Otra alternativa es implementar un [dispositivo virtual de ESET PROTECT](#) preconfigurado (si usa un hipervisor).
 - Si está actualizando desde una versión anterior de ESET PROTECT o ESMC 7.x, siga [estas instrucciones](#).

El [Instalador todo en uno de ESET PROTECT](#) solo está disponible para sistemas operativos Windows. El instalador todo en uno le permite instalar todos los componentes de ESET PROTECT con el asistente de instalación de ESET PROTECT.

1. Abra el paquete de instalación. En la pantalla de bienvenida, use el menú desplegable **Idioma** para ajustar la configuración de idioma. Haga clic en **Siguiente** para continuar.



2. Seleccione **Instalar** y haga clic en **Siguiente**.



3. Desactive la casilla de verificación situada junto a **Participar en el programa para la mejora del producto** si no acepta enviar informes de bloqueo y datos de telemetría anónimos a ESET (versión y tipo de sistema operativo, versión del producto de ESET y otra información específica del producto). Si la casilla de verificación se deja seleccionada, los informes de bloqueo y datos de telemetría se enviarán a ESET. Tras aceptar el EULA, haga clic en **Siguiente**.

4. Seleccione los componentes que desee instalar y haga clic en **Siguiente**.

[Microsoft SQL Server Express](#)

- El [instalador todo en uno](#) de ESET PROTECT 9.0 instala Microsoft SQL Server Express 2019 de forma predeterminada.

OSi utiliza una versión anterior de Windows (Server 2012 o SBS 2011), Microsoft SQL Server Express 2014 se instalará de forma predeterminada.

OEl instalador genera automáticamente una contraseña aleatoria para la autenticación de la base de datos (almacenada en `%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini`).

Microsoft SQL Server Express tiene un límite de tamaño de 10 GB en cada base de datos relacional. No recomendamos el uso de Microsoft SQL Server Express:



- En entornos empresariales o redes de gran tamaño.
- Si desea usar ESET PROTECT con [ESET Enterprise Inspector](#).

• Si ya tiene otra [versión compatible](#) de Microsoft SQL Server o MySQL instalada, o tiene previsto conectarse a una instancia de SQL Server diferente, desmarque la casilla de verificación situada junto a **Microsoft SQL Server Express**.

• [No instale SQL Server en un controlador de dominio](#) (por ejemplo, Windows SBS o Essentials). Le recomendamos que instale ESET PROTECT en un servidor diferente o que no seleccione el componente SQL Server Express durante la instalación (necesita utilizar su SQL o MySQL Server existente para ejecutar la base de datos de ESET PROTECT).

[Agregar certificado HTTPS personalizado para la consola web](#)

- Seleccione esta opción si desea usar un certificado HTTPS personalizado para ESET PROTECT Web Console.
- Si no selecciona esta opción, el instalador genera automáticamente un nuevo almacén de claves para Tomcat nuevo (un certificado HTTPS autofirmado).

[Proxy HTTP Apache](#)

La opción **Proxy HTTP Apache** está diseñada solo para redes pequeñas o centralizadas sin clientes en itinerancia. Si selecciona esta opción, el instalador configura los clientes para tunelar la comunicación con ESET mediante un proxy instalado en la misma máquina que ESET PROTECT Server. Esta conexión no funcionará si no hay visibilidad de red directa entre los clientes y ESET PROTECT Server.

• El uso del proxy HTTP puede ahorrar gran cantidad de ancho de banda en los datos descargados de Internet y mejorar las velocidades de descarga de las actualizaciones de los productos. Le recomendamos que marque la casilla de verificación situada junto a **Proxy HTTP Apache** si va a administrar más de 37 ordenadores desde ESET PROTECT. También puede optar por [instalar el proxy HTTP Apache más tarde](#).

• Para obtener más información, consulte [¿Qué es el proxy HTTP Apache?](#) y [Diferencias entre el proxy HTTP Apache, la herramienta Mirror y la conectividad directa](#).

• Seleccione **Proxy HTTP Apache** para instalar el proxy HTTP Apache y crear y aplicar políticas (por ejemplo, **Uso de proxy HTTP**, aplicada al grupo **Todos**) para los siguientes productos:

oESET Endpoint para Windows

oESET Endpoint para macOS (OS X) y Linux

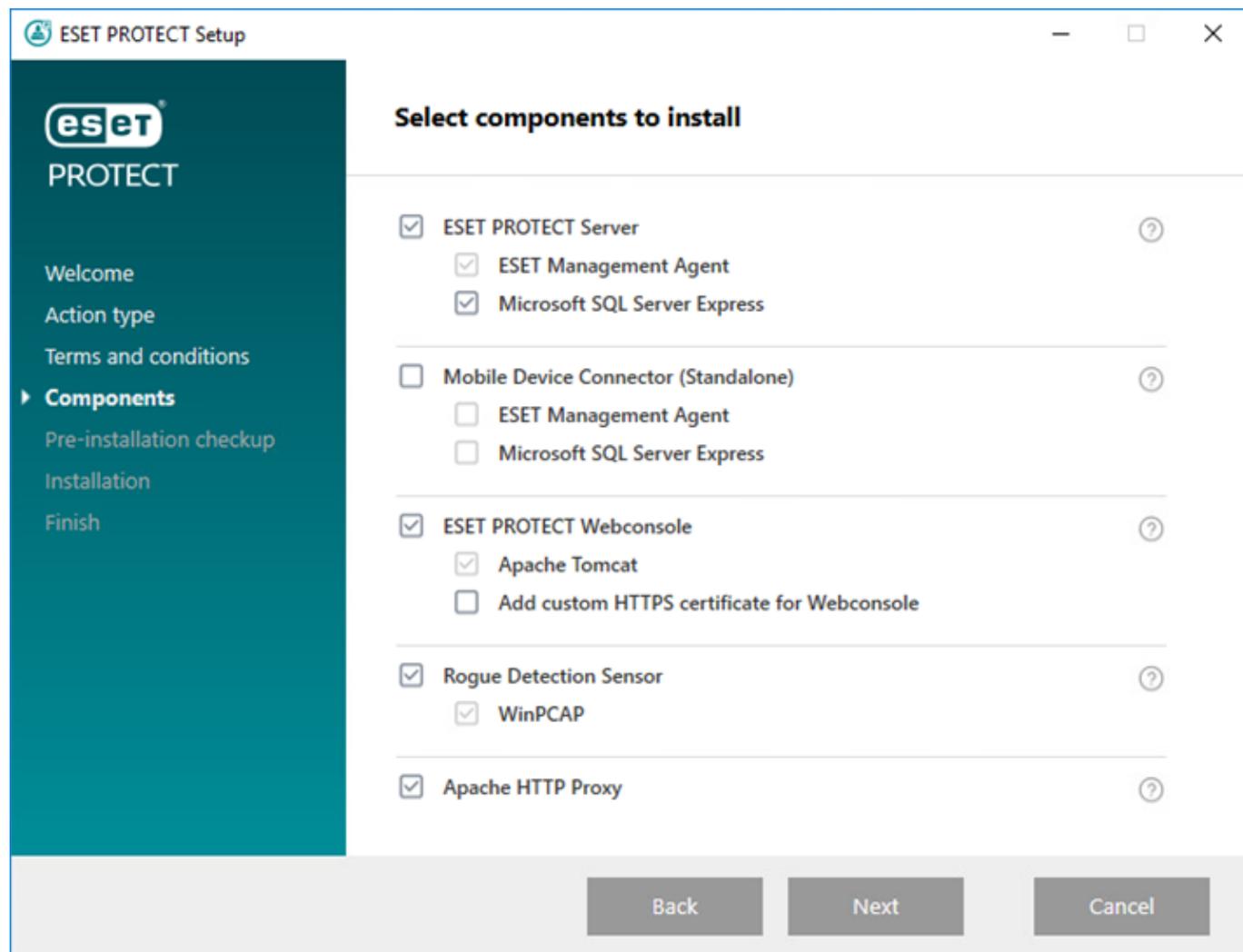
oESET Management Agent

oESET File Security para Windows Server (6+)

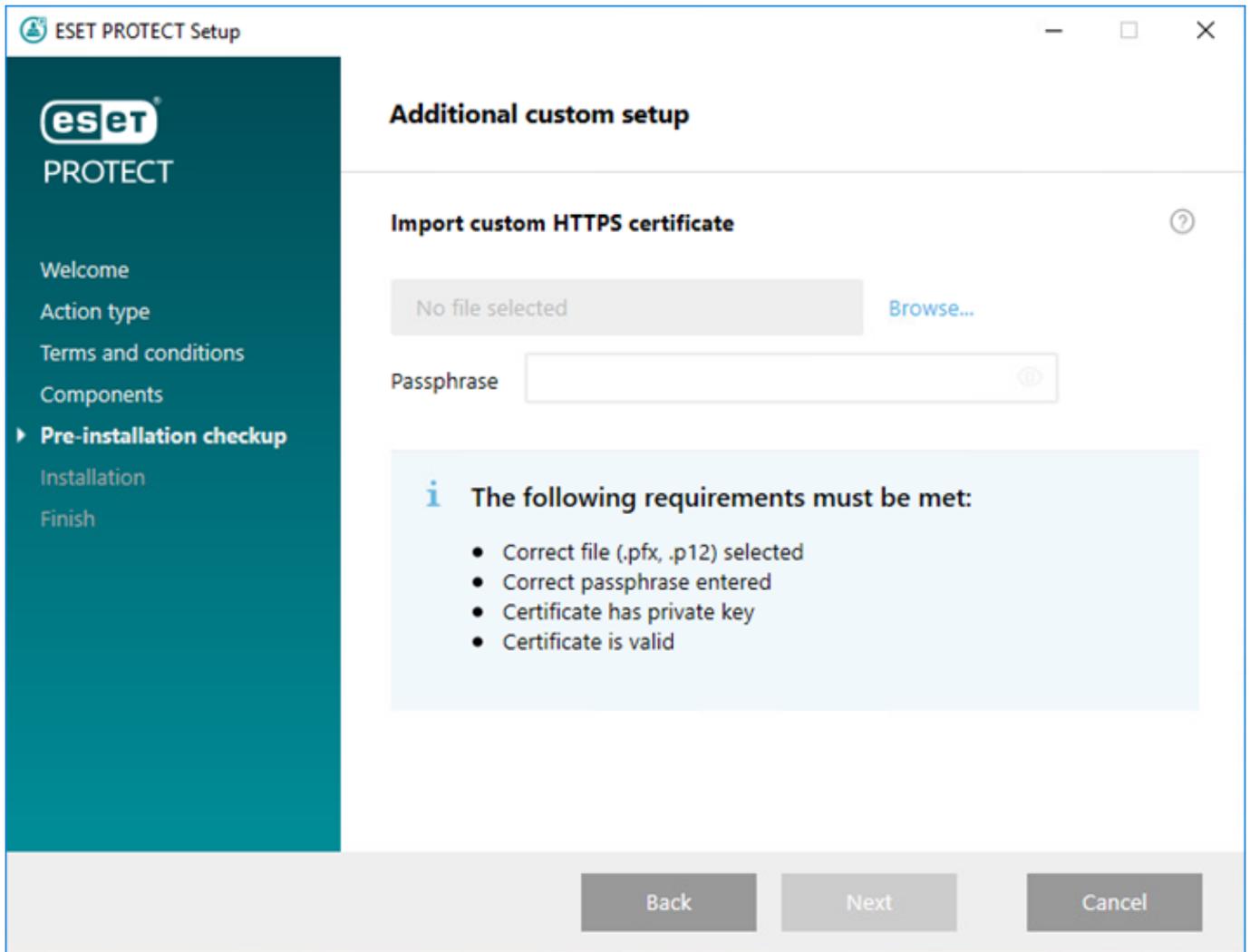
oESET Server Security para Windows (8 o posterior)

oCaché local compartida de ESET

La política activa el proxy HTTP para los productos afectados. El host del proxy HTTP está en la dirección IP local y el puerto 3.128 de ESET PROTECT Server. La autenticación se desactiva. Puede copiar esta configuración en otra política si necesita configurar otros productos.



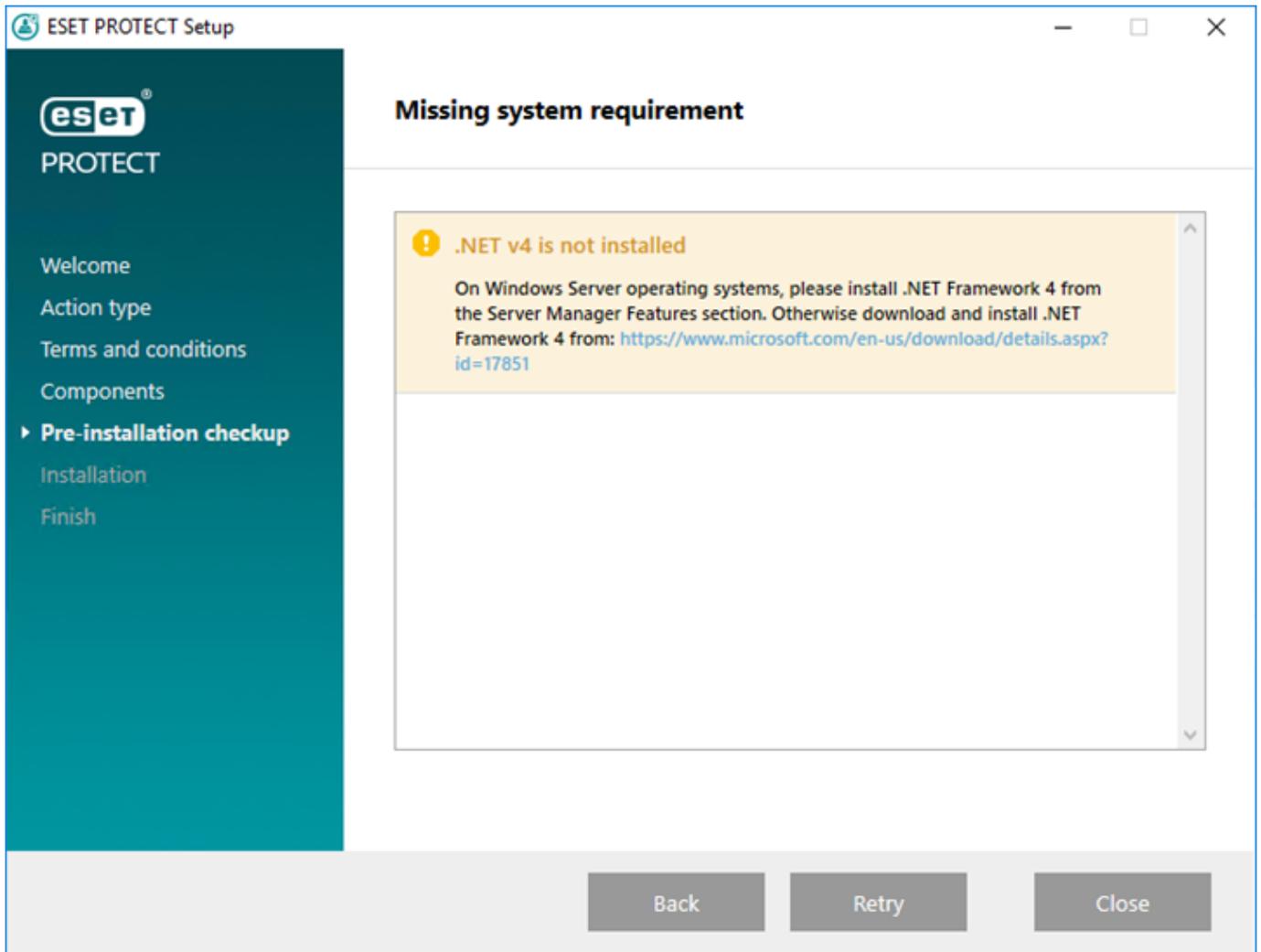
5. Si ha seleccionado **Agregar certificado HTTPS personalizado para la consola web**, haga clic en **Examinar**, seleccione un certificado válido (archivo *.pfx* o *.p12*) y escriba la **contraseña** (o deje el campo vacío si no hay contraseña). El instalador instalará el certificado para el acceso a Web Console en su servidor Tomcat. Haga clic en **Siguiente** para continuar.



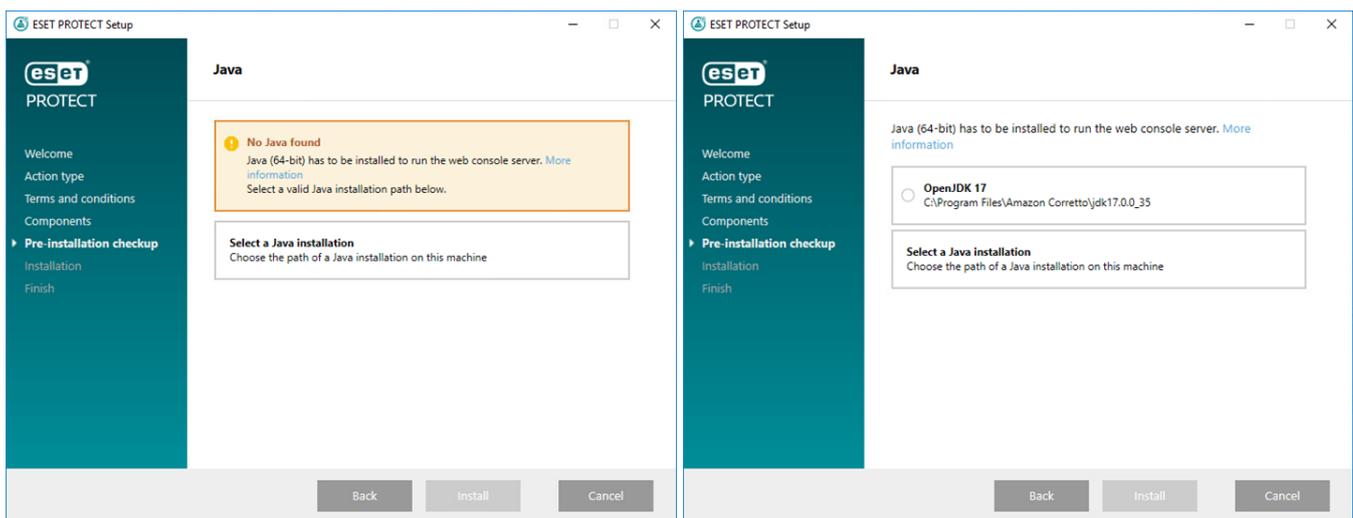
6. Si se encuentran errores durante los requisitos previos, abórdelos como corresponde. Asegúrese de que su sistema cumple con todos los [requisitos previos](#).

[^ .NET v4 no está instalado](#)

[Instalar .NET Framework](#)



[No se encontró Java/se detectó Java \(64 bits\)](#)



Si tiene instaladas en su sistema varias versiones de Java, le recomendamos que desinstale las versiones de Java anteriores y mantenga únicamente la versión de [Java](#) compatible.



Desde enero de 2019, las actualizaciones públicas de Oracle JAVA SE 8 para uso empresarial, comercial o de producción requieren una licencia comercial. Si no compra una suscripción de JAVA SE, puede optar por la transición a una alternativa sin coste siguiendo esta guía. Consulte las [versiones compatibles de JDK](#).

a) Para seleccionar la instancia de Java ya instalada, haga clic en **Seleccionar una instalación de Java**, seleccione la carpeta en la que está instalado Java (con una subcarpeta *bin*, por ejemplo, *C:\Program Files\Amazon Corretto\jdk1.8.0_212*) y haga clic en **Aceptar**. El instalador le pregunta si ha seleccionado una ruta de acceso no válida.

b) Haga clic en **Instalar** para continuar o **cambiar** para cambiar la ruta de instalación de Java.

