

ESET PROTECT

Guía para pequeñas y medianas empresas

[Haga clic aquí para mostrar la versión de ayuda de este documento](#)

Copyright ©2023 de ESET, spol. s r.o.

ESET PROTECT ha sido 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 o 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 la aplicación sin previo aviso.

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

REV. 19/03/2023

1	Acerca de Ayuda	1
2	Introducción	2
	2.1 Productos de punto de conexión de ESET administrables	2
	2.2 Nuevas características en 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	7
	4.3 Red	8
	4.4 Software	9
5	Instalar el servidor ESET PROTECT	9
	5.1 Instalación todo-en-uno del servidor de ESET PROTECT	11
6	Pasos posteriores a la instalación	23
7	Instalar el agente ESET Management y los productos de punto de conexión de ESET	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	Consola web ESET PROTECT	35
	8.1 Asistente de inicio	37
	8.2 Tablero	38
	8.3 Equipos	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 Información general de estado	49
	8.11 Cuarentena	50
	8.12 Administración de licencias	51
	8.13 Usuarios y conjuntos de permisos	52
	8.14 Certificados	53
9	Ayuda y soporte	54
10	Acuerdo de licencia de usuario final	54
11	Política de privacidad	61

Acerca de Ayuda

Por coherencia y para evitar confusiones, la terminología usada en toda la guía está basada en los nombres de los parámetros de ESET PROTECT. Además, usamos un conjunto de símbolos para marcar los asuntos de interés o de especial importancia.

 Las notas pueden proporcionar información valiosa, como características específicas o un enlace a un tema relacionado.

 Esto requiere de su atención y no debe omitirse. Por lo general, proporciona información que no es esencial, pero es importante.

 La información crítica debe ser tratada con cautela. A lo largo de este manual se dan advertencias específicas para evitar un posible error perjudicial. Lea y comprenda el texto entre corchetes, ya que hace referencia a las configuraciones de sistemas altamente sensibles o situaciones riesgosas.

 Ejemplo de una situación que describe el caso de un usuario correspondiente al tema donde está incluido. Los ejemplos sirven para explicar temas más complejos.

Convenio	Significado
Negrita	Nombres de interfaces como botones de cuadros u opciones.
<i>Itálica</i>	Marcadores para la información proporcionada. Por ejemplo, nombre de archivo o ruta indican que debe escribir la ruta o nombre del archivo correspondiente.
Nuevo correo	Comandos o ejemplos de códigos.
Hipervínculo	Proporciona un acceso rápido y sencillo a temas con referencia cruzada o a ubicaciones de sitios web externos. Los hipervínculos están resaltados en azul y pueden aparecer subrayados.
%ArchivosDelPrograma%	El directorio del sistema de Windows que almacena los programas instalados de Windows u otros.

- [Ayuda en línea](#) es la fuente principal de contenido de ayuda. La última versión de Ayuda en línea se mostrará automáticamente cuando disponga de una conexión a internet. Las páginas de ayuda en línea de ESET PROTECT incluyen cuatro pestañas activas en la parte superior del encabezado: [Instalación/Actualización](#), [Administración](#), [Implementación de aparatos virtuales](#) y [guía SMB](#).
- Los temas en la guía están divididos en varios capítulos y subcapítulos. Puede encontrar información importante usando el campo Buscar en la parte superior.

 Cuando abre una Guía del usuario desde la barra de navegación en la parte superior de la página, la búsqueda solo mostrará los resultados de los contenidos de esa guía. Por ejemplo, si abre una Guía del administrador, los temas de la guía de Instalación/Actualización e Instalación de AV no estarán incluidos en los resultados de búsqueda.

- La [Base de conocimiento de ESET](#) incluye respuestas a las preguntas frecuentes, así como también a las soluciones recomendadas para varios temas. Actualizado regularmente por los especialistas técnicos de ESET, la Base de conocimiento es la herramienta más poderosa para solucionar distintos tipos de problemas.
- El [Foro de ESET](#) proporciona a los usuarios un medio sencillo para obtener ayuda y ayudar a los demás. Puede publicar cualquier problema o consulta relacionada con los productos de ESET.

Introducción

Esta guía está destinada para medianas y pequeñas empresas que administran hasta 250 productos Endpoint de ESET para Windows que usan ESET PROTECT 9.

Explica los conceptos básicos importantes para la implementación y uso de los productos de seguridad de ESET.

ESET PROTECT 9

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

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

ESET PROTECT no proporciona protección contra el código malicioso. La protección de su entorno depende de la presencia de una solución de seguridad de ESET en las estaciones de trabajo o servidores, como ESET Endpoint Security.

Productos de punto de conexión de ESET administrables

Los productos ESET Endpoint están diseñados principalmente para usar en estaciones de trabajo de un entorno de empresas pequeñas/empresarial y se pueden usar con ESET PROTECT.

ESET PROTECT 9 es capaz de implementar o administrar los siguientes productos de terminales de ESET:

Administrable a través de ESET PROTECT 9	Versión del producto
ESET Endpoint Security para Windows	6.5 o superior, 7.x, 8.x, 9.x
ESET Endpoint Antivirus para Windows	6.5 o superior, 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 administrables](#).

Nuevas características en ESET PROTECT 9.0

Un clic para acceder a los detalles

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

detección. [Obtener más información](#)

Nuevo dashboard de información general para EDTD

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

Actualizaciones automáticas del producto

Para facilitar su vida, presentamos actualizaciones automáticas de nuestros productos de seguridad (productos para puntos de conexión Windows por el momento) con activación inmediata en el próximo ESET Endpoint Security/Antivirus v9, que se presentará en noviembre. Con las actualizaciones automáticas puede mantener los productos de ESET siempre actualizados en su red. [Obtener más información](#)

Administración de la protección contra ataques por fuerza bruta

En los productos para puntos de conexión Windows v9, presentaremos una nueva característica de seguridad que protege los dispositivos frente a la posibilidad de que se adivinen las credenciales y se establezca una conexión remota. Podrá configurar fácilmente esta característica mediante una política directamente desde la consola y crear exclusiones desde la sección **Detecciones** cuando haya algo bloqueado que no debería estarlo.