[El disco del sistema solo tiene 32 MB libres](#)

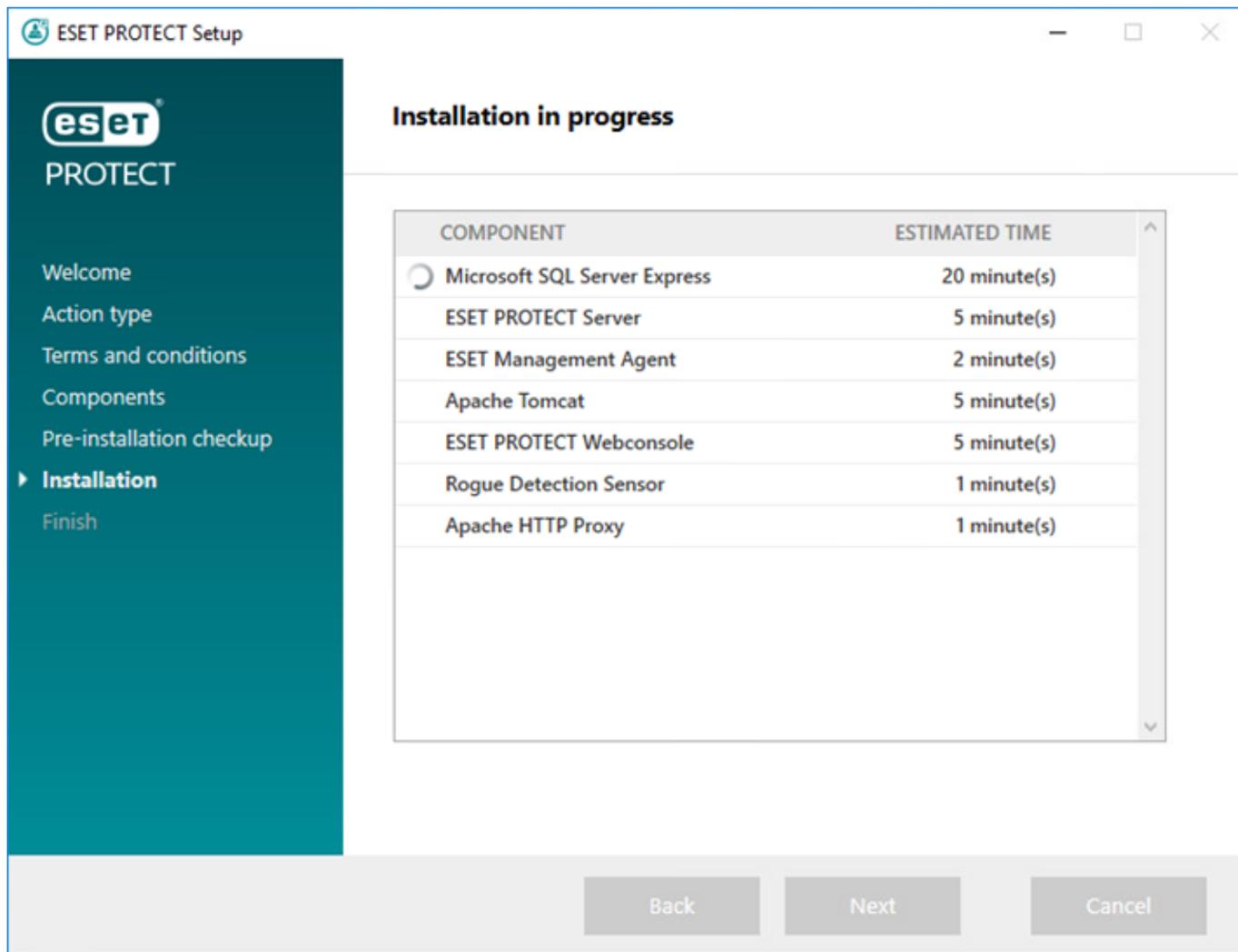
- El instalador puede mostrar esta notificación si su sistema no tiene espacio en disco suficiente para la instalación de ESET PROTECT.
- Para instalar ESET PROTECT y todos sus componentes, debe tener al menos 4.400 MB de espacio libre en el disco.

[En la máquina está instalado ESET Remote Administrator 5.x o una versión anterior, lo que impide que el instalador continúe.](#)

La actualización directa no es compatible; consulte [Migración desde ERA 5.x](#) o [Actualización desde ERA 6.x](#).

7. Cuando finalice la comprobación de los requisitos previos y su entorno cumpla todos los [requisitos](#), se iniciará la instalación. Tenga en cuenta que la instalación puede durar más de una hora, en función del sistema y la configuración de red.

 Cuando la instalación está en curso, el Asistente de instalación de ESET PROTECT no responde.



8. Si decide instalar **Microsoft SQL Server Express** en el paso 4, el instalador realizará una comprobación de la conexión de la base de datos. Si tiene un servidor de base de datos existente, el instalador le pedirá que introduzca los detalles de conexión con la base de datos:

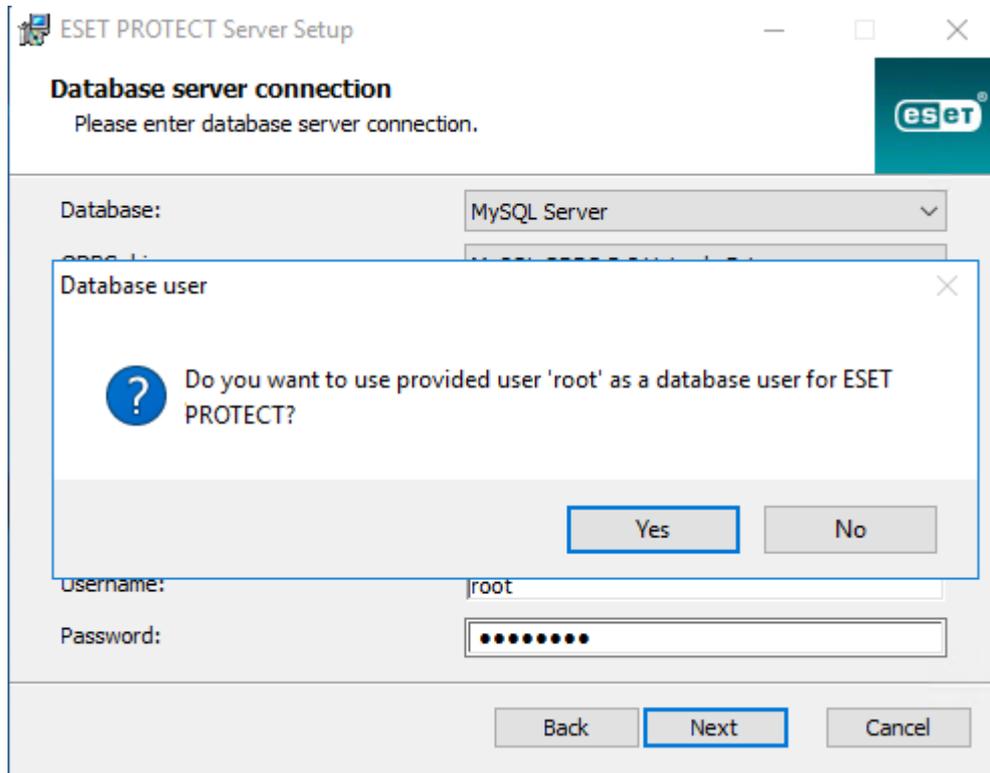
[Configurar la conexión con SQL/MySQL Server](#)

Introduzca el **Nombre de la base de datos**, **Nombre de host**, número de **Puerto** (puede encontrar esta información en el administrador de configuración de Microsoft SQL Server) y los detalles de la **cuenta de la base de datos (nombre de usuario y contraseña)** en los campos correspondientes y, a continuación, haga clic en **Siguiente**. El instalador comprobará la conexión con la base de datos. Si dispone de una base de datos existente (de una instalación de ESMC/ESET PROTECT anterior) en su servidor de base de datos, será eliminada. Puede elegir **Usar base de datos existente y aplicar actualización** o **Quitar la base de datos existente e instalar una versión nueva**.

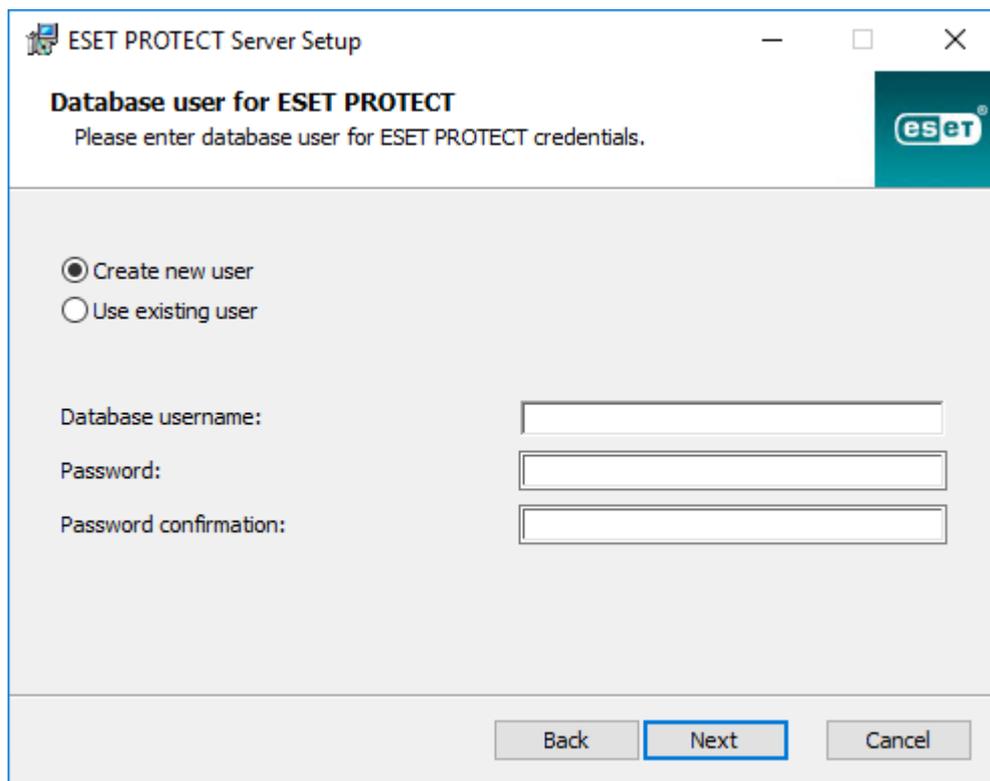
Usar instancia con nombre: si está utilizando una base de datos de MS SQL, también puede marcar la casilla de verificación **Usar instancia con nombre** para usar una instancia de la base de datos personalizada. Puede configurarlo en el campo **Nombre del host** con el formato *NOMBRE_HOST\INSTANCIA_BD* (por ejemplo, *192.168.0.10\ESMCTSQL*). Para las bases de datos en clústeres utilice únicamente el nombre de clúster. Si se selecciona esta opción, no podrá cambiar el puerto de conexión de la base de datos; el sistema utilizará los puertos predeterminados que Microsoft ha definido. Para conectar ESET PROTECT Server a la base de datos de MS SQL instalada en un clúster de conmutación por error, escriba el nombre del clúster en el campo **Nombre del host**.

i Hay dos formas de introducir la información en **Cuenta de la base de datos**. Puede utilizar una **cuenta de usuario de base de datos dedicada** que solo tendrá acceso a la base de datos de ESET PROTECT, o bien una **cuenta SA** (MS SQL) o una **cuenta raíz** (MySQL). Si decide utilizar una cuenta de usuario dedicada, deberá crear la cuenta con privilegios específicos. Para obtener más información, consulte [Cuenta de usuario de base de datos dedicada](#). Si no tiene previsto utilizar una cuenta de usuario dedicada, introduzca la cuenta de administrador (SA o raíz).

Si introdujo una **cuenta de SA** o una **cuenta raíz** en la ventana anterior, haga clic en **Sí** para continuar utilizando la cuenta SA/raíz como usuario de la base de datos de ESET PROTECT.



Si hace clic en **No**, deberá seleccionar **Crear usuario nuevo** (si aún no lo ha creado) o **Utilizar usuario existente** (si tiene una [cuenta de usuario de base de datos dedicada](#)).



9. El instalador le pedirá que introduzca una contraseña para la cuenta de administrador de Web Console. Esta contraseña es importante, ya que la utilizará para iniciar sesión en [ESET PROTECT Web Console](#). Haga clic en **Siguiente**.

ESET PROTECT Server Setup

Web Console user & server connection
Please enter Web Console user password and server connection.

Web Console user: Administrator

Password:

Password confirmation:

Agent port:

Console port:

Back Next Cancel

10. Deje los campos como están o escriba su información corporativa para que aparezca en los detalles de los certificados de ESET Management Agent y ESET PROTECT Server. Si decide introducir una contraseña en el campo **Contraseña de la autoridad**, asegúrese de recordarla. Haga clic en **Siguiente**.

ESET PROTECT Server Setup

Certificate information
Please enter common certificate information below.

Organizational unit:

Organization:

Locality:

State / Country:

Certificate validity: *

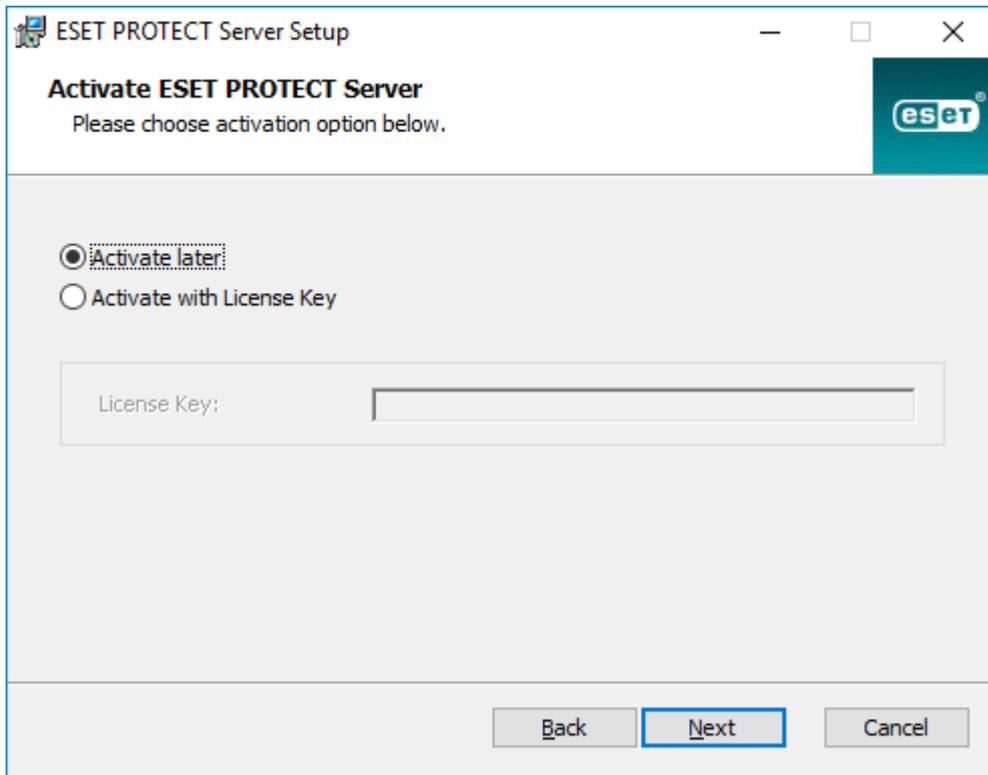
Authority common name: *

Authority password:

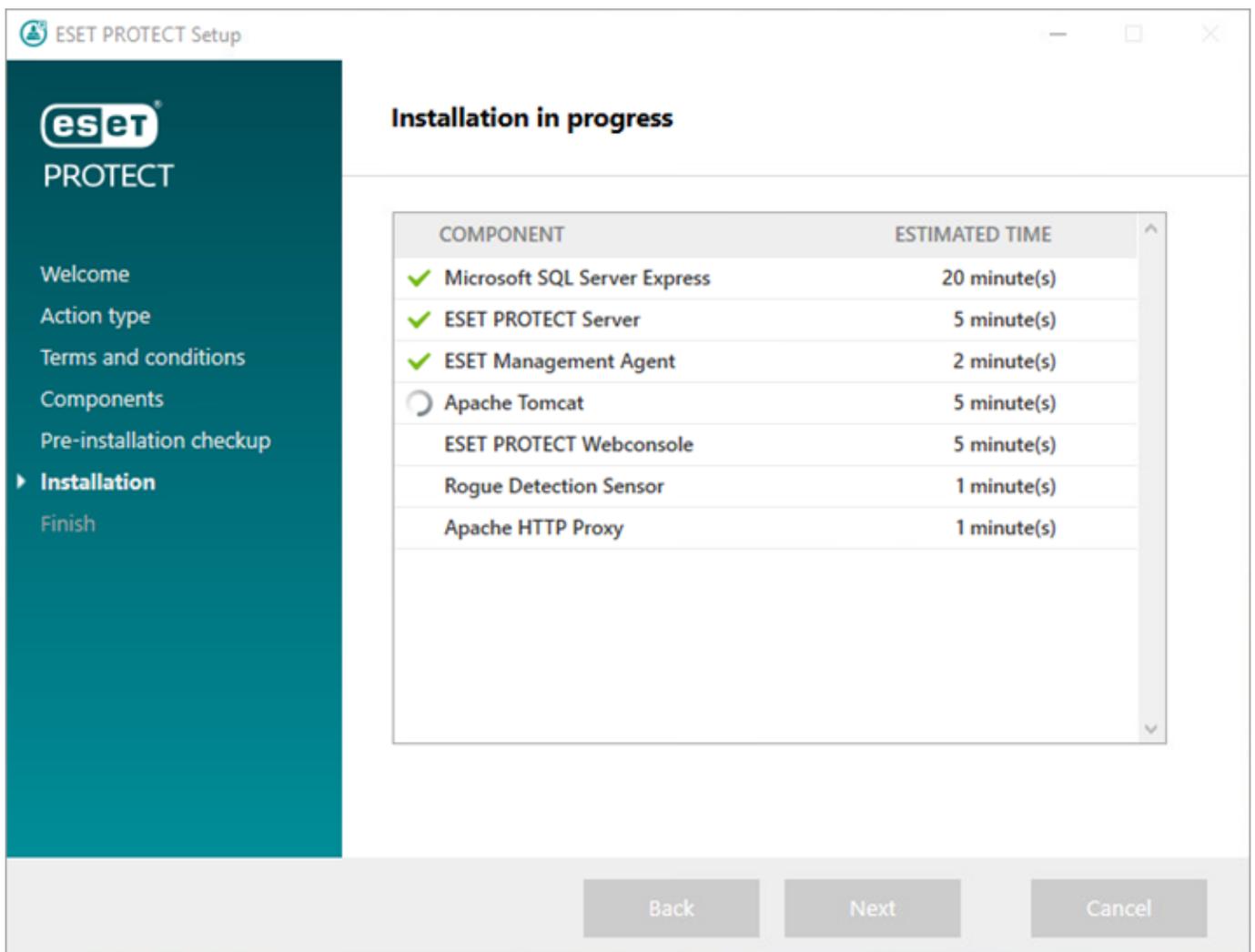
* required fields

Back Next Cancel

11. Introduzca una **clave de licencia** válida (que se incluye en el correo electrónico de compra que recibió de ESET) y haga clic en **Siguiente**. Si está utilizando credenciales de licencias en el formato antiguo (nombre de usuario y contraseña), [conviértalas](#) en una clave de licencia. También puede optar por **Activar más tarde** (consulte el capítulo [Activación](#) para obtener instrucciones adicionales).



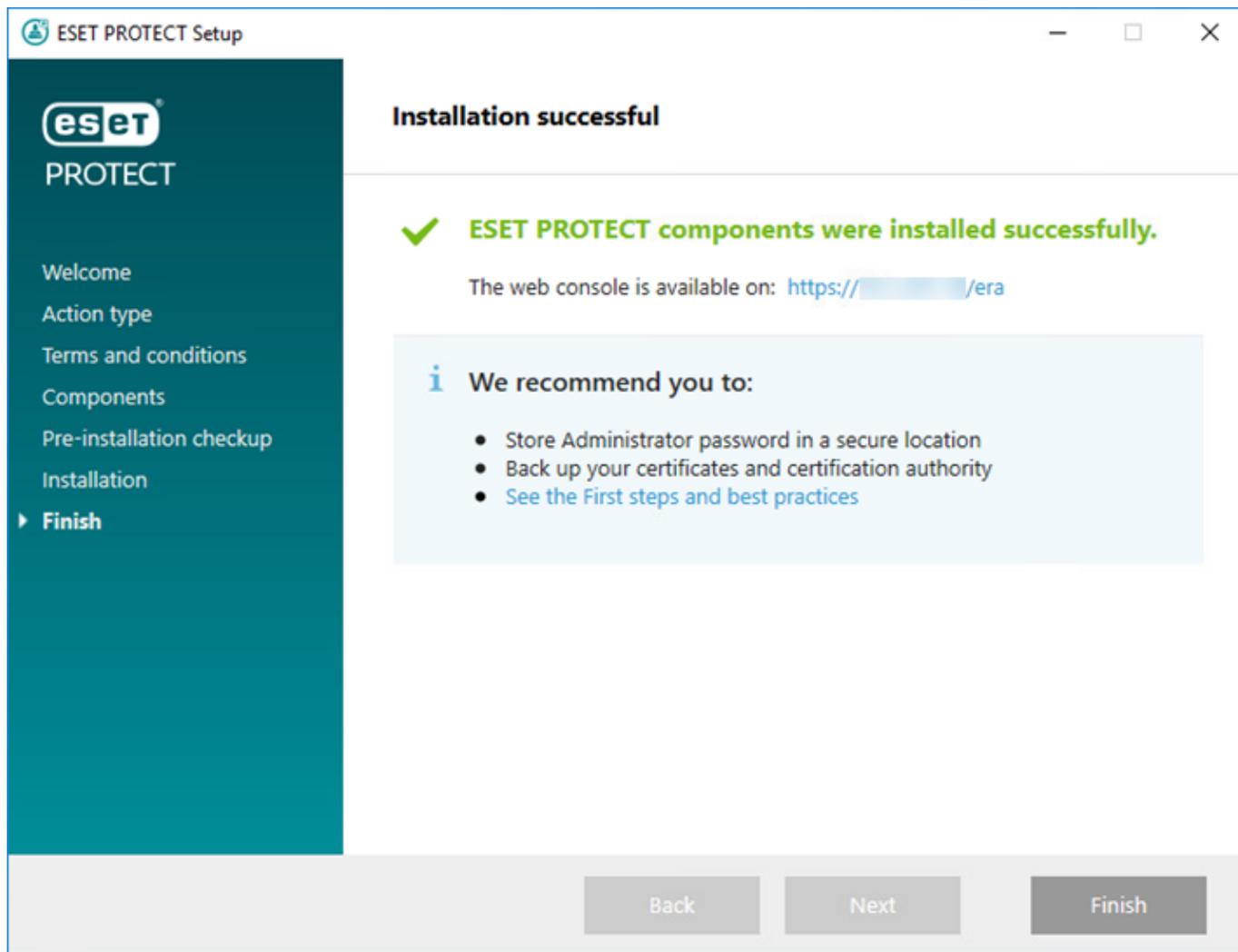
12. Verá el progreso de la instalación.



13. Si ha seleccionado la instalación de **Rogue Detection Sensor**, aparecerá la ventana de instalación del

controlador WinPcap. Asegúrese de seleccionar la casilla de verificación **Iniciar automáticamente el controlador WinPcap en el momento de inicio**.

14. Cuando finalice la instalación, aparecerá el mensaje "Los componentes de ESET PROTECT se han instalado correctamente" además de la dirección URL de ESET PROTECT Web Console. Haga clic en la dirección URL para abrir [Web Console](#) o haga clic en **Finalizar**.



Si la instalación no finaliza correctamente:

- Revise los archivos de registro de la instalación en el paquete de instalación todo en uno. El directorio de registros es el mismo que el directorio del instalador todo en uno, por ejemplo:
C:\Users\Administrator\Downloads\x64\logs\
- Consulte [Resolución de problemas](#) para conocer los pasos adicionales para resolver su problema.

Pasos posteriores a la instalación

Tras la instalación de ESET PROTECT puede iniciar la configuración.

Primeros pasos después de la implementación de ESET PROTECT Server

1. Conéctese a [ESET PROTECT Web Console](#).

2. Lea las instrucciones del [Asistente de inicio](#).

3. Agregue sus [licencias](#).

4. [Implemente ESET Management Agent y los productos ESET Endpoint](#) en los ordenadores de su red.

i El [Resumen del estado](#) puede resultarle útil en la configuración inicial de ESET PROTECT.

Cuando instale ESET PROTECT Server en el servidor y las soluciones ESET Endpoint en los clientes, podrá empezar a administrar su red. Consulte la [Guía del administrador](#) para obtener más información sobre cómo administrar productos ESET Endpoint.

Pasos adicionales recomendados

- Utilice [notificaciones](#) e [informes](#) para supervisar el estado de los ordenadores cliente de su entorno, por ejemplo, si desea recibir una notificación sobre determinados tipos de eventos o consultar o descargar un informe.
- Configure una conexión con el [servidor SMTP](#). Esta configuración es opcional: solo si desea recibir [notificaciones](#) o [informes](#) por correo electrónico. Puede configurar ESET PROTECT Server para que envíe notificaciones a su [servidor de Syslog](#).
- Cree un [nuevo usuario de ESET PROTECT Web Console](#).

Implementación de ESET Management Agent y el producto ESET Endpoint

Tras una instalación correcta de ESET PROTECT, es necesario implementar ESET Management Agent y los productos de ESET Endpoint en los ordenadores de la red.

El proceso de implementación conlleva los siguientes pasos:

1. [Creación del paquete de implementación](#)
2. [Instalación del paquete de implementación](#)

Consulte también [otras opciones de implementación](#). Si la red es de un tamaño considerable, se recomienda usar [ESET Remote Deployment Tool](#).

Creación del paquete de implementación

El procedimiento de creación de un paquete de instalador integral (que incluye ESET Management Agent y un producto de seguridad de ESET) es similar a un [asistente de inicio](#).

Haga clic en **Otras opciones de implementación** en la sección **Vínculos rápidos** de la barra de menús. En la ventana **Implementar agente**, haga clic en **Crear instalador** bajo **Crear instalador integral (solo en Windows)**. Se abrirá la ventana **Crear instalador integral**.

 El paquete del instalador es un archivo .exe, y solo es válido para sistemas operativos Microsoft Windows.

Básico

Desactive la casilla de verificación situada junto a **Participar en el programa para la mejora del producto** si no acepta enviar informes de bloqueo y datos de telemetría anónimos a ESET (versión y tipo de sistema operativo, versión del producto de ESET y otra información específica del producto). Si la casilla de verificación se deja seleccionada, los informes de bloqueo y datos de telemetría se enviarán a ESET.

Contenido del paquete: marque las casillas de verificación de las siguientes opciones:

- **Management Agent:** si no selecciona otros elementos en el **Contenido del paquete**, el instalador solo incluirá ESET Management Agent. Seleccione esta opción si quiere instalar el producto de seguridad de ESET en el ordenador cliente posteriormente o si el ordenador cliente ya tiene un producto de seguridad de ESET instalado.
- **Producto de seguridad:** incluya el producto de seguridad de ESET con ESET Management Agent. Seleccione esta opción si el ordenador cliente no tiene ningún producto de seguridad de ESET instalado y quiere instalarlo con ESET Management Agent.
- **Cifrado de disco completo:** la opción de cifrado solo está visible si la licencia de [ESET Full Disk Encryption](#) está activa.
- **Enterprise Inspector Agent:** incluya ESET Enterprise Inspector Agent en el instalador.

Producto de seguridad

1. **Licencia** (Opcional): puede agregar una licencia con uno de los métodos descritos en [Administración de licencias](#). Si ya tiene licencias en [Administración de licencias](#), solo tiene que elegir la licencia que se utilizará para activar el producto de seguridad de ESET durante la instalación. Si no elige una licencia, puede crear un instalador sin ella y [activar el producto posteriormente](#). Solo el administrador cuyo grupo de inicio esté establecido en **Todo** y tenga permiso de **Escritura** para las licencias de ese grupo puede agregar o eliminar licencias.
2. **Producto:** seleccione el producto de seguridad de ESET que se instalará junto con ESET Management Agent.

 Si no ve los archivos de instalación de ningún producto, asegúrese de que tiene el repositorio configurado como **AUTOSELECT**. Si desea más información, consulte la sección **Configuración avanzada de Configuración del servidor**.

3. **Idioma:** seleccione la versión del idioma del instalador del producto de seguridad de ESET.

4. También puede seleccionar una **política** para que se aplique al producto de seguridad de ESET durante la instalación.

5. **Ajustes de protección:** marque la casilla de verificación situada junto al ajuste para activarlo para el instalador:

o Activar el sistema de respuesta de ESET LiveGrid® (recomendado)

o Activar la detección de aplicaciones potencialmente indeseables: obtenga más información en este [artículo de la base de conocimiento](#).

Seleccione la casilla junto a **No definir los ajustes de protección ahora (no recomendado)** si no desea definir estos ajustes de protección para el instalador y desea definirlos más tarde a través de la política.

6. Marque la casilla **Acepto los términos del Contrato de licencia para el usuario final y la Política de privacidad de la aplicación**. Consulte el [Acuerdo de licencia para el usuario final \(EULA\)](#), [los Términos de uso y la Política de privacidad de los productos de ESET](#) para obtener más información.

Enterprise Inspector Agent

Requisitos de ESET Enterprise Inspector Agent:

- Debe tener una licencia de ESET Enterprise Inspector para activar ESET Enterprise Inspector Agent.
- [Un producto de seguridad de ESET compatible](#) instalado en el ordenador administrado.

1. **Licencia** (opcional): ESET le recomienda seleccionar la licencia de ESET Enterprise Inspector para activar ESET Enterprise Inspector Agent durante la instalación. Si crea el instalador sin la licencia, puede activar ESET Enterprise Inspector Agent más tarde.

2. **Producto o versión:** seleccione la versión de ESET Enterprise Inspector Agent. Aparece preseleccionada la versión disponible más reciente.

3. **Política de configuración** (opcional): seleccione una política de ESET Enterprise Inspector Agent para aplicar la configuración de la política durante la instalación de ESET Enterprise Inspector Agent.

4. Marque la casilla **Acepto los términos del Contrato de licencia para el usuario final y la Política de privacidad de la aplicación**. Consulte el [Acuerdo de licencia para el usuario final \(EULA\)](#), [los Términos de uso y la Política de privacidad de los productos de ESET](#) para obtener más información.

5. Escriba el **Nombre de host del servidor** de ESET Enterprise Inspector y el **puerto** de conexión especificado durante la instalación del servidor de ESET Enterprise Inspector (el puerto predeterminado es 8093).

6. Seleccione la **autoridad certificadora** para conectarse al servidor de ESET Enterprise Inspector.

Certificado

El certificado de igual y la autoridad certificadora de ESET PROTECT se seleccionan automáticamente según los certificados disponibles. Para utilizar un certificado que no sea el seleccionado automáticamente, haga clic en **Certificado de ESET PROTECT** para ver una lista de los certificados disponibles y, a continuación, seleccione el que quiera utilizar. Para utilizar su propio [Certificado personalizado](#), haga clic en el botón de opción y cargue un archivo de certificado *.pfx*.

Introduzca la **Contraseña del certificado** si es necesario. Por ejemplo, si especificó la contraseña durante la instalación de ESET PROTECT, o si está utilizando un certificado personalizado con contraseña. De lo contrario, deje en blanco el campo **Contraseña del certificado**.

 La frase de contraseña del certificado no puede contener los siguientes caracteres: " \ Este caracteres provocan un error crítico durante la inicialización del agente.

 Tenga en cuenta que es posible extraer la **Contraseña del certificado** porque está incrustada en el archivo `.exe`.

Avanzado

En esta sección puede personalizar el paquete del instalador todo en uno:

1. También puede cambiar el **Nombre** e introducir una **Descripción** del paquete del instalador.
2. Haga clic en **Seleccione las etiquetas** para [asignar etiquetas](#).
3. **Grupo principal (opcional)**: seleccione el grupo principal en el que se situará el ordenador tras la instalación. Puede seleccionar un grupo estático existente o crear un nuevo grupo estático a los que se les asignará el dispositivo una vez implementado el instalador.
4. **ESET AV Remover**: marque la casilla de verificación para desinstalar o quitar por completo otros programas antivirus del dispositivo de destino.
5. **Configuración inicial del instalador (opcional)**: utilice esta opción si desea aplicar una [política de configuración](#) a ESET Management Agent. Haga clic en **Seleccionar** en **Configuración del agente (opcional)** y elija en la lista de políticas disponibles. Si ninguna de las políticas predefinidas es adecuada, puede crear [una nueva política](#) o personalizar las existentes.
6. **Nombre de cliente del servidor (opcional)**: escriba el nombre de cliente o la dirección IP de ESET PROTECT. Si es necesario, puede especificar el número de **Puerto** (el valor predeterminado es 2222).
7. Si utiliza un proxy HTTP, marque la casilla de verificación **Activar configuración del proxy HTTP** y especifique la configuración del proxy (**Cliente**, **Puerto**, **Nombre de usuario** y **Contraseña**) para establecer la conexión de ESET Management Agent al proxy y permitir el reenvío de comunicaciones entre ESET Management Agent y ESET PROTECT Server. El campo **Cliente** es la dirección del equipo donde se ejecuta el [proxy HTTP](#). El proxy HTTP usa el puerto 3128 de forma predeterminada. Puede establecer un puerto distinto si lo necesita. Asegúrese de establecer el mismo puerto en la configuración del proxy HTTP.

 El protocolo de comunicación entre Agent y ESET PROTECT Server no admite la autenticación. No funcionará ninguna solución proxy que se utilice para reenviar la comunicación del agente a una instancia de ESET PROTECT que requiere autenticación.
Si opta por utilizar un puerto que no es el predeterminado para la Consola web o el agente, puede ser necesario un ajuste del cortafuegos. De lo contrario, la instalación puede fallar.

Active **Usar conexión directa si el proxy HTTP no está disponible** si quiere permitir esta opción de reserva.

8. Haga clic en **Finalizar**.
9. Descargue el paquete de instalación todo en uno generado. Seleccione la versión que desee implementar:

○ **Descargar versión de 32 bits** (por ejemplo, *PROTECT_Installer_x86_en_US.exe*)

○ **Descargar versión de 64 bits** (por ejemplo, *PROTECT_Installer_x64_en_US.exe*)

○ **Descargar la versión ARM64** (por ejemplo, *PROTECT_Installer_arm64.exe*): no puede instalar la versión x86 o x64 de ESET Management Agent o un producto de seguridad de ESET en Windows ARM64.



Todos los datos descargados del repositorio (repositorio de ESET o mirror del repositorio personalizado) están firmados digitalmente por ESET y ESET PROTECT Server verifica los hashes y las firmas PGP de los archivos. ESET PROTECT Server genera el instalador todo en uno a nivel local. Por tanto, el instalador todo en uno no está firmado digitalmente, lo que puede generar una advertencia del navegador web durante la descarga del instalador, o generar una [alerta](#) del sistema operativo e impedir la instalación en sistemas en los que se bloqueen los instaladores no firmados.

10. Ejecute el archivo del paquete de instalación en un ordenador cliente. Instalará ESET Management Agent y el producto de seguridad de ESET en el dispositivo y conectará el dispositivo a ESET PROTECT. Para obtener instrucciones detalladas, consulte la [instalación del paquete de implementación](#). Puede [ejecutar el paquete de instalación en modo silencioso](#) para ocultar la ventana del asistente de instalación.

Instalación del paquete de implementación

Puede crear este paquete del instalador en [ESET PROTECT](#).

El paquete del instalador instala ESET Management Agent y también puede instalar los siguientes componentes (si se seleccionan durante la creación del paquete del instalador):

- Producto de seguridad de ESET (para equipo o servidor)
- [ESET Full Disk Encryption](#)
- [ESET Inspect Connector](#)



- El paquete del instalador se presenta en forma de archivo *.exe* y solo es válido para el sistema operativo Windows.
- Si ejecuta el instalador en un equipo cliente en el que ya están instalados el producto de seguridad de ESET o ESET Management Agent, el instalador lo actualizará a la versión del instalador.
- Debe ejecutar el instalador con la cuenta de administrador integrado o en una cuenta de administrador de dominio (si tiene desactivada la cuenta de administrador integrado). Los demás usuarios no tienen los derechos de acceso suficientes, aunque sean miembros de un grupo de administradores. Por este motivo debe utilizar la cuenta de administrador integrado, ya que la instalación solo se puede completar con la cuenta de administrador local o de dominio.
- Todos los datos descargados del repositorio (repositorio de ESET o un mirror del repositorio personalizado) están firmados digitalmente por ESET y ESET PROTECT Server verifica los hash y las firmas PGP de los archivos. ESET PROTECT Server genera el instalador todo en uno a nivel local. Por tanto, el instalador todo en uno no está firmado digitalmente, lo que puede generar una advertencia del navegador web durante la descarga del instalador, o generar una [alerta](#) del sistema operativo e impedir la instalación en sistemas en los que se bloqueen los instaladores no firmados.
- Tenga en cuenta que es posible extraer datos confidenciales (por ejemplo, la Contraseña del certificado) porque están incrustados en el instalador.
- El instalador de ESET Endpoint Antivirus/Security creado en ESET PROTECT 8.1 y versiones posteriores es compatible con el modo multisesión de Windows 10 Enterprise for Virtual Desktops y Windows 10.

Proceso de instalación

- Si quiere ejecutar el instalador sin que se muestre ningún cuadro de diálogo, siga las [instrucciones para una instalación silenciosa](#).
- Si se produce algún error durante la instalación, consulte en la [sección de resolución de problemas](#) los errores de instalación más frecuentes.

1. Ejecute el paquete del instalador.

Antes de instalar el producto de seguridad de ESET, asegúrese de desinstalar del ordenador cualquier producto de seguridad de terceros.