Mejoras de ESET Full Disk Encryption

Ahora puede ahorrar tiempo de ejecución mediante la actualización de los módulos de ESET Full Disk Encryption de forma sencilla. 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 del usuario para mostrar los módulos ESET Full Disk Encryption instalados actualmente.

Otras mejoras y cambios de facilidad de 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:

- Servidor ESET PROTECT (controla la comunicación con los equipos cliente)
- ESET PROTECT Consola web de ERA (interfaz web de usuario para el Servidor ESET PROTECT)
- Agente ESET Management (implementado en los equipos clientes, se comunica con el Servidor ESET PROTECT)

Los siguientes componentes de soporte son opcionales, pero se recomienda que los instale para obtener un mejor rendimiento de la aplicación en la red:

- Apache HTTP Proxy
- RD Sensor (detecta equipos no administrados en la red)

Servidor

El servidor ESET PROTECT (Servidor) es la aplicación que procesa todos los datos recibidos de los clientes que se conectan al servidor (a través del Agente de ESET Management).

Agente

El ESET Management Agente es una parte esencial de ESET PROTECT. Los equipos cliente no se comunican directamente con el servidor, más bien el agente facilita esta comunicación. El Agente recopila la información del cliente y la envía al Servidor ESET PROTECT. Si el servidor de ESET PROTECT envía una tarea para el cliente, dicha tarea se envía al agente que, luego, la envía al producto de punto de conexión de ESET que se ejecuta en el cliente.

Consola web

La consola web de ESET PROTECT es una interfaz del usuario en el navegador que le permite administrar las soluciones de seguridad de ESET en su entorno. Muestra una visión general del estado de los clientes en su red y se puede usar para implementar las soluciones de ESET en equipos no administrados en forma remota. Si elige que el servidor web sea accesible desde Internet, puede usar ESET PROTECT desde prácticamente cualquier lugar y dispositivo.

Apache HTTP Proxy

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 equipos cliente. Actúa como un proxy transparente, lo que significa que hace un caché de archivos que ya se han descargado para minimizar el tráfico de Internet en la red.

Su uso brinda los siguientes beneficios:

- Descargas y cachés de lo siguiente:
 - Actualizaciones de motor de detección
 - Tareas de activación, que incluyen comunicación con servidores de activación y realizar caches de solicitudes de licencia
 - Datos de repositorio de ESET PROTECT
 - Actualizaciones de componentes del producto: el proxy de Apache almacena en caché y distribuye actualizaciones a clientes del extremo en su red.
- Tráfico de Internet minimizado en su red.

Sensor de Rogue Detection

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

i El Rogue Detection Sensor puede demorar hasta 24 horas en ubicar equipos nuevos en su red.

Las máquinas recientemente detectadas se enumeran en un [informe predefinido](#), lo que facilita la instalación del agente ESET Management en ellas, asignarlas a grupos estáticos específicos y administrarlas mediante [tareas](#) y [políticas](#).

Requisitos del sistema

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

Hardware

El equipo del servidor de ESET PROTECT debe cumplir con las siguientes recomendaciones de hardware indicadas en la tabla que se encuentra a continuación.

Cantidad de clientes	ESET PROTECTServidor + servidor de la base de datos SQL				
	Núcleos de CPU	Velocidad del reloj de la CPU (GHz)	RAM (GB)	Unidad de disco ¹	IOPS ² de disco
Hasta 1.000	4	2.1	4	Individual	500
5.000	8	2.1	8		1.000
10.000 ³	4	2.1	16	Separado	2.000
20.000	4	2.1	16		4.000
50.000	8	2.1	32		10.000
100.000	16	2.1	Más de 64		20.000

¹ Unidad de disco individual/separada: le recomendamos que instale la [base de datos](#) en una unidad separada para sistemas que tienen más de 10.000 clientes.

² IOPS (total de operaciones de entrada o salida por segundo) - valor mínimo requerido.

- Le recomendamos que tenga aproximadamente 0,2 IOPS por cliente conectado, pero no menos de 500.
- Puede verificar los IOPS de la unidad con la herramienta [diskspd](#); use el siguiente comando:

Cantidad 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 la [situación de ejemplo](#) para un entorno de 10 000 clientes.

Recomendaciones de unidad de disco

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

- La instancia del servidor SQL puede compartir recursos con el Servidor ESET PROTECT para maximizar el

uso y minimizar la latencia. Ejecute el servidor de ESET PROTECT y el servidor de la base de datos en un solo equipo para aumentar el rendimiento de ESET PROTECT.

- El rendimiento de un servidor SQL mejora si ubica la base de datos y los archivos de registro de transacción en unidades separadas, preferentemente en unidades SSD físicas separadas.
- Si tiene una sola unidad de disco, le recomendamos usar una unidad SSD.
- Le recomendamos que utilice la arquitectura todo flash. Los discos sólidos (SSD) son mucho más rápidos que los HDD estándar.
- Si tiene una configuración de RAM alta, es suficiente configurar el SAS con R5. La configuración probada: 10 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 una empresa de SSD nivel IOPS superior.
- La capacidad de 100 GB es suficiente para cualquier cantidad de clientes. Es probable que necesite una capacidad más elevada si realiza una copia de seguridad de la base de datos con frecuencia.
- No use una unidad de red porque el rendimiento de ESET PROTECT será más lento.
- Si tiene una infraestructura de almacenamiento de varios niveles que permite la migración del almacenamiento en línea, le recomendamos que empiece por compartir niveles más lentos y supervise el rendimiento de ESET PROTECT. Si nota que la latencia de lectura/escritura supera los 20 ms, puede realizar un traslado sin interrupciones de la capa de almacenamiento a un "mesón" más rápido para utilizar el backend más económico. Puede hacer lo mismo en un hipervisor (si utiliza ESET PROTECT como máquina virtual).