- Si optó por incluir **ESET AV Remove** al crear el paquete de instalación, **ESET AV Remove** le ayudará a desinstalar o quitar completamente el software de seguridad de terceros:

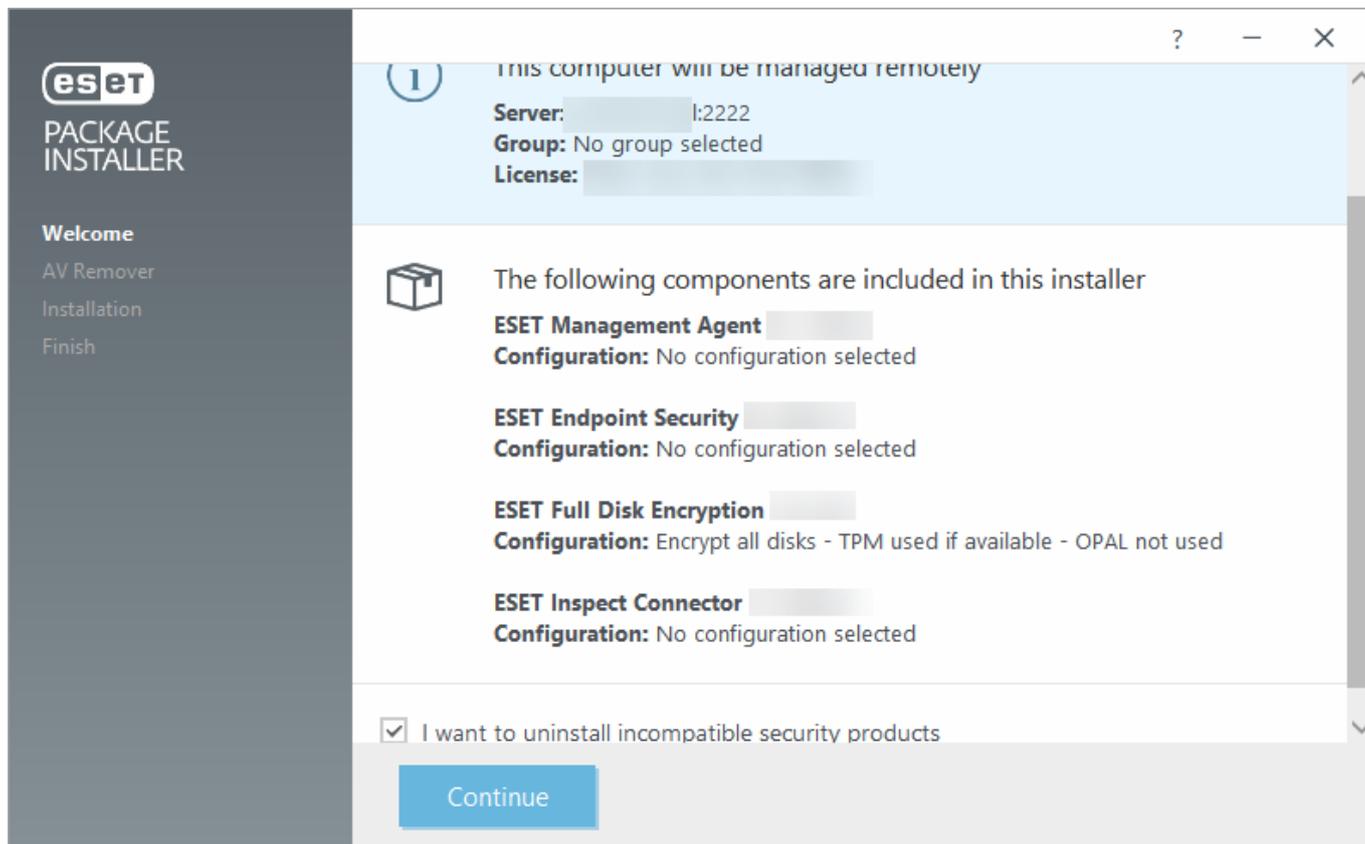
a) Marque la casilla de verificación **Quiero desinstalar los productos de seguridad no compatibles** para quitar o desinstalar el software de seguridad de terceros que esté en ejecución o instalado en su ordenador. Consulte la [lista de software compatible](#).

b) Haga clic en **Continuar**.

c) Tras el análisis de las aplicaciones instaladas, seleccione la casilla situada junto a las aplicaciones que quiera quitar y haga clic en **Quitar**. Consulte el [artículo de la Base de conocimiento](#) sobre ESET AV Remove si desea más información.

d) Cuando ESET AV Remove desinstale el software de seguridad de terceros, o si no ha quitado ninguna aplicación, haga clic en **Continuar con la instalación**.

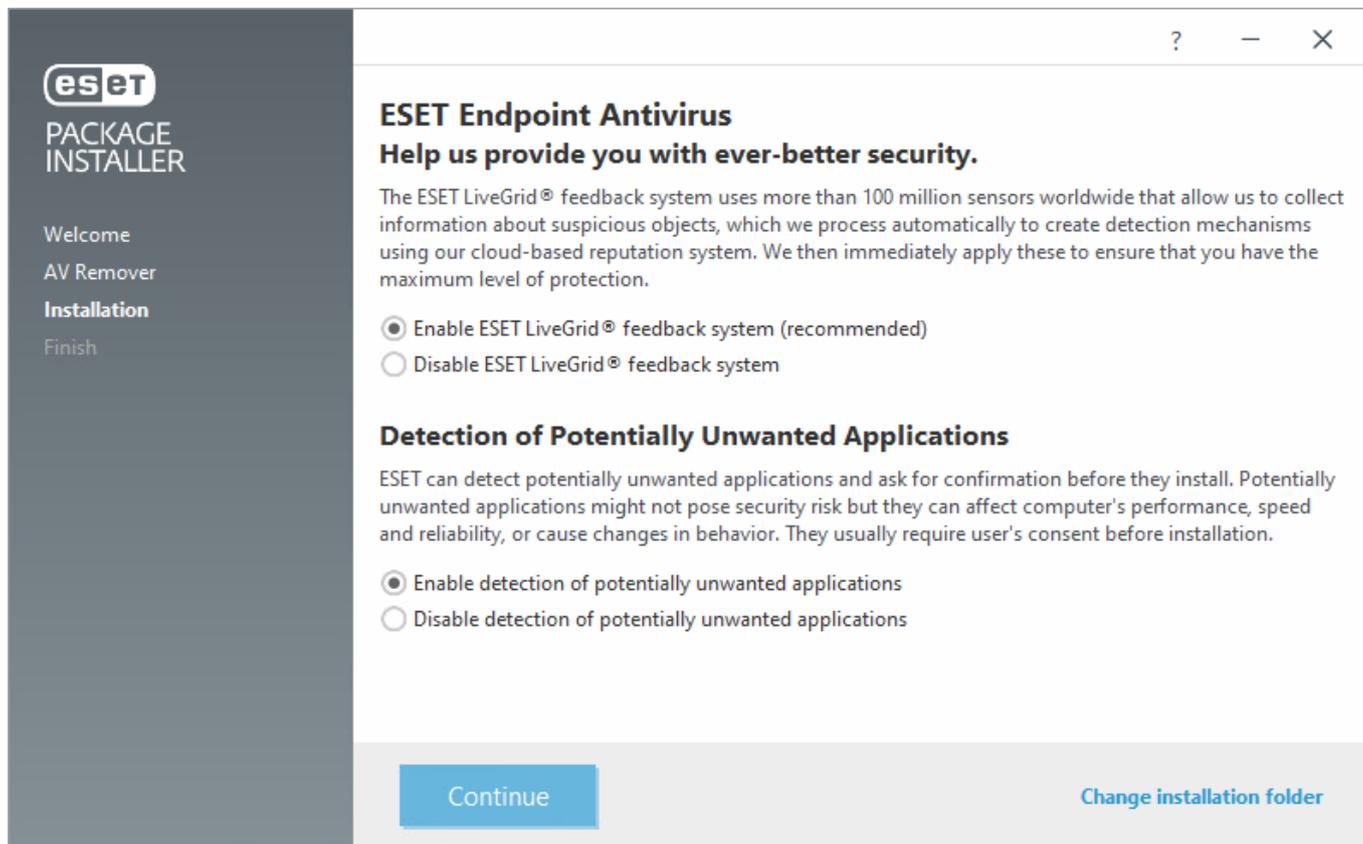
- Si no utiliza ningún producto de seguridad de terceros en su ordenador local, haga clic en **Continuar**.



2. **Ajustes de protección:** marque la casilla de verificación situada junto al ajuste para activarlo para el instalador:

o **Activar el sistema de respuesta de ESET LiveGrid® (recomendado)**

o **Activar la detección de aplicaciones potencialmente indeseables:** obtenga más información en este [artículo de la base de conocimiento](#).



3. Una vez completada la instalación, haga clic en **Hecho**. El producto de seguridad de ESET se abrirá automáticamente. Puede consultar el registro de estado (`C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.html`, esta ubicación está oculta de forma predeterminada) en el equipo cliente para asegurarse de que ESET Management Agent funcione correctamente. Si hay algún problema con el agente ESET Management Agent instalado (por ejemplo, si no se conecta a ESET PROTECT Server), consulte la sección [Resolución de problemas de conexión del agente](#).

Resolución de problemas

Si se produce algún error durante la instalación, consulte en la [sección de resolución de problemas](#) los errores de instalación más frecuentes.

Otros métodos de implementación

Hay varias formas de implementar ESET Management Agent y los productos ESET Endpoint. Puede implementarlos por separado.

Implementación de ESET Management Agent

Implementación local:

- [Instalador todo en uno](#): el paquete contiene ESET Management Agent y un producto de seguridad de ESET.
- [Live Installer del agente](#)

- [Descargue el agente del sitio web de ESET](#) y utilice la instalación asistida por el servidor o la instalación sin conexión.

Implementación remota (recomendado para redes de gran tamaño):

- [ESET Remote Deployment Tool](#): implemente el [Instalador todo en uno](#) de forma remota.
- [Objeto de política de grupo \(GPO\)](#)
- [Tarea del servidor Implementación de agente](#)

Implementación de productos ESET Endpoint

Tras la implementación de ESET Management Agent puede instalar un producto ESET Endpoint directamente desde ESET PROTECT de dos formas distintas:

- Utilizando la [tarea Instalación del software](#)
- De forma local, utilizando la instalación del producto ESET estándar

ESET Remote Deployment Tool

ESET Remote Deployment Tool permite distribuir con facilidad el [paquete de instaladores](#) creado por ESET PROTECT para implementar ESET Management Agent y productos de seguridad de ESET de forma remota en los ordenadores de una red.

ESET Remote Deployment Tool está disponible de forma gratuita en el [sitio web](#) de ESET como componente de ESET PROTECT independiente. La herramienta de implementación está pensada principalmente para redes pequeñas y medianas, y se ejecuta con privilegios de administrador.

 ESET Remote Deployment Tool solo se utiliza para implementar ESET Management Agent en ordenadores cliente con sistemas operativos Microsoft Windows [compatibles](#).

Requisitos previos de la Herramienta de implementación remota de ESET

 En implementaciones remotas, compruebe que todos los ordenadores cliente disponen de conexión a Internet.

Para poder usar la Herramienta de implementación remota de ESET en Windows se deben cumplir los siguientes requisitos:

- ESET PROTECT Server y ESET PROTECT Web Console deben estar instalados (en un ordenador con Server).
- Deben estar abiertos los puertos correspondientes. Consulte [los puertos utilizados para la implementación remota de ESET Management Agent en un ordenador de destino con el sistema operativo Windows](#).
- El nombre de los paquetes de instalación debe incluir la cadena "x86" o "x64". De lo contrario, la implementación no funcionará.
- Se debe haber [creado](#) y [descargado](#) un paquete instalador agrupado (todo en uno) en su unidad local.

- Es necesario tener permiso para [crear el instalador todo en uno](#).

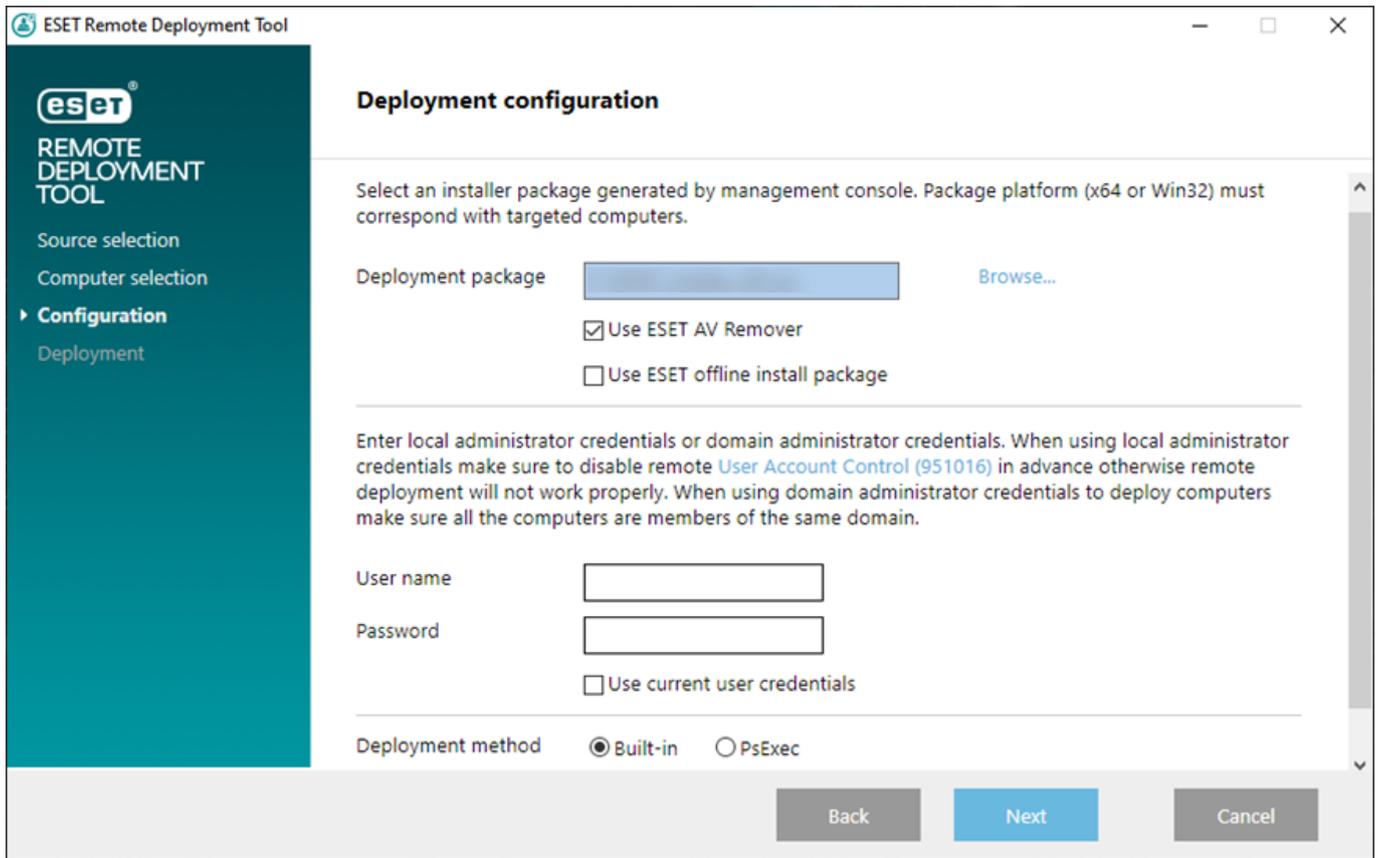
i La implementación puede fallar por diversos motivos. Si tiene cualquier problema con la implementación, lea el [capítulo Resolución de problemas](#) o [Situaciones de ejemplo de implementación de ESET Management Agent verificadas](#).

Para implementar instancias de ESET Management Agent en ordenadores cliente, siga estos pasos:

1. [Descargue](#) ESET Remote Deployment Tool del sitio web de ESET.
2. Asegúrese de que se cumplen todos los [requisitos previos](#).
3. Ejecute la Herramienta de implementación remota de ESET en el ordenador cliente.
4. Seleccione **Agregar ordenadores manualmente**. Tendrá que introducir manualmente la lista de nombres de host o direcciones IP.
5. Introduzca los nombres de host o las direcciones IP y haga clic en **Siguiente**. Cada dirección IP o nombre de host deben estar en una línea nueva.

! Asegúrese de que todos los ordenadores seleccionados tengan la misma plataforma (sistema operativo de 64 bits o 32 bits).

6. Se mostrarán los ordenadores seleccionados para la implementación remota. Asegúrese de que se han agregado todos los ordenadores y, a continuación, haga clic en **Siguiente**.
7. Haga clic en **Examinar** y seleccione el paquete instalador agrupado que ha creado en [ESET PROTECT](#) o [ESET PROTECT Cloud](#) Web Console. También puede seleccionar **Utilizar paquete de instalación sin conexión de ESET** (archivo *.dat*) creado con ESET PROTECT Live Installer. Si no tiene instalada otras aplicaciones seguridad en el ordenador local, desmarque la casilla situada junto a **Usar ESET AV Remover**. ESET AV Remover puede quitar [determinadas aplicaciones](#).
8. Especifique las credenciales de inicio de sesión de los ordenadores de destino. Si los ordenadores forman parte de un dominio, especifique las **credenciales de administrador del dominio**. Si inicia sesión con **credenciales de administración local**, es necesario [desactivar el control de cuentas de usuario remoto en los ordenadores de destino](#). También puede marcar la casilla situada junto a **Usar las credenciales de usuario actuales**, y las credenciales de inicio de sesión se introducirán automáticamente.
9. El **método de implementación** se utiliza para ejecutar programas en ordenadores remotos. El método **Integrado** es un ajuste predeterminado, y es compatible con los mensajes de error de Windows. **PsExec** es una herramienta externa, alternativa al método integrado. Seleccione una de estas opciones y haga clic en **Siguiente**.



Si ha seleccionado **PsExec**, la implementación fallará porque la herramienta no puede aceptar el Acuerdo de licencia para el usuario final de **PsExec**. Para llevar a cabo una implementación correcta, abra la línea de comandos y ejecute el comando **PsExec** manualmente.

10. Cuando la instalación comience, se mostrará "Éxito". Haga clic en **Finalizar** para terminar la implementación. Si la implementación falla, puede exportar una lista de los ordenadores que han fallado. Haga clic en **Examinar** junto al campo **Exportar ordenadores fallidos**, seleccione el archivo **.txt** en el que quiere guardar la lista y, a continuación, haga clic en **Exportar ordenador fallido**.

Progress	
COMPUTER	STATUS
✓ [blurred]	Success

Puede consultar el registro de estado (*C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html*) en la máquina cliente para verificar que el ESET Management Agent funciona correctamente.

Otros métodos para implementar instancias de ESET Management Agent con ESET Remote Deployment Tool

- [Active Directory](#): proporcione las credenciales de Active Directory. Esta opción incluye una exportación de la estructura de Active Directory para su posterior importación en ESET PROTECT.

- [Análisis de red](#): proporcione rangos de IP para analizar los ordenadores de la red.
- [Importar lista](#): proporcione una lista de los nombres de host o las direcciones IP.

Resolución de problemas

i La implementación puede fallar por diversos motivos. Si tiene cualquier problema con la implementación, lea el [capítulo Resolución de problemas](#) o [Situaciones de ejemplo de implementación de ESET Management Agent verificadas](#).

ESET PROTECT Web Console

Inicie sesión en la Consola Web de ESET PROTECT

- En su servidor local de Windows (la máquina que aloja su Web Console):

Haga clic en **Inicio > Todos los programas > ESET > ESET PROTECT Web Console**.

- Desde cualquier lugar con acceso a Internet que le permita acceder a su servidor web, escriba la dirección URL en el siguiente formato (sustituya "yourservername" por el nombre real o la dirección IP de su servidor web): `https://yourservername/era/`

Se abrirá una pantalla de inicio de sesión en el navegador web predeterminado. Si se muestra una advertencia de certificado SSL, agregue la excepción del certificado a su navegador web.

! Utilice un [navegador web compatible](#) para conectarse a ESET PROTECT Web Console.