Recomendaciones de dimensionamiento para distintos recuentos de clientes

A continuación, encontrará los resultados de rendimiento para un entorno virtual con una cantidad determinada de clientes en ejecución por un año.

i La base de datos y ESET PROTECT se ejecutan en máquinas virtuales separadas con configuraciones idénticas de hardware.

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

Sistema operativo

La siguiente tabla muestra 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 instalados		✓	✓	
Windows Server 2008 R2 CORE x64 con KB4474419 y KB4490628 instalados		✓	✓	
Windows Storage Server 2008 R2 x64 con KB4474419 y KB4490628 instalados		✓	✓	
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 más recientes de Windows (al menos KB4474419 y KB4490628)		✓	✓	
Windows 7 x64 SP1 con las actualizaciones más recientes de Windows (al menos KB4474419 y KB4490628)		✓	✓	
Windows 8 x86		✓	✓	
Windows 8 x64	❓*	✓	✓	❓*
Windows 8.1 x86		✓	✓	

Sistema operativo	Servidor	Agente	RD Sensor	MDM
Windows 8.1 x64	?	✓	✓	?
Windows 10 x86		✓	✓	
Windows 10 x64 (todas las versiones oficiales)	?	✓	✓	?
Windows 10 en ARM		✓		
Windows 11 x64	?	✓	✓	?

* La instalación ESET PROTECT de componentes en el sistema operativo de un cliente podría no estar alineada con la política de licencias de Microsoft. Para obtener más información, verifique la política de licencias de Microsoft o consulte con su proveedor de software. En los entornos de SMB / redes pequeñas, recomendamos considerar la instalación ESET PROTECT de Linux o el [aparato virtual](#), donde corresponda.

En sistemas MS Windows más antiguos:

- Tenga siempre instalado el Service Pack más reciente, especialmente en sistemas más antiguos como Server 2008 y Windows 7.
 - ESET PROTECT no admite la administración de equipos que ejecutan Windows 7 (sin SP), Windows Vista y Windows XP.
 - A partir del 24 de marzo de 2020, ESET ya no será compatible de manera oficial ni brindará soporte técnico para ESET PROTECT (Aervidor y MDM) instalados en los siguientes sistemas operativos de Windows: Windows 7, Windows Server 2008 (todas las versiones).
- No es compatible con 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 pasar a una alternativa sin costo. Consulte las [versiones compatibles de JDK](#).



Puede ejecutar ESET PROTECT en un sistema operativo sin servidor, sin la necesidad de ESXi. Instalar [VMware Player](#) en un Sistema operativo de escritorio e implementar el [ESET PROTECT Aparato virtual](#).

Red

Es esencial que los equipos de clientes y el Servidor ESET PROTECT administrados por ESET PROTECT tengan una conexión a Internet activa para llegar a los servidores de activación y el repositorio ESET. Si prefiere no tener clientes conectados directamente a Internet, puede usar un servidor proxy (no el mismo que el Proxy Apache HTTP) para facilitar la comunicación con su red e Internet.

Los equipos administrados por ESET PROTECT deben estar conectados al mismo LAN o se deben encontrar en el mismo dominio de Active Directory que su servidor ESET PROTECT. El Servidor ESET PROTECT debe ser visible para los equipos cliente. Además, los equipos cliente deben comunicarse con su servidor ESET PROTECT para usar la instalación remota y la función [Llamada de activación](#).

Puertos usados

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

Software

Los siguientes prerequisites se deben cumplir para poder instalar el Servidor ESET PROTECT en Windows:

- Debe tener una [licencia](#) válida.
- Se debe instalar Microsoft .NET Framework 4; puede instalarlo con el **Asistente para agregar roles y características**.
- La consola web de ESET PROTECT 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 pasar a una alternativa sin costo. Consulte las [versiones compatibles de JDK](#).

- ESET PROTECT es compatible con dos tipos de servidores de la base de datos: MS SQL eMySQL. Recomendamos usar Microsoft SQL Server Express2019 incluido con el instalador todo en uno de ESET PROTECT para Windows. Si ya tiene un servidor de base de datos y desea usarlo para ESET PROTECT, asegúrese de que cumple con los [requisitos de la base de datos](#).
- La consola web ESET PROTECT se puede ejecutar en los siguientes navegadores web:

oMozilla Firefox

oMicrosoft Edge

oGoogle Chrome

oSafari

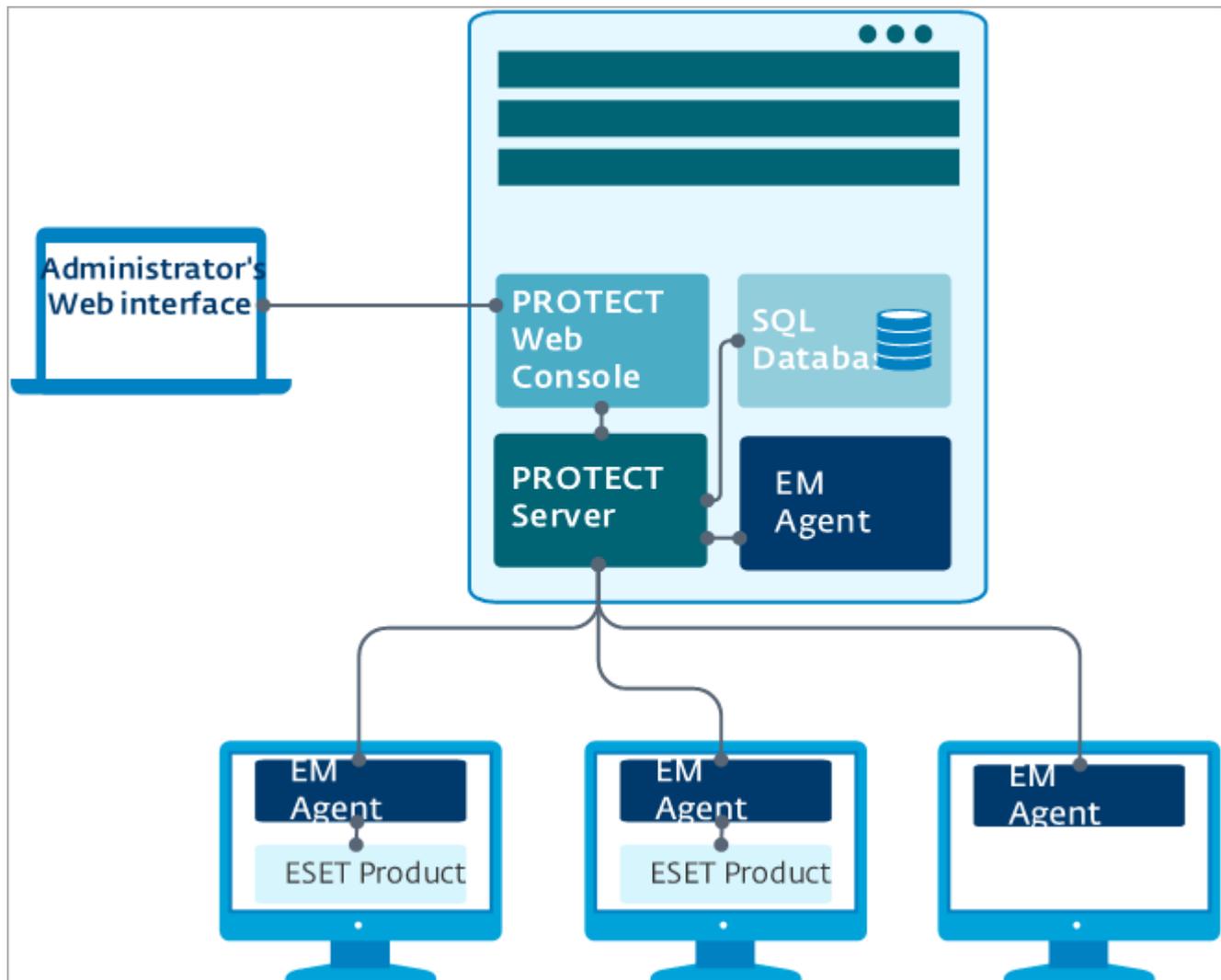
oOpera

 Para vivir la mejor experiencia con la consola web de ESET PROTECT, le recomendamos que tenga actualizados los navegadores web. Si usa Internet Explorer, la consola web de ESET PROTECT le informará que está usando un navegador web no compatible.

Instalar el servidor ESET PROTECT

Estructura de componentes de ESET PROTECT

Para administrar redes pequeñas a medianas (1000 clientes o menos), una única máquina con el servidor de ESET PROTECT y todos sus componentes (servidor web suministrado, base de datos, etc.) instalados allí generalmente es suficiente. Puede pensarlo como un servidor único o una instalación independiente. Todos los clientes administrados se conectan directamente al servidor de ESET PROTECT por medio del agente ESET Management. El administrador se puede conectar a la Consola web ESET PROTECT por medio del navegador web desde cualquier equipo en la red o ejecutar la consola web directamente desde el Servidor ESET PROTECT.



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 instalaciones en Windows.
- ESET recomienda instalar un [aparato virtual de ESET PROTECT](#) preconfigurado (en ejecución en CentOS Linux) si usa un hipervisor. Su instalación es rápida y más directa que la instalación en Windows.

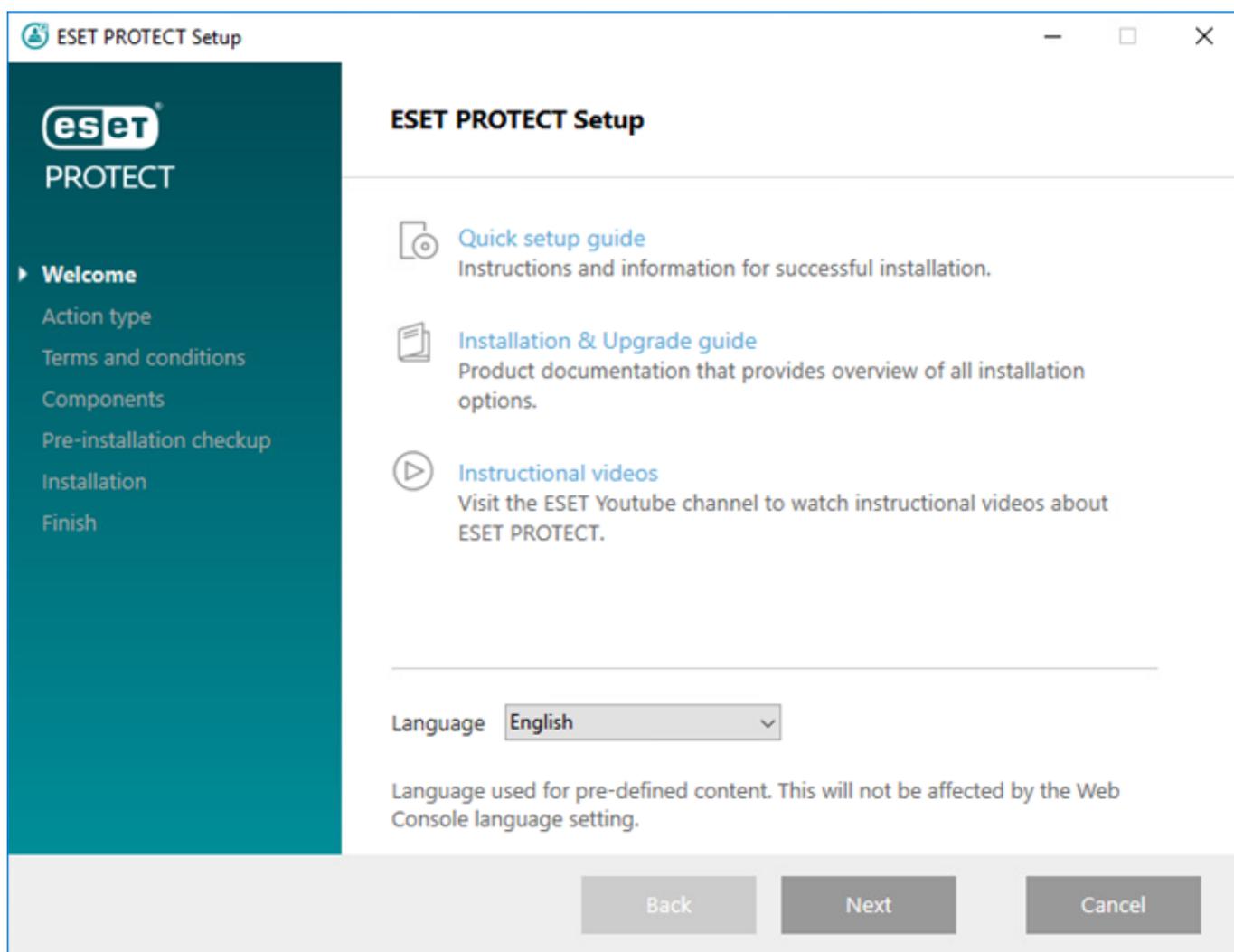
i Si actualiza desde una versión anterior de ESET PROTECT o ESMC 7.x, siga [estas instrucciones](#).