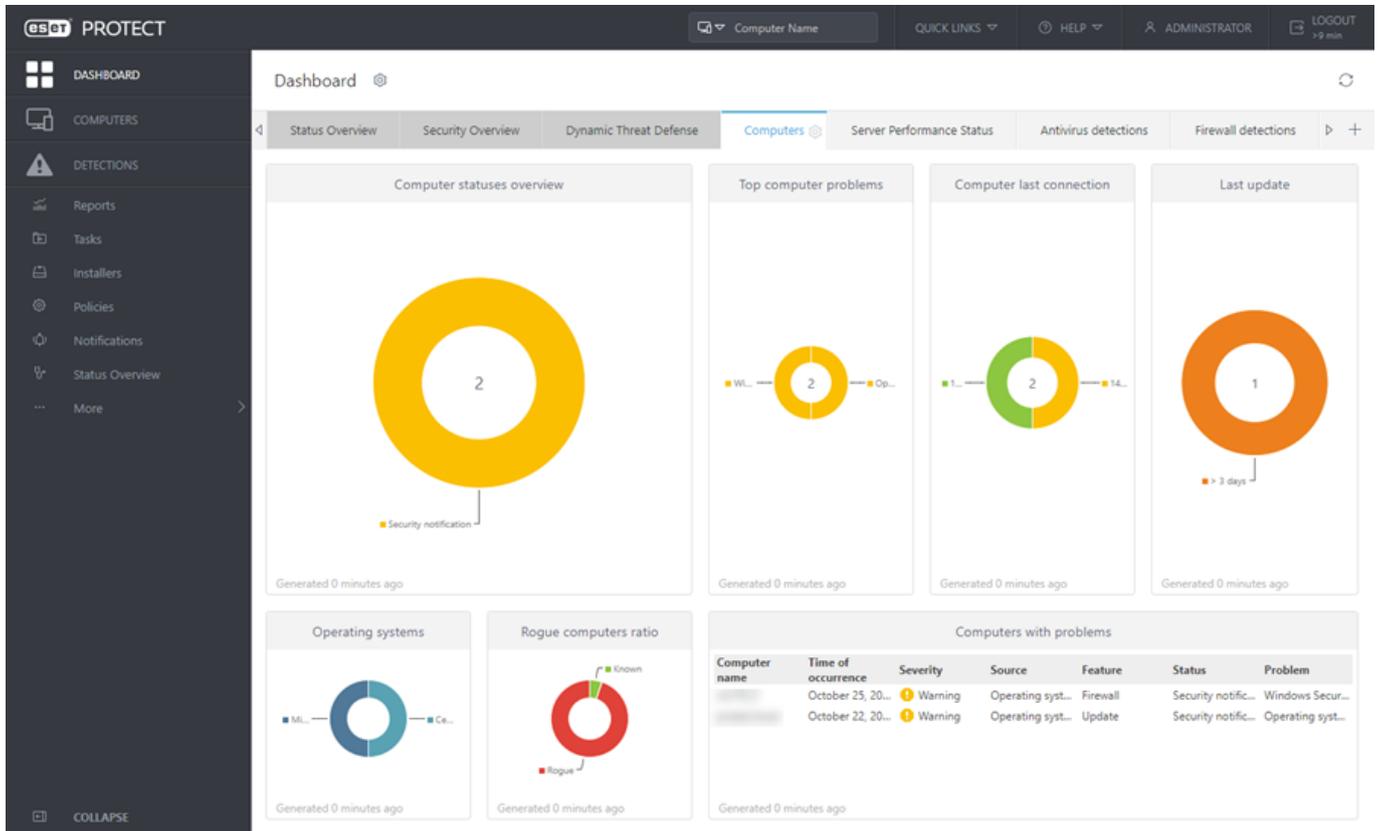
Cuando inicia sesión en Web Console por primera vez, aparece un [Asistente de inicio](#) para ESET PROTECT, y podrá utilizarlo para implementar instancias de ESET Management Agent en ordenadores de su red.

Interfaz de usuario de ESET PROTECT Web Console

La interfaz de usuario de ESET PROTECT Web Console consta de varios elementos:

- Puede utilizar la herramienta **Buscar** en la parte superior de ESET PROTECT Web Console.
- Haga clic en **Vínculos rápidos** para realizar algunas de las acciones de Web Console más utilizadas.
- Si necesita ayuda para trabajar con ESET PROTECT, haga clic en el icono  **Ayuda** situado en la esquina superior derecha y haga clic en **<Current topic> - Ayuda**. Se mostrará la ventana de ayuda correspondiente para la página actual.
- En la esquina superior derecha se muestra el [usuario](#) actual con la cuenta atrás del tiempo de espera de la sesión del usuario. Puede hacer clic en **Cerrar sesión** para cerrar sesión en cualquier momento. Cuando se agote el tiempo de espera de la sesión (debido a la inactividad del usuario), deberá iniciar sesión de nuevo.

- El menú principal de la parte izquierda de Web Console contiene herramientas que pueden utilizar los administradores para administrar las soluciones de seguridad del cliente y la configuración del servidor de ESET PROTECT. Puede utilizar las herramientas de **Más** para configurar el entorno de red y minimizar las necesidades de mantenimiento. También puede configurar [notificaciones](#) y [paneles](#) para controlar el estado de la red.

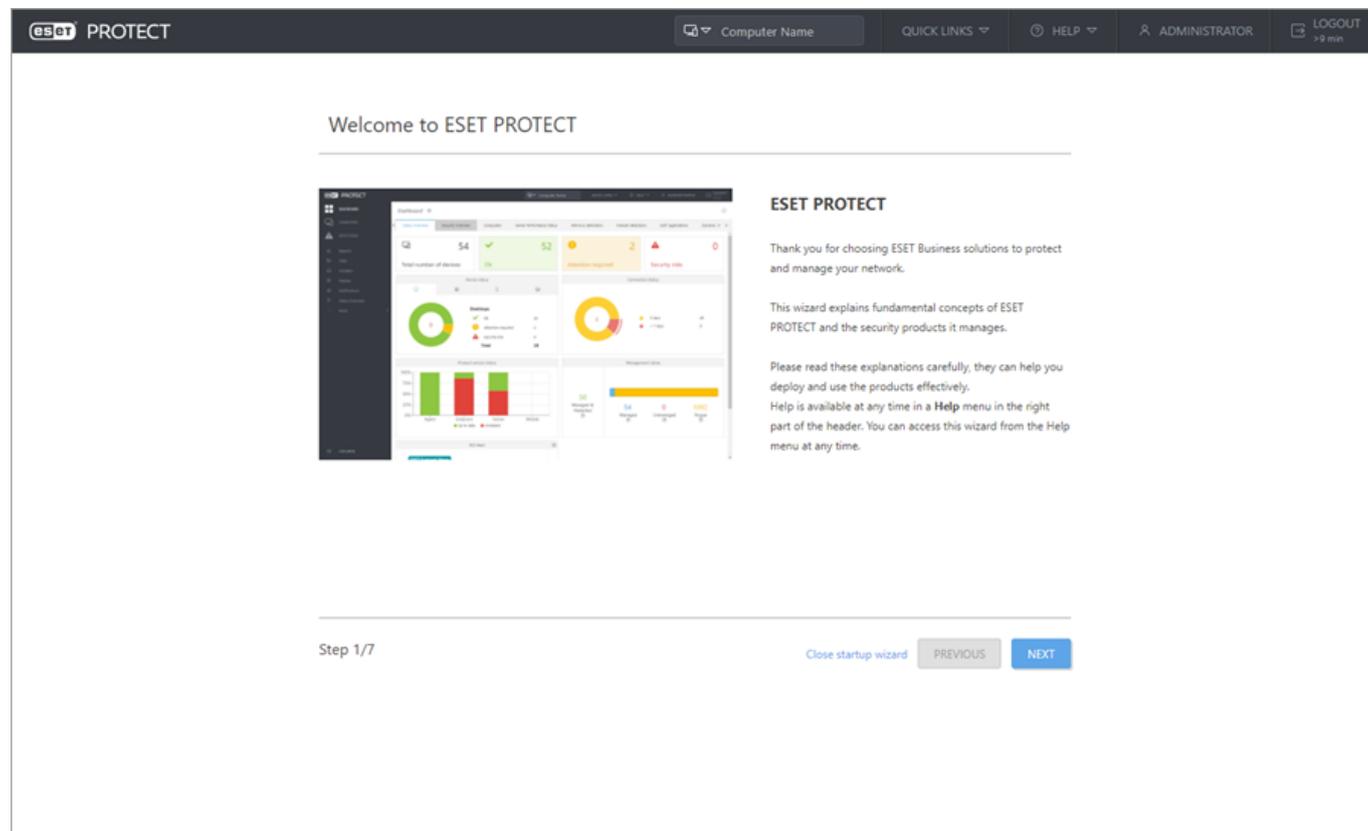


En los temas que se indican a continuación se describen los elementos principales del menú:

Panel
Ordenadores y Grupos
Detecciones
Informes
Tareas
Políticas
Notificaciones
Resumen del estado
*** Más > Exclusiones
*** Más > Cuarentena
*** Más > Conjuntos de permisos y usuarios
*** Más > Administración de licencias
*** Más > Certificados

Asistente de inicio

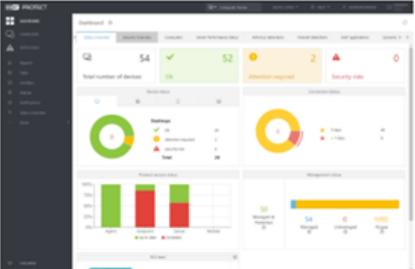
Cuando inicie sesión en Web Console por primera vez, aparecerá un **Asistente de inicio** para ESET PROTECT, y podrá utilizarlo para implementar instancias de ESET Management Agent en ordenadores de su red. Este asistente le ofrecerá una explicación básica de secciones importantes de ESET PROTECT Web Console.



ES ESET PROTECT

Computer Name QUICK LINKS HELP ADMINISTRATOR LOGOUT >9 min

Welcome to ESET PROTECT



ESET PROTECT

Thank you for choosing ESET Business solutions to protect and manage your network.

This wizard explains fundamental concepts of ESET PROTECT and the security products it manages.

Please read these explanations carefully, they can help you deploy and use the products effectively.

Help is available at any time in a **Help** menu in the right part of the header. You can access this wizard from the Help menu at any time.

Step 1/7

Close startup wizard PREVIOUS NEXT

El último paso del asistente de inicio, denominado **Implementación**, le ayuda a crear un paquete del instalador todo en uno (con ESET Management Agent y el producto de seguridad de ESET). También puede [crear un instalador todo en uno para el agente](#) sin usar el asistente si hace clic en **Otras opciones de implementación** en la sección **Vínculos rápidos**.

eset PROTECT Computer Name QUICK LINKS HELP ADMINISTRATOR LOGOUT > 9 min

Deployment

Create an installer for Endpoint deployment

The installer file contains all necessary components (ESET Management Agent, ESET security product) with the necessary configuration and license. Run the installer with admin privileges on computers that are to be managed with ESET PROTECT.

After successful installation, the computers appear in the **Lost & found** Static group in the **Computers** section.

For more deployment options, use the **Quick links** option **Other Deployment Options**.

Choose license
[Add license](#)

Product
ESET Endpoint Security; version [] for windows (WINDOWS), language en_US

Language
English

I accept the [End User License Agreement](#) and acknowledge the [Privacy Policy](#).

Protection settings

The ESET LiveGrid® feedback system
 Enable The ESET LiveGrid® feedback system (recommended)

Detection of Potentially Unwanted Applications
 Enable detection of potentially unwanted applications
 Do not define the Protection settings right now. The end-user will be able to define them during installation. (not recommended)

Product improvement program ⓘ
 Participate in product improvement program

Advanced
 Show advanced settings

Full Disk Encryption
 Show ESET Full Disk Encryption settings

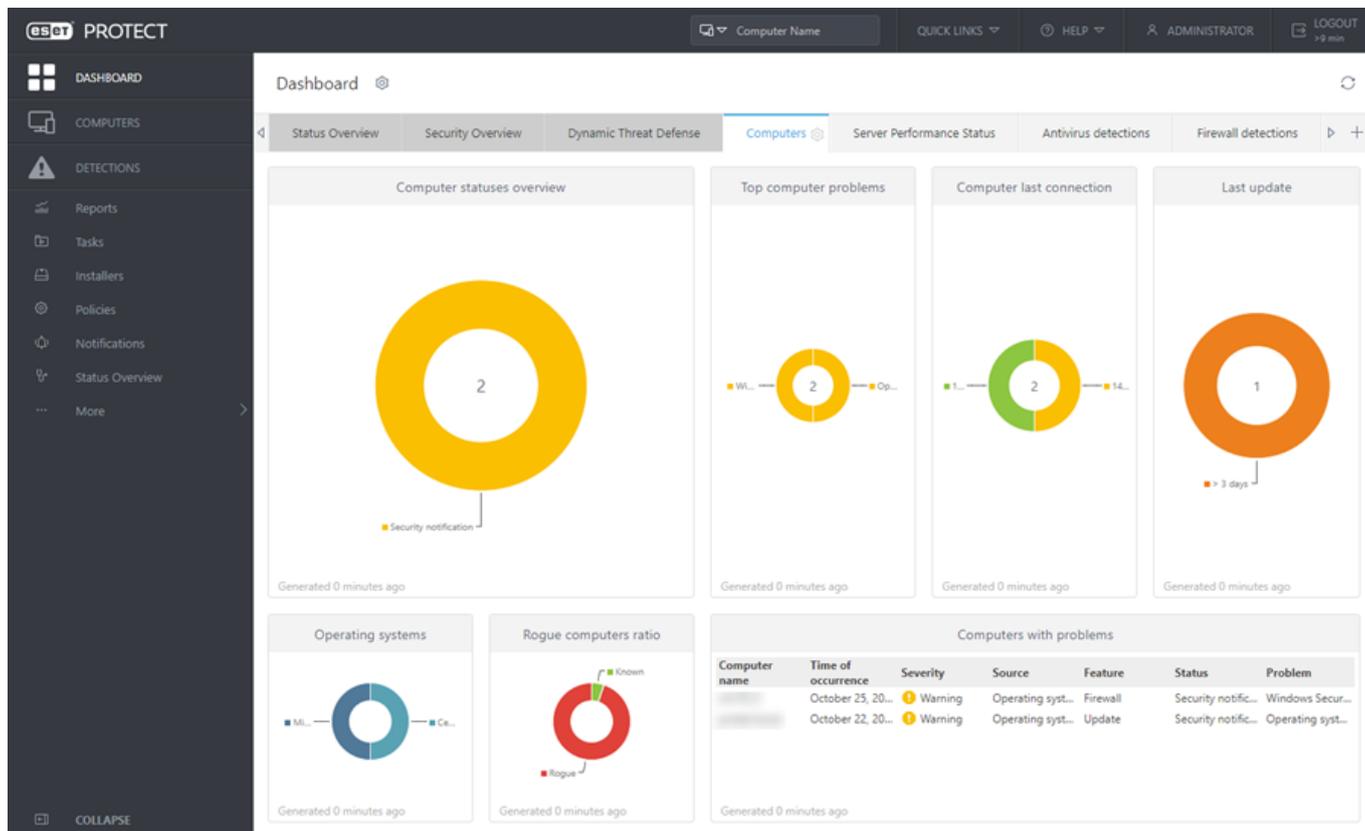
Enterprise Inspector Agent
 Show ESET Enterprise Inspector Agent settings

Step 7/7 Close startup wizard

i Puede volver a ver el asistente de inicio haciendo clic en **Ayuda > Asistente de inicio**.

Consola

El panel es la pantalla predeterminada que se muestra cuando el usuario inicia sesión en ESET PROTECT Web Console. Muestra informes predefinidos sobre su red. Puede cambiar entre los paneles utilizando las fichas de la barra de menú superior. Cada tablero se compone de varios informes.



Puede personalizar los paneles (excepto **Resumen del estado**, **Resumen de incidentes** y **Dynamic Threat Defense**) al agregar [informes](#), modificar otros, redimensionarlos, moverlos y reorganizarlos. Esta flexibilidad le permite crear una completa visión general de ESET PROTECT y sus objetos ([ordenadores](#), [grupos](#), [tareas](#), [políticas](#), [usuarios](#), etc.).

En ESET PROTECT vienen preconfiguradas las siguientes consolas:

- **Resumen del estado:** ventana de panel básica con información clave sobre su red de ESET PROTECT. Este panel no se puede modificar.
- **Resumen de incidentes:** este panel ofrece información general sobre las detecciones sin resolver notificadas en los últimos 7 días, e incluye datos como su gravedad, el método de detección, el estado de resolución y los 10 ordenadores o usuarios con más detecciones. Este panel no se puede modificar.
- **Dynamic Threat Defense:** si está utilizando [ESET Dynamic Threat Defense](#), aquí encontrará una visión general de informes útiles de ESET Dynamic Threat Defense.
- **Ordenadores:** esta consola ofrece una visión general de las máquinas cliente, su estado de protección, sistemas operativos, estado de actualización, etc.
- **Estado del rendimiento del servidor:** en esta consola puede ver información sobre el servidor ESET PROTECT, como la carga del servidor, los clientes con problemas, la carga de la CPU, las conexiones a bases de datos, etc.
- **Detecciones del antivirus:** aquí puede ver los informes del módulo antivirus de los productos de seguridad del cliente, como detecciones activas, detecciones en los últimos 7/30 días, etc.
- **Alertas del detecciones:** eventos del cortafuegos de los clientes conectados, en función de su gravedad, cuándo se notifican, etc.

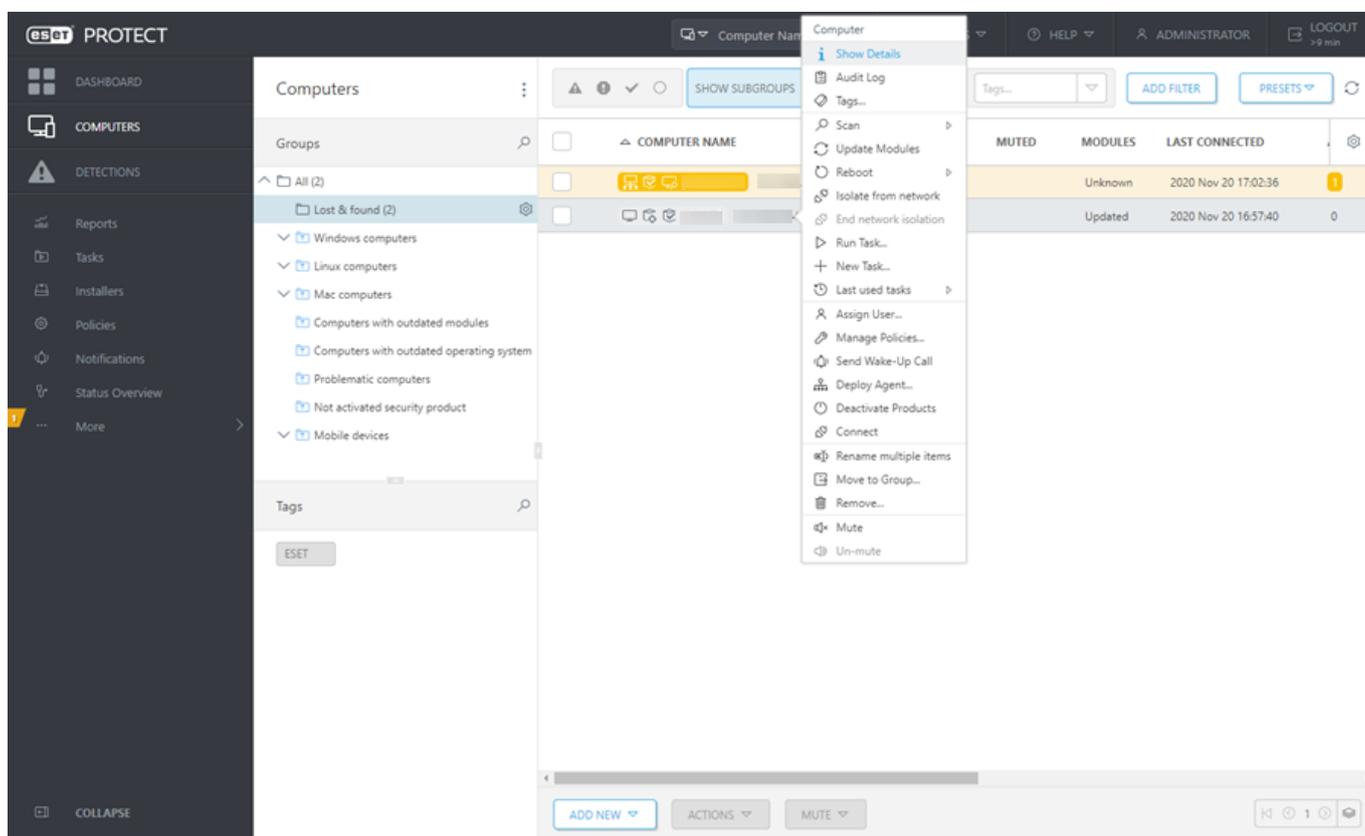
- **Aplicaciones de ESET:** en esta consola puede ver información sobre las aplicaciones de ESET instaladas.
- **Protección basada en la nube:** este panel le ofrece una visión general de los informes de protección basados en la nube (ESET LiveGrid® y, si tiene una licencia válida, también de ESET Dynamic Threat Defense).