Instalación todo-en-uno del servidor de ESET PROTECT

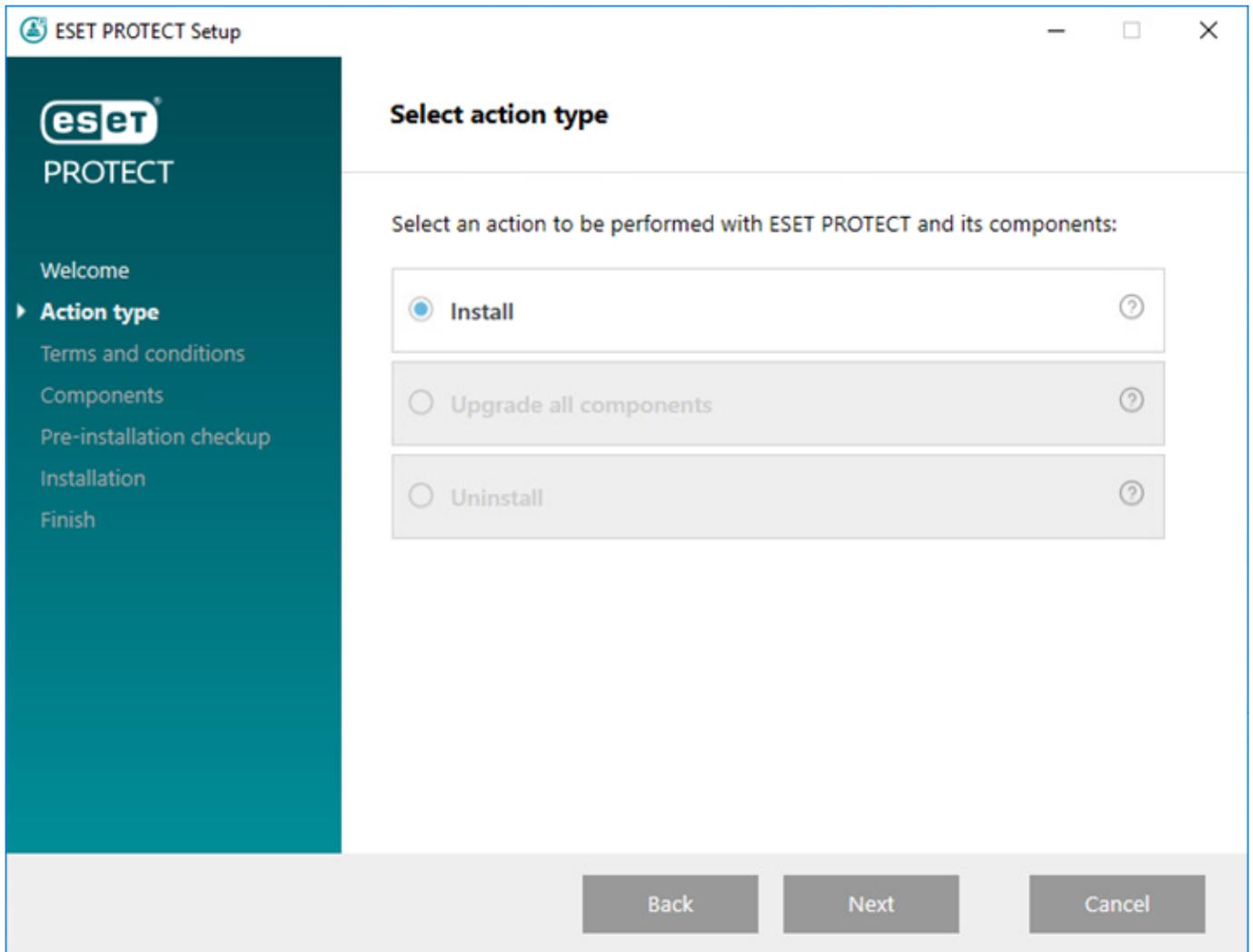
- Otra alternativa es instalar un [aparato virtual de ESET PROTECT](#) preconfigurado (si usa un hipervisor).
- Si actualiza desde una versión anterior de ESET PROTECT o ESMC 7.x, siga [estas instrucciones](#).

El [instalador todo en uno ESET PROTECT](#) está disponible únicamente para los sistemas operativos de Windows. El instalador todo en uno le permite instalar todos los componentes de ESET PROTECT al usar 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 del idioma. Haga clic en **Siguiente** para continuar.



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



3. Desmarque la casilla de verificación al lado de **Participar en el programa de mejora del producto** si no está de acuerdo en enviar informes de fallas y datos de telemetría anónimos a ESET (versión y tipo de sistema operativo, versión de producto ESET y otra información específica del producto). Si la casilla de verificación está seleccionada, se enviará informes de fallas y datos de telemetría a ESET. Luego de aceptar el EULA, haga clic en **Siguiente**.

4. Seleccione los componentes para Instalar y haga clic en **Siguiente**.

[Microsoft SQL Server Express](#)

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

OSi usa una edición anterior de Windows (servidor 2012 o SBS 2011), Microsoft SQL Server Express 2014 se instalará de manera 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 de cada base de datos relacionada. 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 instalada otra [versión compatible](#) de Microsoft SQL Server o MySQL o si planea conectarse a un SQL Server diferente, quite la marca de la casilla junto a **Microsoft SQL Server Express**.
- [No instale SQL Server en un controlador de dominio](#) (por ejemplo, Windows SBS/Essentials). Recomendamos que instale ESET PROTECT en un servidor diferente o que no seleccione el componente SQL Server Express durante la instalación (esto requiere que use un SQL Server o un MySQL existente para ejecutar la base de datos ESET PROTECT).

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

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

[Apache HTTP Proxy](#)

La opción **Proxy HTTP Apache** está destinada únicamente para redes más pequeñas o centralizadas, sin clientes de itinerancia. Si selecciona esta opción, el instalador configura los clientes para la comunicación a través de túnel con ESET mediante el proxy instalado en el mismo equipo que el servidor de ESET PROTECT. Esta conexión no funcionará si no hay visibilidad de red directa entre clientes y el Servidor ESET PROTECT.

- El uso del Proxy HTTP puede ahorrarle bastante ancho de banda en las descargas de Internet y mejorar las velocidades de descarga para las actualizaciones de productos. Se recomienda seleccionar la casilla de verificación junto al **Apache HTTP Proxy** si gestiona más de 37 equipos desde ESET PROTECT. También puede elegir instalar [Instalar el proxy Apache HTTP más adelante](#).
- Para obtener más información, consulte [¿Qué es Apache HTTP Proxy?](#) y [Diferencias entre Apache HTTP Proxy, herramienta de replicación y conectividad directa](#).
- Seleccione **Apache HTTP Proxy** para instalar el Proxy HTTP Apache, crear y aplicar políticas (llamadas **Uso del Proxy HTTP**, aplicadas al grupo **Todo**) para los siguientes productos:

oESET Endpoint para Windows

oESET Endpoint para macOS (OS X) y Linux

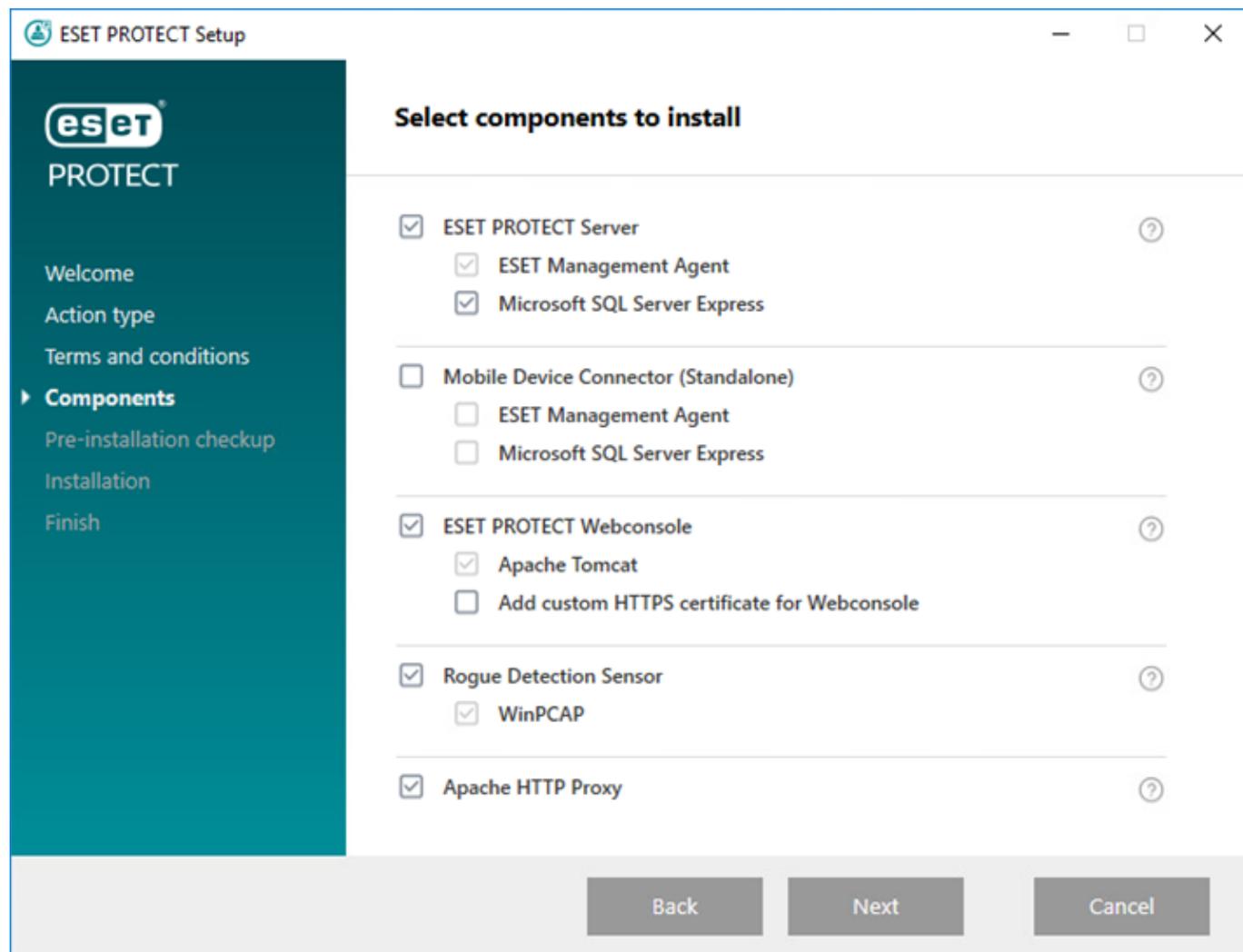
oESET Management Agent

oSeguridad de archivos de ESET para Windows Server (6+)