Ordenadores

Todos los ordenadores cliente a los que puede acceder ESET PROTECT se muestran en  **Ordenadores** y se organizan en **grupos**. Al hacer clic en un grupo de la lista (panel izquierdo) se muestran los miembros (clientes) de este grupo en el panel derecho. Puede arrastrar y colocar clientes para moverlos entre los grupos.

Administrar ordenadores

Haga clic en un dispositivo para abrir un nuevo menú con acciones disponibles para ese dispositivo. También puede marcar la casilla de verificación junto a un dispositivo y hacer clic en **Acciones** de la barra inferior. El menú **Acciones** mostrará distintas opciones en función del tipo de dispositivo.



Filtrar ordenadores

 Si no encuentra un ordenador específico en la lista y sabe que está en su infraestructura de ESET PROTECT, asegúrese de desactivar todos los filtros.

Puede filtrar los clientes (ordenadores) con los filtros de la parte superior de la página:

- Marque la casilla **Mostrar subgrupos** para mostrar los subgrupos del grupo seleccionado.
- Al hacer clic en **Agregar filtro** se muestran los criterios de filtrado disponibles. También hay algunos filtros

predefinidos disponibles y se puede acceder a ellos rápidamente.

- Puede hacer clic en **Agregar filtro > Categoría del producto** y seleccionar una de las categorías disponibles:

OTodos los dispositivos: se muestran todos los ordenadores cliente sin filtrar. Puede utilizar una combinación de todas las opciones de filtrado anteriores para reducir la vista.

OProtegido por ESET: se muestran los clientes que están protegidos por un producto de ESET.

O ESET PROTECT: se muestran componentes de ESET PROTECT específicos, como Agent, RD Sensor y Proxy.

OOtros: se muestran solo los ordenadores cliente que ejecuten el producto seleccionado (Shared Local Cache, Dispositivo de seguridad de virtual o Enterprise Inspector).

- Puede utilizar los iconos de estado para filtrar clientes por la gravedad de los problemas detectados ( rojo para errores,  amarillo para advertencias,  verde para avisos y  gris para ordenadores no administrados). El icono de estado representa el estado actual de un ordenador cliente concreto y la solución de ESET instalada en el mismo. Puede ocultar o mostrar los iconos de estado de diferente gravedad para evaluar los clientes de su red en función del estado. Por ejemplo, para ver solo los ordenadores con advertencias, active solo el icono amarillo (los demás iconos deben estar inactivos). Para ver tanto advertencias como errores, active los iconos de estado rojo y amarillo. Los ordenadores no administrados  (clientes de la red que no tienen ESET Management Agent ni un producto de seguridad de ESET instalados) suelen aparecer en el grupo estático **Perdidos y encontrados**.
- También puede hacer clic en el encabezado de una columna para clasificar los ordenadores por ese atributo.

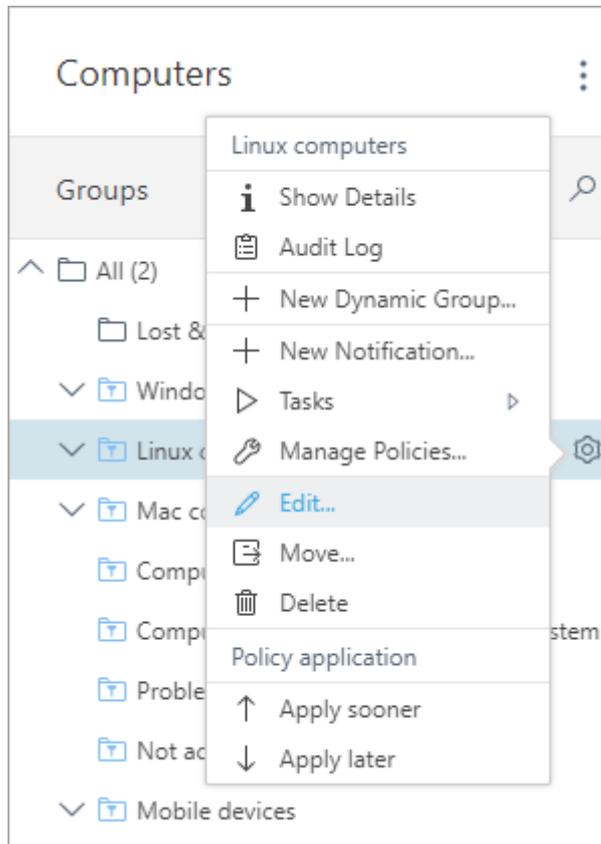
Última conexión muestra la fecha y la hora de la última conexión del dispositivo administrado. Un punto verde indica que el ordenador se conectó hace menos de 10 minutos. La información de **Última conexión** se resalta para indicar que el ordenador no está conectado:

oAmarillo (error): hace entre 2 y 14 días que el ordenador no se conecta.

oRojo (advertencia): el ordenador no se conecta desde hace más de 14 días.

Grupos

Puede administrar grupos desde  [Ordenadores](#). Los grupos le permiten organizar los equipos de la red, para poder asignarles [políticas](#) y [tareas](#) de forma sistemática. La configuración se aplica a todos los miembros del grupo. Los ordenadores que son miembros de un grupo aparecen en el panel de la derecha. Haga clic en el icono del engranaje  que aparece junto al nombre de un grupo para ver las acciones de grupo y los detalles de grupo disponibles.



Existen dos tipos de grupos: grupos estáticos y dinámicos.

Grupos estáticos

- Los grupos estáticos son grupos de ordenadores cliente seleccionados y otros objetos.
- Todos los dispositivos móviles e informáticos se encuentran en un grupo estático.
- Puede seleccionar manualmente qué equipos pertenecen a cualquier grupo estático.
- Cada objeto solo puede estar presente en un grupo estático.
- Los grupos estáticos juegan un papel importante en el [modelo de seguridad de ESET PROTECT](#).

Grupos dinámicos

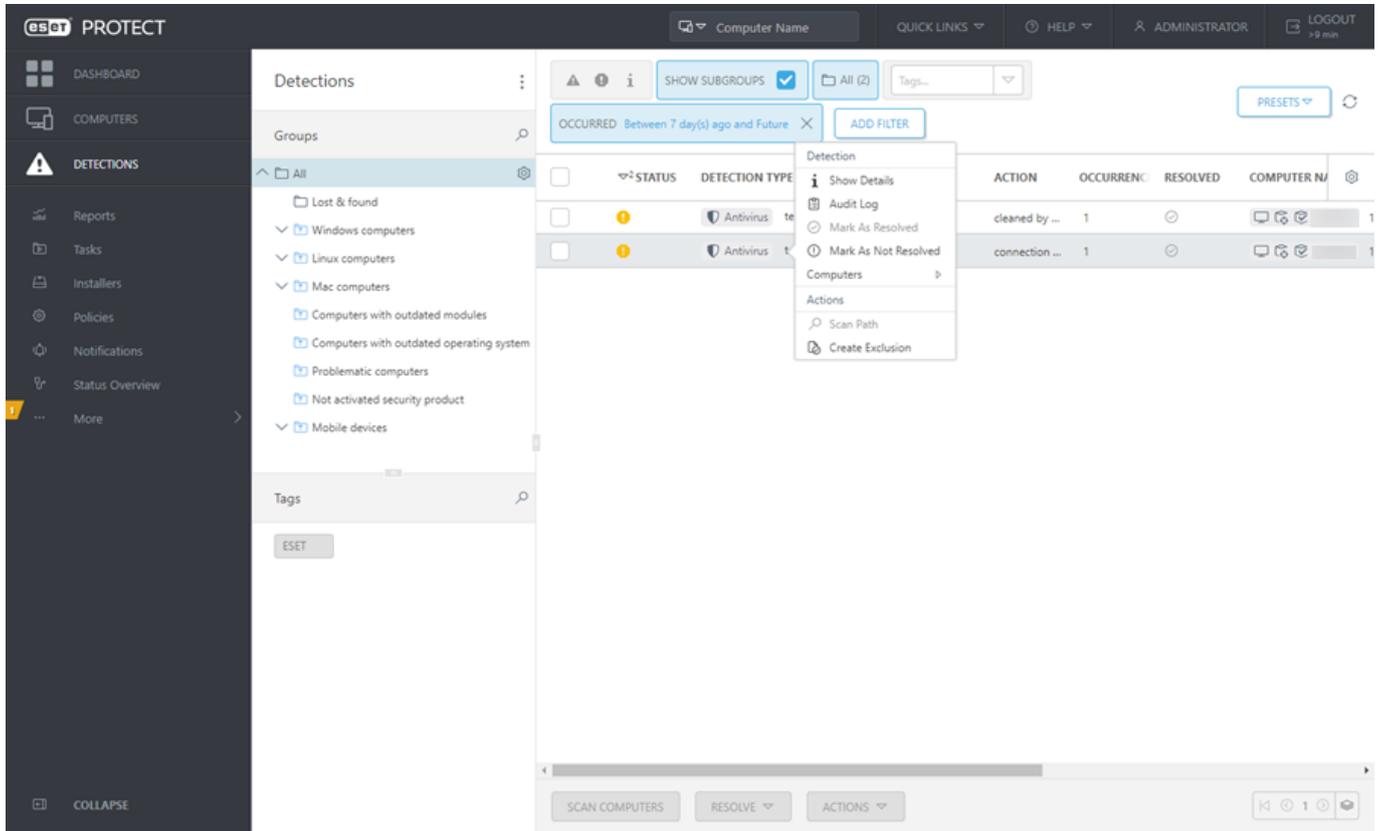
- Puede pensar en los grupos dinámicos como filtros personalizados en los que se pueden definir reglas para filtrar los ordenadores según corresponda.
- Los grupos dinámicos se basan en plantillas, e incluyen automáticamente aquellos equipos que cumplen los criterios establecidos en su plantilla.
- Si el dispositivo cliente no cumple los criterios, se elimina automáticamente del grupo dinámico.
- Un ordenador puede estar en varios grupos dinámicos al mismo tiempo o no estar en ninguno de ellos.

Tiene a su disposición artículos de la base de conocimiento que le ayudarán a [agregar ordenadores a los grupos estáticos](#), [crear plantillas para nuevos grupos dinámicos](#) y [asignar una política a un grupo](#).

Encontrará más información sobre los grupos en la sección [Grupos](#).

Detecciones

Para acceder a los informes sobre detecciones, haga clic en **Detecciones** en el menú principal de Web Console a la izquierda. En el panel **Detecciones** se muestra una descripción general de todas las detecciones encontradas en los ordenadores de su red.



Puede examinar los grupos y ver las detecciones en miembros de un grupo determinado. Puede filtrar la vista; de forma predeterminada, se ven todos los tipos de detección de los últimos siete días. Puede definir las detecciones como **Marcada como resuelta** en la sección **Detecciones** o en los detalles de un cliente específico.

Las detecciones se agregan por hora y otros criterios para simplificar su resolución. Las detecciones con una antigüedad superior a 24 horas se agregan automáticamente cada medianoche. Puede identificar las detecciones agregadas según el valor X/Y (elementos resueltos/elementos totales) de la columna **Resueltas**. Puede ver la lista de detecciones agregadas en la pestaña **Ocurrencias** en los detalles de la detección.

Encontrará las detecciones en cuarentena en **Más > Cuarentena**.

Exclusiones

Puede excluir los elementos seleccionados para que no se **detecten** en el futuro. Haga clic en una detección y seleccione **Crear exclusión**. Solo puede excluir las detecciones del **Antivirus** y **Cortafuegos - Reglas de IDS**. Puede crear una exclusión y aplicarla a más ordenadores y grupos.

⚠ Utilice las exclusiones con precaución. Pueden provocar que su ordenador se infecte.

La sección **Más > Exclusiones** contiene todas las exclusiones creadas, aumenta su visibilidad y simplifica su administración.

Detecciones en archivos comprimidos

Si se detectan una o más detecciones en un archivo comprimido, el archivo comprimido y la detección se guardan en **Detecciones**.

 La exclusión de un archivo comprimido que contiene una detección no excluye la detección. Tiene que excluir las detecciones individuales dentro del archivo comprimido. El tamaño máximo de archivo de los archivos contenidos en archivos comprimidos es de 3 GB.

Las detecciones excluidas ya no se detectarán, incluso si se realizan en otro archivo comprimido o sin archivar.

Protección contra ransomware

Los productos empresariales de ESET (versión 7 y posteriores) incluyen **Protección contra ransomware**. Esta nueva función de seguridad forma parte de HIPS y protege los ordenadores contra el ransomware. Cuando se detecta ransomware en un ordenador cliente, puede ver los detalles de la detección en ESET PROTECT Web Console, en **Detecciones**. Para filtrar solo detecciones de ransomware, haga clic en **Agregar filtro > Análisis > Análisis antirransomware**. Para obtener más información acerca de Protección contra ransomware, consulte el [Glosario de ESET](#).

Puede configurar de forma remota **Protección contra ransomware** desde la Consola web de ESET PROTECT utilizando la configuración de **Política** para su producto empresarial de ESET:

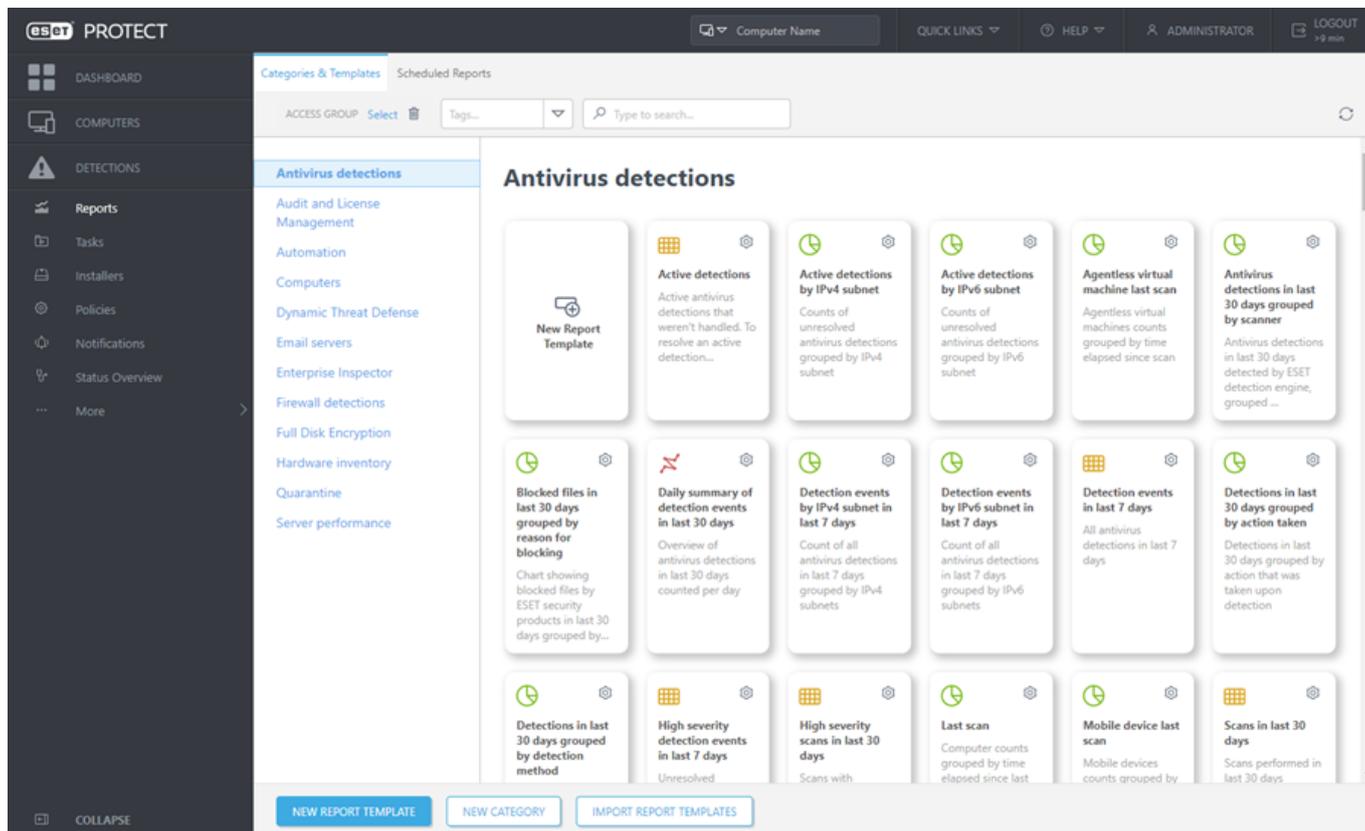
- **Activar protección contra ransomware:** el producto empresarial de ESET bloquea automáticamente todas las aplicaciones sospechosas que se comporten como ransomware.
- **Habilitar modo de auditoría:** cuando se habilita el modo de auditoría, las detecciones identificadas por Protección contra ransomware se informan en la ESET PROTECT Web Console, pero el producto de seguridad de ESET no las bloquea. El administrador puede decidir bloquear la detección comunicada o excluirla seleccionando [Crear exclusión](#). Esta configuración de Política solo está disponible a través de la Consola web de ESET PROTECT.

 De forma predeterminada, Protección contra ransomware bloquea todas las aplicaciones con comportamiento de ransomware potencial, incluidas las aplicaciones legítimas. Le recomendamos **Activar modo de auditoría** durante un breve periodo en un nuevo ordenador administrado para que pueda excluir aplicaciones legítimas detectadas como ransomware por su comportamiento (falsos positivos). No le recomendamos que utilice el Modo de auditoría permanentemente, porque el ransomware de los ordenadores administrados no se bloquea de forma automática cuando está activado el Modo de auditoría.

Informes

Los informes le permiten acceder y filtrar los datos de la base de datos de una manera sencilla. Los informes tienen categorías, y cada categoría incluye una descripción breve.

Para acceder a los informes, haga clic en la opción **Informes** en el menú Web Console de la izquierda, seleccione la plantilla de informe (una ventana dinámica con descripción, acción) de la que desee ver el informe y haga clic en  (icono del engranaje) > **Generar ahora**.



i De forma predeterminada, el administrador es el único que puede acceder a todas las plantillas de informes. El [resto de usuarios](#) no podrá ver ni utilizar estas plantillas a menos que se les haya asignado el permiso correspondiente (o si las plantillas se encuentran en otra ubicación).

Para recibir informes por correo electrónico, debe configurar correctamente una conexión al [servidor SMTP](#).