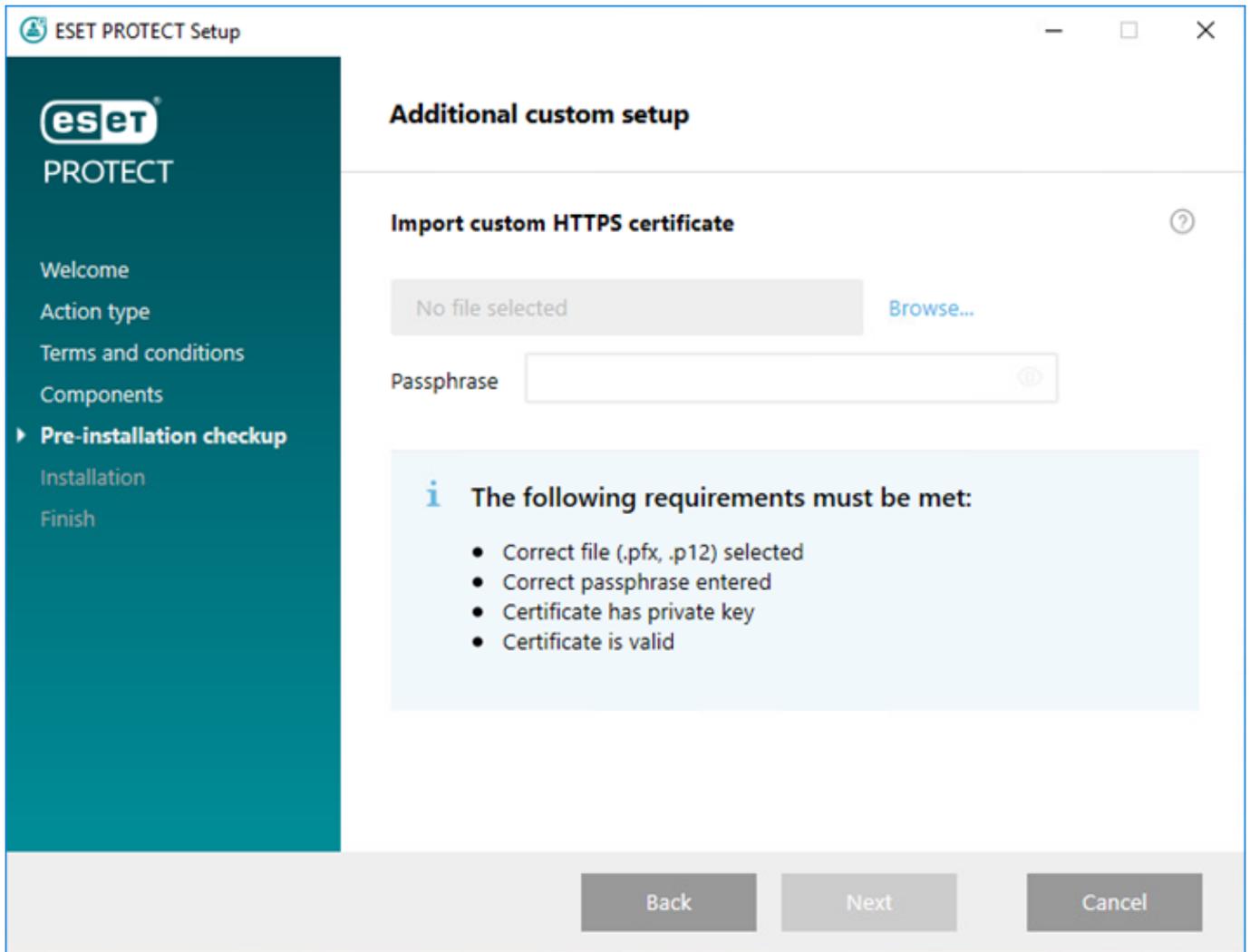
oESET Server Security para Windows (8 o posterior)

oCaché local compartido de ESET

La política habilita el Proxy HTTP para el producto afectado. El host del Proxy HTTP se encuentra en la dirección IP local y el puerto 3128 del servidor de ESET PROTECT. Se deshabilita la autenticación. Puede copiar esta configuración a otra política, si necesita configurar otro producto.