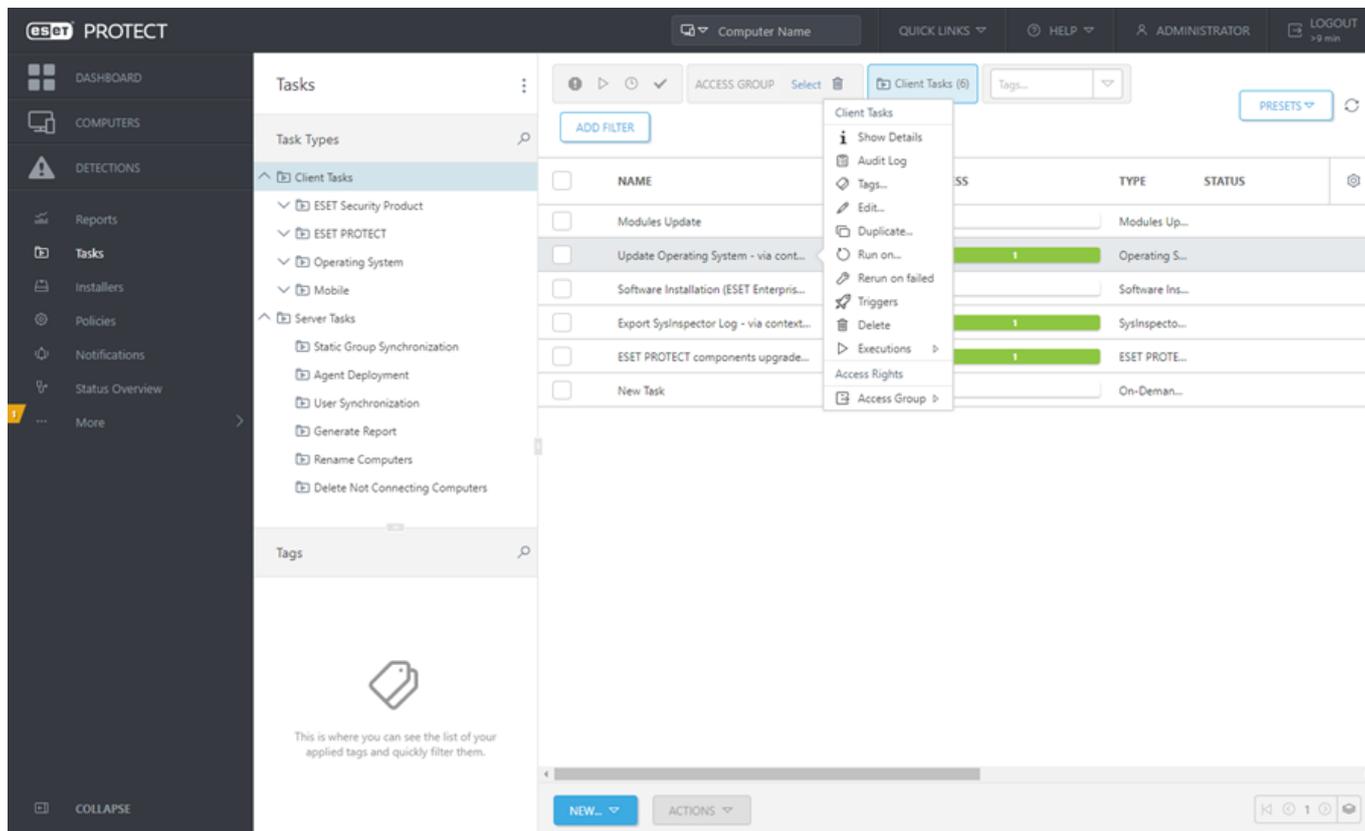
Consulte el [artículo de la base de conocimiento](#) de ESET para obtener instrucciones detalladas sobre cómo configurar los informes automáticos en ESET PROTECT.

Tareas

Las tareas se pueden utilizar para administrar ESET PROTECT Server, los ordenadores cliente y productos de ESET. Las tareas pueden automatizar trabajos rutinarios. Los destinos de la tarea pueden ser [ordenadores](#) y [grupos](#) concretos.

Las tareas le permiten asignar procedimientos concretos a clientes determinados o a grupos de clientes.

Además de en la ventana **Tareas**, puede crear tareas desde menús contextuales de la sección [Ordenadores](#). Para ver el estado de las tareas ejecutadas, haga clic en **Tareas** y observe si las tareas se han completado correctamente.



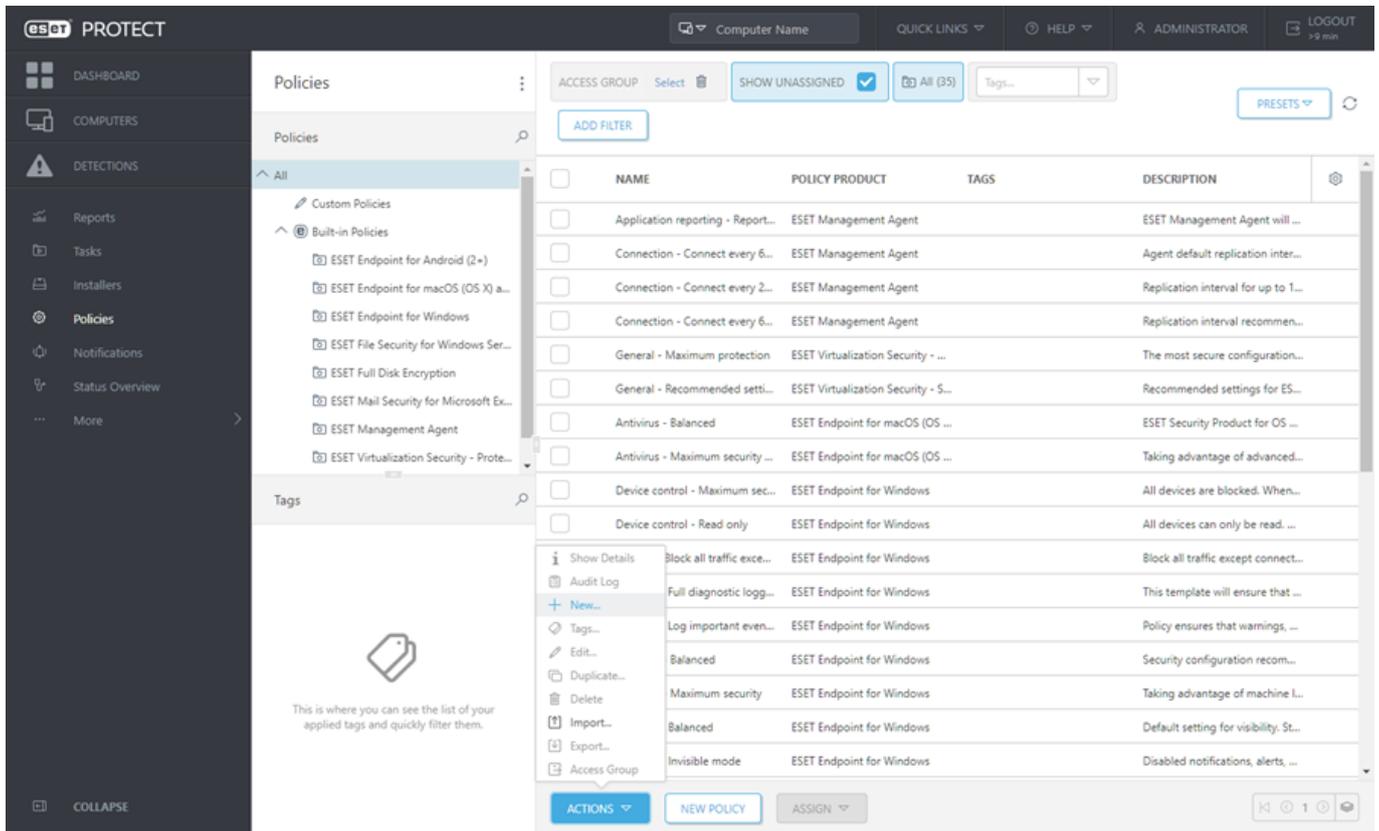
La sección [Tareas](#) de la Guía del administrador de ESET PROTECT contiene información sobre cómo crear, asignar y programar nuevas tareas.

La base de conocimiento de ESET cuenta con ejemplos de procedimientos para configurar tareas específicas, como las siguientes:

- [Envíe una llamada de activación a los ordenadores cliente para ejecutar una tarea inmediatamente en ESET PROTECT.](#)
- [Cambie el intervalo de conexión del agente para los ordenadores cliente en ESET PROTECT.](#)
- [Utilice la tarea del cliente Instalación del software para implementar o actualizar productos ESET Endpoint.](#)
- [Sincronizar ESET PROTECT con Active Directory.](#)

Políticas

Puede utilizar políticas para administrar ordenadores cliente. Las políticas son conjuntos de reglas de configuración que puede aplicar a los productos de ESET que se ejecutan en ordenadores cliente para evitar la configuración manual del producto de ESET de cada cliente. Puede aplicar una política directamente a [ordenadores](#) y [grupos](#) concretos. Asimismo, puede asignar varias políticas a un ordenador o un grupo.



Siga los pasos del [artículo de la base de conocimiento](#) de ESET para crear una política nueva y asignarla a un grupo.

Las políticas se aplican en el orden de disposición de los grupos estáticos. Esta regla no es válida para grupos dinámicos, ya que primero se recorren los grupos dinámicos secundarios para poder aplicar políticas con más consecuencias en la parte superior del árbol de grupos y aplicar políticas más específicas para los subgrupos.

i ESET le recomienda que asigne políticas más genéricas (por ejemplo, el servidor de actualización) a grupos que están más arriba en el árbol de grupos. Debe asignar políticas más específicas (por ejemplo, de configuración del control de dispositivos) más abajo del árbol de grupos.

Consulte la [sección Políticas](#) de la Guía del administrador de ESET PROTECT para obtener más información sobre la administración y la aplicación de políticas y sobre las reglas de eliminación de políticas.

Notificaciones

Puede configurar notificaciones automáticas basadas en eventos concretos como detecciones, instancias de Endpoint no actualizadas, etc. Consulte la sección [Notificaciones](#) de la Guía del administrador de ESET PROTECT o el [artículo de nuestra base de conocimiento](#) para obtener más información sobre la configuración y la administración de las notificaciones.

NAME	TAGS	ENABLED	STATUS	NOTIFICATION DESCRIPTION	LAST M
Malware outbreak alert (count per time criteria)		Disabled		Notification is sent when count of antivirus detection events in d...	Administrator
Network attack alert		Enabled	✓	Notification is sent when count of firewall events in defined perio...	Administrator
Computers report problems alert		Disabled		Notification is sent when at least 5% of managed computers hav...	Administrator
Outdated modules alert		Enabled	✓	Notification is sent when at least 5% of managed computers hav...	Administrator
Managed clients not connecting alert		Disabled		Notification is sent when at least 5% of all managed clients have ...	Administrator
Outdated ESET software alert		Disabled		Notification is sent when outdated ESET software is detected on ...	Administrator
Malicious file detected (trojan / worm / virus / application)		Disabled		Notification is sent when a malicious file is detected (trojan / wor...	Administrator
Notification has invalid configuration and will not be triggered		Disabled		At least one of the enabled notifications became invalid and will ...	Administrator
Outdated version of ESET Endpoint Antivirus detected		Enabled	✓	Notification is sent every day when at least one outdated instanc...	Administrator
At least one computer has not connected for more than 14 ...		Disabled		Notification is sent, when at least one computer has not been co...	Administrator
Potentially unsafe application detected		Disabled		Notification is sent when a potentially unsafe application is detec...	Administrator
At least one infected file that was not cleaned automatically ...		Disabled		Executed computer scan has detected at least one infected file th...	Administrator
Detection occurred in memory		Disabled		Notification is sent, when a detection event is detected by advan...	Administrator
Potentially unwanted application (PUA) detected		Disabled		Notification is sent when PUA (potentially unwanted application) ...	Administrator
High severity alert detected by HIPS occurred		Disabled		Notification is sent when a high severity detection triggered by H...	Administrator
Suspicious application detected		Enabled	✓	Notification is sent when a suspicious application is detected in y...	Administrator
Client task has invalid configuration and therefore will fail		Disabled		At least one of the created client tasks has invalid configuration a...	Administrator
New computer connected for the first time		Disabled		This notification is triggered when and ESET Management Agent ...	Administrator

Para recibir notificaciones por correo electrónico, debe configurar correctamente una conexión al servidor SMTP.

ESET PROTECT puede enviar automáticamente notificaciones e informes por correo electrónico. Active **Utilizar servidor SMTP**, haga clic en **Más > Configuración del servidor > Configuración avanzada > Servidor SMTP** y especifique lo siguiente:

- **Host:** nombre de host o dirección IP de su servidor SMTP.
- **Puerto:** SMTP utiliza el puerto 25 de forma predeterminada, pero puede cambiarlo si su servidor SMTP utiliza un puerto diferente.
- **Nombre de usuario:** si su servidor SMTP requiere autenticación, especifique el nombre de la cuenta de usuario SMTP (no incluya el dominio, pues no funcionará).
- **Contraseña:** la contraseña asociada con la cuenta de usuario SMTP.
- **Tipo de seguridad de la conexión:** especifique un tipo de conexión; el predeterminado es **No protegido**, pero si su servidor SMTP permite conexiones protegidas, elija TLS o STARTTLS. Si desea que su conexión sea más segura, utilice una extensión STARTTLS o SSL/TLS, ya que estas utilizan un puerto diferente para la comunicación cifrada.
- **Tipo de autenticación:** el valor predeterminado es **Sin autenticación**. No obstante, puede seleccionar el tipo de autenticación apropiado en la lista desplegable (por ejemplo, inicio de sesión, CRAM-MD5, CRAM-SHA1, SCRAM-SHA1, NTLM o automática).
- **Dirección del remitente:** especifique la dirección del remitente que se mostrará en el encabezado de los mensajes de correo electrónico de notificación (De:)
- **Probar servidor SMTP:** sirve para garantizar que la configuración SMTP sea correcta. Haga clic en **Enviar correo electrónico de prueba** para abrir una ventana emergente. Introduzca la dirección de correo electrónico

del destinatario y el mensaje de correo electrónico de prueba se enviará a esta dirección a través del servidor SMTP. Compruebe la bandeja de entrada del destinatario para verificar la entrega del mensaje de correo electrónico de prueba.

Puede usar Gmail como servidor SMTP si tiene una cuenta de Gmail. Utilice los siguientes ajustes:

Ajuste	Valor
Usar servidor SMTP	<i>Verdadero</i>
Host	<i>smtp.gmail.com</i>
Puerto	465 (TLS) o 587 (STARTTLS)
Nombre de usuario	<i>su dirección de Gmail</i>
Contraseña	<i>su contraseña de Gmail</i>
Tipo de seguridad de la conexión	TLS o STARTTLS
Tipo de autenticación	Automatic
Dirección del remitente	<i>su dirección de Gmail</i>

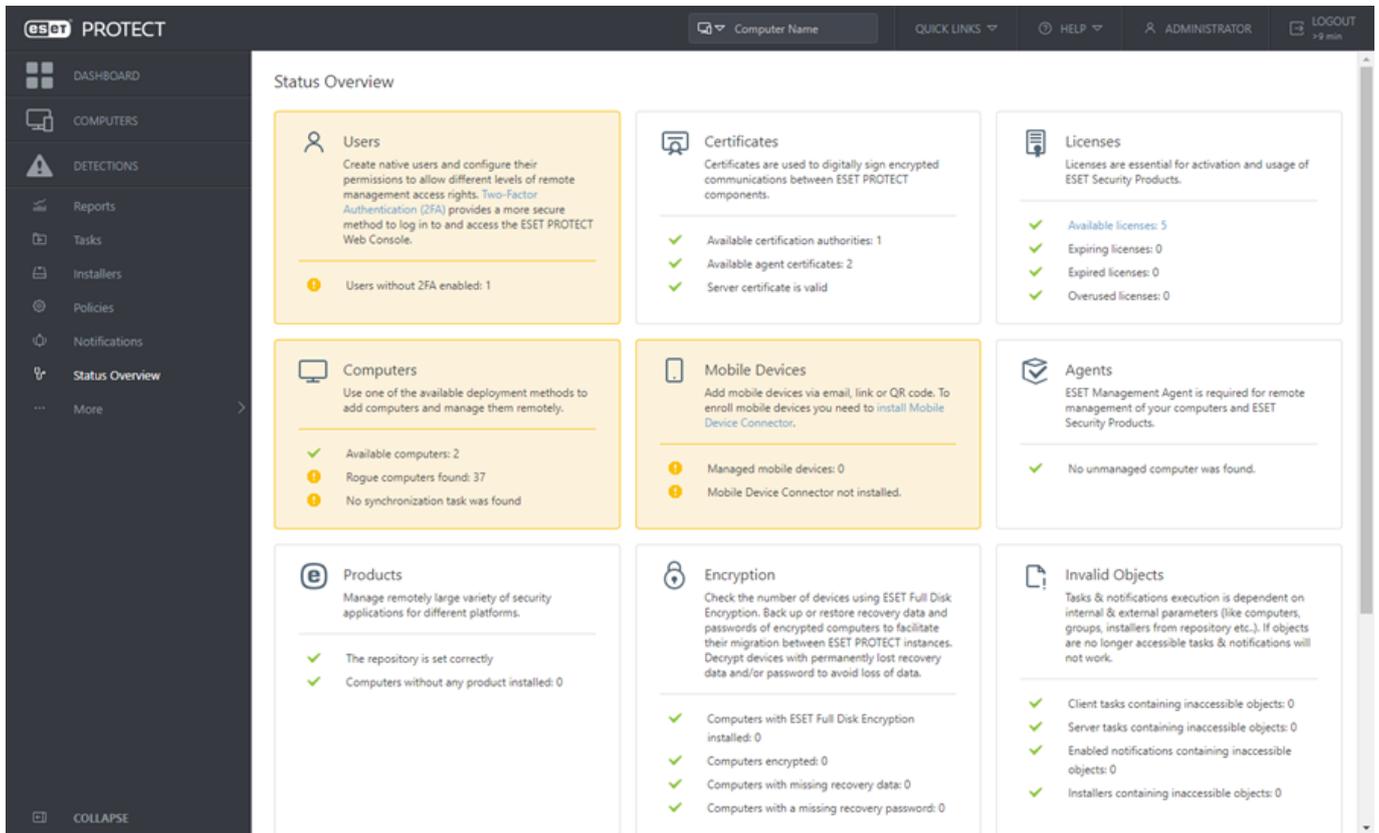
Si el envío de correos electrónicos falla, es posible que deba [Permitir aplicaciones menos seguras](#) en su cuenta de Gmail o [desbloquear](#) su cuenta de Gmail.

Resumen del estado

ESET PROTECT Server realiza comprobaciones de diagnóstico periódicas.

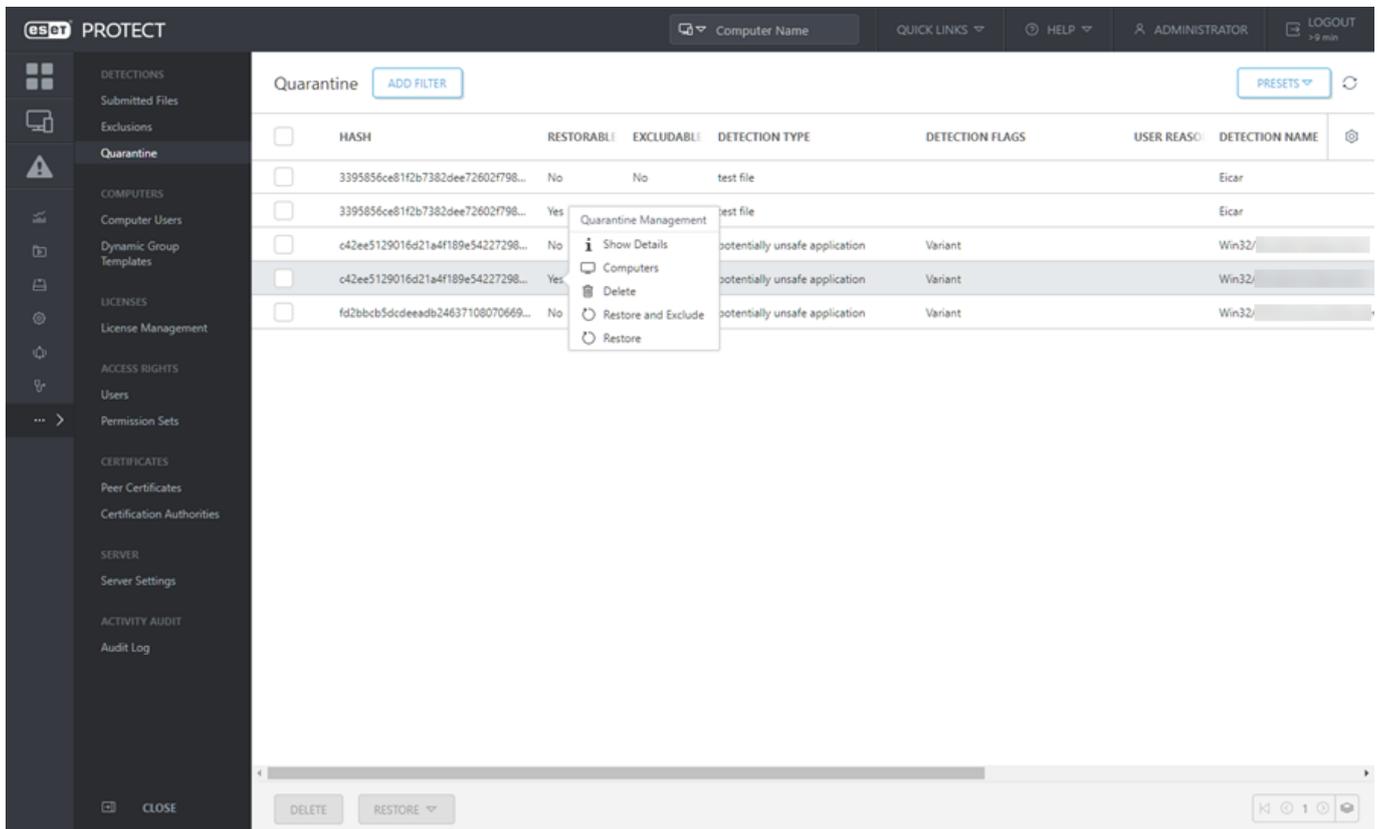
1. Haga clic en **Resumen del estado** para ver información de estado detallada sobre ESET PROTECT. Utilice el  **Resumen del estado** para ver estadísticas de uso y el estado general de su ESET PROTECT. También puede resultar útil en la configuración inicial de ESET PROTECT.

2. Haga clic en la ventana dinámica de una sección para mostrar una barra de tareas a la derecha con acciones.



Cuarentena

La sección Cuarentena se encuentra en Web Console, en **Más > Cuarentena**. En esta sección se muestran todos los archivos que están en cuarentena en dispositivos cliente.



Los archivos deben ponerse en cuarentena si no es posible desinfectarlos, si no es seguro ni aconsejable eliminarlos o si un producto de ESET los detecta incorrectamente como infectados.

No todas las detecciones encontradas en los dispositivos cliente se mueven a la cuarentena. Entre las detecciones que no se mueven a la cuarentena se incluyen las siguientes:

- Detecciones que no se pueden eliminar
- Detecciones sospechosas por su comportamiento, pero no identificadas como malware, por ejemplo, las [PUA](#).

Consulte también el [artículo de la base de conocimiento](#) de ESET sobre la administración de la cuarentena.

Administración de licencias

Seleccione **Más > Administración de licencias** para administrar sus licencias.

The screenshot shows the ESET PROTECT web console interface. The top navigation bar includes 'Computer Name', 'QUICK LINKS', 'HELP', 'ADMINISTRATOR', and 'LOGOUT'. The left sidebar contains a menu with 'DASHBOARD', 'COMPUTERS', 'DETECTIONS', 'Reports', 'Tasks', 'Installers', 'Policies', 'Notifications', 'Status Overview', and 'More'. The main content area is titled 'License Management' and features a 'Tags' section with a search icon. Below this is a table with columns: 'OWNER NAME', 'LICENSE USER', 'CONTACT', and 'PRODUCT'. The table contains three rows of data, with the first row highlighted in yellow. A context menu is open over the table, listing actions: 'Tags...', 'Add Licenses', 'Remove Licenses', 'Access Group' (with a sub-menu 'Move'), 'Synchronize Licenses', 'Open EBA', and 'Open EMA'. At the bottom, there is a blue 'ACTIONS' button and a green notification: 'Synchronization successful (2020 Nov 30 14:00:41)'.

Para agregar una licencia nueva ESET PROTECT:

1. Haga clic en **Más > Administración de licencias** y haga clic en **Acciones > Agregar licencias**.

2. Seleccione el método que desea utilizar para agregar las nuevas licencias:

a. **ESET Business Account o ESET MSP Administrator:** sincronice las licencias desde su cuenta de [ESET Business Account](#) o [ESET MSP Administrator](#) con ESET PROTECT Web Console. Ahora puede importar la estructura completa de su ESET Business Account, incluida la distribución de puestos de licencia entre los [sitios](#).

b. **Clave de licencia:** escriba o copie y pegue la clave de licencia que recibió cuando compró su solución

de seguridad de ESET en el campo **Clave de licencia**.

c. **Archivo de licencia sin conexión**.

3. Haga clic en **Agregar licencias**.

Add License ✕

You can add your license using one of the following options:

ESET Business Account or ESET MSP Administrator

License Key

Offline License File

License Key

⚠

[I have a Username and Password, what do I do?](#)

i ESET PROTECT permite administrar licencias de suscripción. Puede agregar una licencia mediante ESET Business Account, ESET MSP Administrator o una clave de licencia. Puede comprobar la validez de su suscripción en **Administración de licencias** en la columna **Validez** o haciendo clic en  **Ordenadores >** [Mostrar detalles](#).

Conjuntos de permisos y usuarios

ESET PROTECT modelo de seguridad

Estos son los principales términos utilizados en el modelo de seguridad:

Término	Explicación
Grupo doméstico	El grupo de inicio es donde se almacenan automáticamente todos los objetos (dispositivos, tareas, plantillas, entre otros) que crea un usuario. Cada usuario solo debe tener un grupo principal.
Objeto	Cada objeto (ordenador, tarea, política, informe o notificación) se localiza en un grupo estático . El acceso a los objetos es a través de grupos, no usuarios (proporcionar acceso por grupo facilita la participación de varios usuarios, por ejemplo, cuando un usuario está de vacaciones).
Grupo de acceso	Un grupo de acceso es un grupo estático que permite a los usuarios filtrar la ubicación del objeto en función de sus derechos de acceso.
Administrador	Un administrador es un usuario con el grupo de inicio Todo y un conjunto de permisos completo sobre el grupo.
Derecho de acceso	El derecho para acceder a un objeto o ejecutar una tarea se asigna mediante un conjunto de permisos.
Conjunto de permisos	Un conjunto de permisos representa los permisos de los usuarios que acceden a ESET PROTECT Web Console. Un conjunto de permisos define lo que un usuario puede ver o hacer en ESET PROTECT Web Console. A un usuario pueden asignarse varios conjuntos de permisos. Los conjuntos de permisos solo se aplican a objetos de grupos estáticos definidos.
Funcionalidad	Una funcionalidad es un tipo de objeto o acción. Normalmente, las funcionalidades reciben estos valores: Lectura, Escritura o Uso . La combinación de funcionalidades aplicadas a un grupo de acceso recibe el nombre de conjunto de permisos.

Si desea información más detallada, consulte la sección [Derechos de acceso](#) en la Guía de administración de ESET PROTECT.

Creación de un nuevo usuario de ESET PROTECT Web Console

Cuando [se configura ESET PROTECT por primera vez](#), se incluye un **administrador** predeterminado (usuario con el grupo de inicio **Todo** y acceso a todo) como único usuario.



ESET no recomienda utilizar la cuenta de usuario de administrador predeterminado. Debe [crear otra cuenta de administrador](#). También puede crear cuentas de usuario adicionales con menos derechos de acceso según las competencias deseadas de la cuenta.

Certificados

Certificados

Los certificados son una parte esencial de ESET PROTECT. Sirven para establecer una comunicación segura entre los componentes de ESET PROTECT y el servidor de ESET PROTECT y establecer una conexión segura de ESET PROTECT Web Console. Puede administrar certificados de ESET PROTECT en **Más > Certificados de iguales**.



Puede utilizar certificados que se generan automáticamente durante la instalación de [ESET PROTECT](#).

Autoridades certificadoras

Una autoridad certificadora legitima los certificados distribuidos desde su red. En un entorno empresarial, se utiliza una clave pública para una asociación automática del software cliente con el servidor de ESET PROTECT y permitir la instalación remota de productos de ESET. Puede administrar las autoridades certificadoras de ESET PROTECT en **Más > Autoridades certificadoras**.



Todos los certificados de iguales deben ser válidos y estar firmados por la misma autoridad certificadora para garantizar que todos los componentes puedan comunicarse correctamente.

Para obtener más información sobre los certificados y la autoridad certificadora, lea el [artículo de la base de conocimiento](#) de ESET o la [ayuda en línea](#).

Ayuda y asistencia técnica

ESET trabaja constantemente para actualizar y mejorar los productos ESET PROTECT y ESET Endpoint.

oLa [Base de conocimiento de ESET](#) es un repositorio de artículos de asistencia técnica en el que pueden realizarse búsquedas, y está diseñado para ayudarle a resolver sus problemas y a responder sus preguntas.

oEl [Foro de usuarios de ESET](#) está controlado por personal de ESET, y permite que los usuarios de ESET compartan los problemas que tienen y encuentren soluciones a los mismos.

oEl [Canal de vídeo de la Base de conocimiento de ESET](#) contiene instrucciones en vídeo de procedimientos habituales de los productos de ESET.

oVisite las [Noticias de asistencia técnica de ESET](#) y los Consejos a clientes para estar al tanto de las últimas novedades de las funciones y actualizaciones de los productos de ESET.

oPuede [enviar una solicitud al servicio de atención al cliente de ESET](#) si no puede resolver un problema o no encuentra la respuesta a su duda.

También puede consultar la [Guía de instalación](#) de ESET PROTECT (con temas sobre actualización, migración y solución de problemas), la [Guía de administración](#) (administración de ESET PROTECT con ESET PROTECT Web Console) y la [Guía del dispositivo virtual](#) (ESET PROTECT en un hipervisor) para obtener información más detallada.

Acuerdo de licencia para el usuario final

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

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

Acuerdo de licencia para el usuario final

En virtud de los términos de este Acuerdo de licencia para el usuario final ("Acuerdo"), firmado por ESET, spol. s r. o., con domicilio social en Einsteinova 24, 85101 Bratislava, Slovak Republic, empresa inscrita en el Registro

Mercantil administrado por el tribunal de distrito de Bratislava I, sección Sro, número de entrada 3586/B, número de registro comercial 31333532 ("ESET" o "el Proveedor") y usted, una persona física o jurídica ("Usted" o el "Usuario final"), tiene derecho a utilizar el Software definido en el artículo 1 del presente Acuerdo. El Software definido en el artículo 1 del presente Acuerdo puede almacenarse en un soporte de datos, enviarse por correo electrónico, descargarse de Internet, descargarse de los servidores del Proveedor u obtenerse de otras fuentes en virtud de los términos y condiciones especificados a continuación.

ESTO NO ES UN CONTRATO DE VENTA, SINO UN ACUERDO SOBRE LOS DERECHOS DEL USUARIO FINAL. El proveedor sigue siendo el propietario de la copia del software y del soporte físico incluidos en el paquete de venta, así como de todas las copias que el usuario final pueda realizar en virtud de este acuerdo.

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

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

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

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

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

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

b) **Estipulación del número de licencias.** El derecho de uso del software está sujeto a un número de usuarios finales. La expresión "un usuario final" se utilizará cuando se haga referencia a lo siguiente: (i) la instalación del

software en un sistema informático o (ii) un usuario informático que acepta correo electrónico a través de un Agente de usuario de correo ("un AUC") cuando el alcance de una licencia esté vinculado al número de buzones de correo. Si el AUC acepta correo electrónico y, posteriormente, lo distribuye de forma automática a varios usuarios, el número de usuarios finales se determinará según el número real de usuarios para los que se distribuyó el correo electrónico. Si un servidor de correo realiza la función de una pasarela de correo, el número de usuarios finales será equivalente al número de usuarios de servidor de correo a los que dicha pasarela preste servicios. Si se envía un número indefinido de direcciones de correo electrónico a un usuario, que las acepta (por ejemplo, mediante alias), y el cliente no distribuye los mensajes automáticamente a más usuarios, se necesita una licencia para un ordenador. No utilice la misma licencia en varios ordenadores de forma simultánea. El Usuario final tiene derecho a introducir la Clave de licencia en el Software si tiene derecho a utilizar el Software de acuerdo con la limitación derivada del número de licencias otorgadas por el Proveedor. La Clave de licencia se considera confidencial: no debe compartir la Licencia con terceros ni permitir que terceros utilicen la Clave de licencia, a menos que lo permitan este Acuerdo o el Proveedor. Si su Clave de licencia se ve expuesta, notifíquesele inmediatamente al Proveedor.

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

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

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

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

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

4. **Funciones con requisitos de recopilación de datos y conexión a Internet.** El Software necesita conexión a Internet para funcionar correctamente, y debe conectarse periódicamente a los servidores del Proveedor o a servidores de terceros; además, se recopilarán datos de acuerdo con la Política de Privacidad. La conexión a Internet y la recopilación de datos aplicable son necesarias para el funcionamiento del Software y para actualizar dicho Software. El Proveedor podrá publicar actualizaciones del Software ("Actualizaciones"), aunque no está obligado a proporcionarlas. Esta función se activa en la sección de configuración estándar del software y las actualizaciones se instalan automáticamente, a menos que el usuario final haya desactivado la instalación automática de actualizaciones. Para proporcionar Actualizaciones, es necesario verificar la autenticidad de la licencia, lo que incluye información sobre el ordenador o la plataforma en los que está instalado el Software, de acuerdo con la Política de Privacidad.

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

A los efectos de este Acuerdo, es necesario recopilar, procesar y almacenar datos que permitan al Proveedor

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

13. LIMITACIÓN DE RESPONSABILIDAD. HASTA EL ALCANCE MÁXIMO PERMITIDO POR LA LEGISLACIÓN APLICABLE, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O SUS PROVEEDORES DE LICENCIAS SERÁN RESPONSABLES DE PÉRDIDAS DE BENEFICIOS, DE INGRESOS, DE VENTAS O DE DATOS NI DE COSTES DERIVADOS DE LA OBTENCIÓN DE PRODUCTOS O SERVICIOS DE SUSTITUCIÓN, DE DAÑOS A LA PROPIEDAD, DE DAÑOS PERSONALES, DE LA INTERRUPCIÓN DEL NEGOCIO, DE LA PÉRDIDA DE INFORMACIÓN COMERCIAL O DE DAÑOS ESPECIALES, DIRECTOS, INDIRECTOS, ACCIDENTALES, ECONÓMICOS, DE COBERTURA, CRIMINALES O SUCESIVOS,

CAUSADOS DE CUALQUIER MODO, YA SEA A CAUSA DE UN CONTRATO, UNA CONDUCTA INADECUADA INTENCIONADA, UNA NEGLIGENCIA U OTRO HECHO QUE ESTABLEZCA RESPONSABILIDAD, DERIVADOS DE LA INSTALACIÓN, EL USO O LA INCAPACIDAD DE USO DEL SOFTWARE, INCLUSO EN EL CASO DE QUE AL PROVEEDOR O A SUS PROVEEDORES DE LICENCIAS O FILIALES SE LES HAYA NOTIFICADO LA POSIBILIDAD DE DICHOS DAÑOS. DADO QUE DETERMINADOS PAÍSES Y JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE RESPONSABILIDAD, PERO PUEDEN PERMITIR LA LIMITACIÓN DE RESPONSABILIDAD, EN DICHOS CASOS, LA RESPONSABILIDAD DEL PROVEEDOR, SUS EMPLEADOS, LICENCIATARIOS O AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR LA LICENCIA.

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

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

16. **Transferencia de la licencia.** El software se puede transferir de un sistema informático a otro, a no ser que se indique lo contrario en los términos del acuerdo. Si no se infringen los términos del acuerdo, el usuario solo puede transferir la licencia y todos los derechos derivados de este acuerdo a otro usuario final de forma permanente con el consentimiento del proveedor, y con sujeción a las siguientes condiciones: (i) el usuario final original no conserva ninguna copia del software; (ii) la transferencia de derechos es directa, es decir, del usuario final original al nuevo usuario final; (iii) el nuevo usuario final asume todos los derechos y obligaciones correspondientes al usuario final original en virtud de los términos de este acuerdo; (iv) el usuario final original proporciona al nuevo usuario final la documentación necesaria para verificar la autenticidad del software, tal como se especifica en el artículo 17.

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

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

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

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

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

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

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

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

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

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

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

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

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

22. Disposiciones generales. El hecho de que alguna de las disposiciones de este acuerdo no sea válida o aplicable no afectará a la validez de las demás disposiciones del acuerdo, que seguirán siendo válidas y aplicables de conformidad con las condiciones aquí estipuladas. Este Acuerdo se ha formalizado en inglés. Si se realiza una

traducción del Acuerdo por motivos de comodidad o por cualquier otro motivo, o en caso de discrepancia entre las versiones de este Acuerdo en diferentes idiomas, prevalecerá la versión en inglés.

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

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

ANEXO AL ACUERDO

Envío de información al proveedor. Al envío de información al proveedor se le aplican las siguientes disposiciones adicionales:

El Software incluye funciones que recogen datos sobre el proceso de instalación, el Ordenador o la plataforma en la que está instalado el Software, información sobre las operaciones y la funcionalidad del Software e información sobre dispositivos administrados (en adelante, "Información") y posteriormente los envían al Proveedor. La Información puede contener datos (incluidos datos personales obtenidos aleatoria o accidentalmente) relativos a dispositivos administrados. Si se activa esta función del Software, el Proveedor podrá recopilar la Información como se especifica en la Política de Privacidad y de acuerdo con la normativa legal relevante.

El Software necesita que haya un componente instalado en el ordenador administrado, que permite transferir información entre el ordenador administrado y el software de administración remota. La información que se puede transferir contiene datos de administración como información sobre hardware y software del ordenador administrado e instrucciones de administración del software de administración remota. El resto del contenido de los datos transferidos desde el ordenador administrado lo determinará la configuración del software instalado en el ordenador administrado. El contenido de las instrucciones del software de administración lo determinará la configuración del software de administración remota.

EULAID: EULA-PRODUCT-PROTECT; 3537.0

Política de privacidad

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

- Procesamiento de datos personales
- Confidencialidad de los datos

- Derechos del titular de los datos

Procesamiento de datos personales

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

- La administración de los productos de seguridad de ESET requiere y almacena de manera local información como el ID y el nombre del puesto, el nombre del producto, información sobre la licencia, información de activación y caducidad, información de hardware y software relativa al ordenador administrado con el producto de seguridad de ESET instalado. Se recopilan registros relacionados con las actividades de los productos y de seguridad de ESET y los dispositivos administrados, y están disponibles para facilitar las funciones y los servicios de administración sin envío automatizado a ESET.
- Información relativa al proceso de instalación, incluida la plataforma en la que se instala nuestro producto e información sobre las operaciones y la funcionalidad de nuestros productos, como la huella digital de hardware, los ID de instalación, los volcados de bloqueo, los ID de licencia, la dirección IP, la dirección MAC, los ajustes de configuración del producto, lo que también podría incluir los dispositivos administrados.
- La información sobre licencias, como el ID de licencia, y datos personales como el nombre, los apellidos, la dirección y la dirección de correo electrónico son necesarios para la facturación, la verificación de la autenticidad de las licencias y la prestación de nuestros servicios.
- La información de contacto y los datos contenidos en sus solicitudes de soporte pueden ser necesarios para el servicio de soporte. Según el canal que elija para ponerse en contacto con nosotros, podemos recopilar datos como su dirección de correo electrónico, su número de teléfono, información sobre licencias, datos del producto y descripción de su caso de asistencia. Es posible que le pidamos que nos facilite otra información para prestar el servicio de asistencia técnica, como los archivos de registro generados.
- Los datos relativos al uso de nuestros servicios son totalmente anónimos al finalizar la sesión. Una vez concluida la sesión, no se guarda ningún tipo de información personal.

Confidencialidad de los datos

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

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

ESET implementa medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado

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

Derechos del titular de los datos.

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

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

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

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