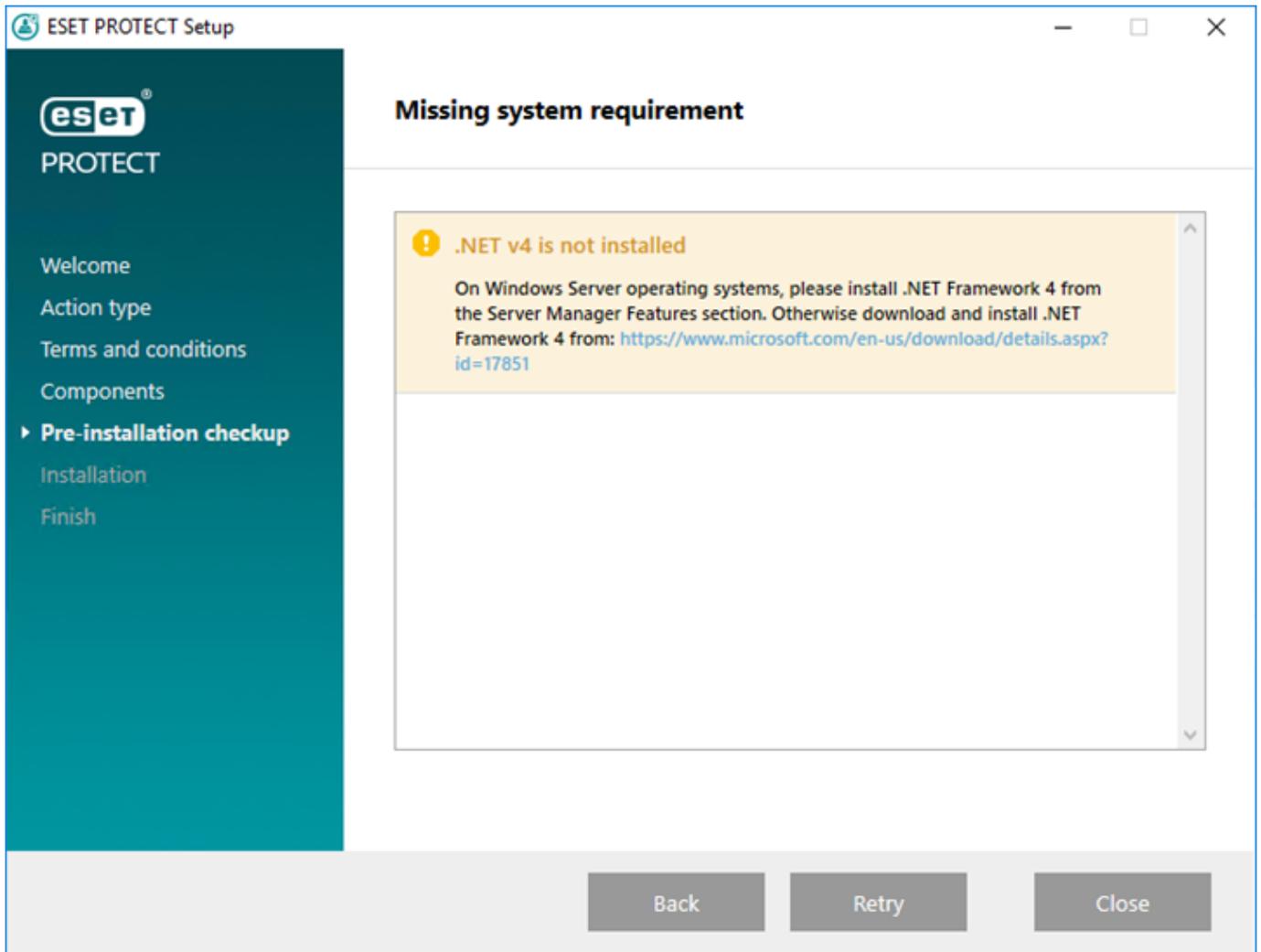
5. Si seleccionó **Agregar un certificado HTTPS personalizado para la consola web**, haga clic **Navegar** y seleccione un certificado válido (archivo *.pfx* o *.p12*) y escriba su **frase de contraseña** (o deje el campo en blanco si no hay frase de contraseña). El instalador instalará el certificado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



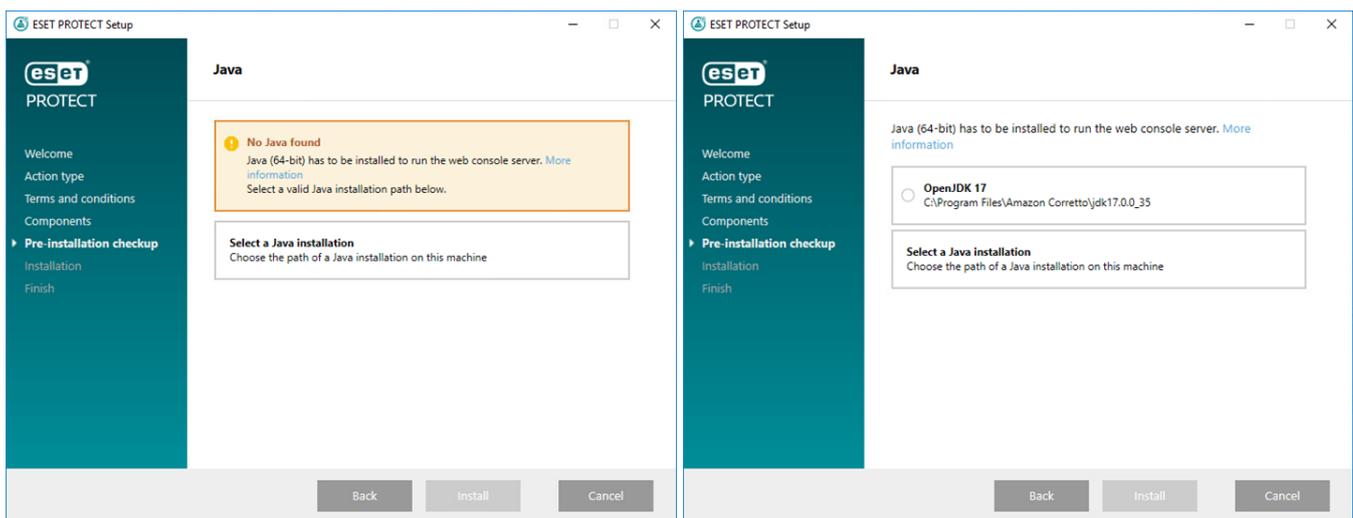
6. Si se encuentran errores durante la verificación de los prerrequisitos, abórdelos de la manera correspondiente. Asegúrese de que su sistema cumpla con todos los [prerrequisitos](#).

[^ .NET v4 no está instalado](#)

[Instalar .NET Framework](#)



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



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

⚠ 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 pasar a una alternativa sin costo. Consulte las [versiones compatibles de JDK](#).

a) Para seleccionar Java ya instalado, haga clic en **Seleccionar una instalación de Java**, seleccione la carpeta donde 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 indica si ha seleccionado una ruta no válida.

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

[Solo hay 32 MB libres en el disco del sistema](#)

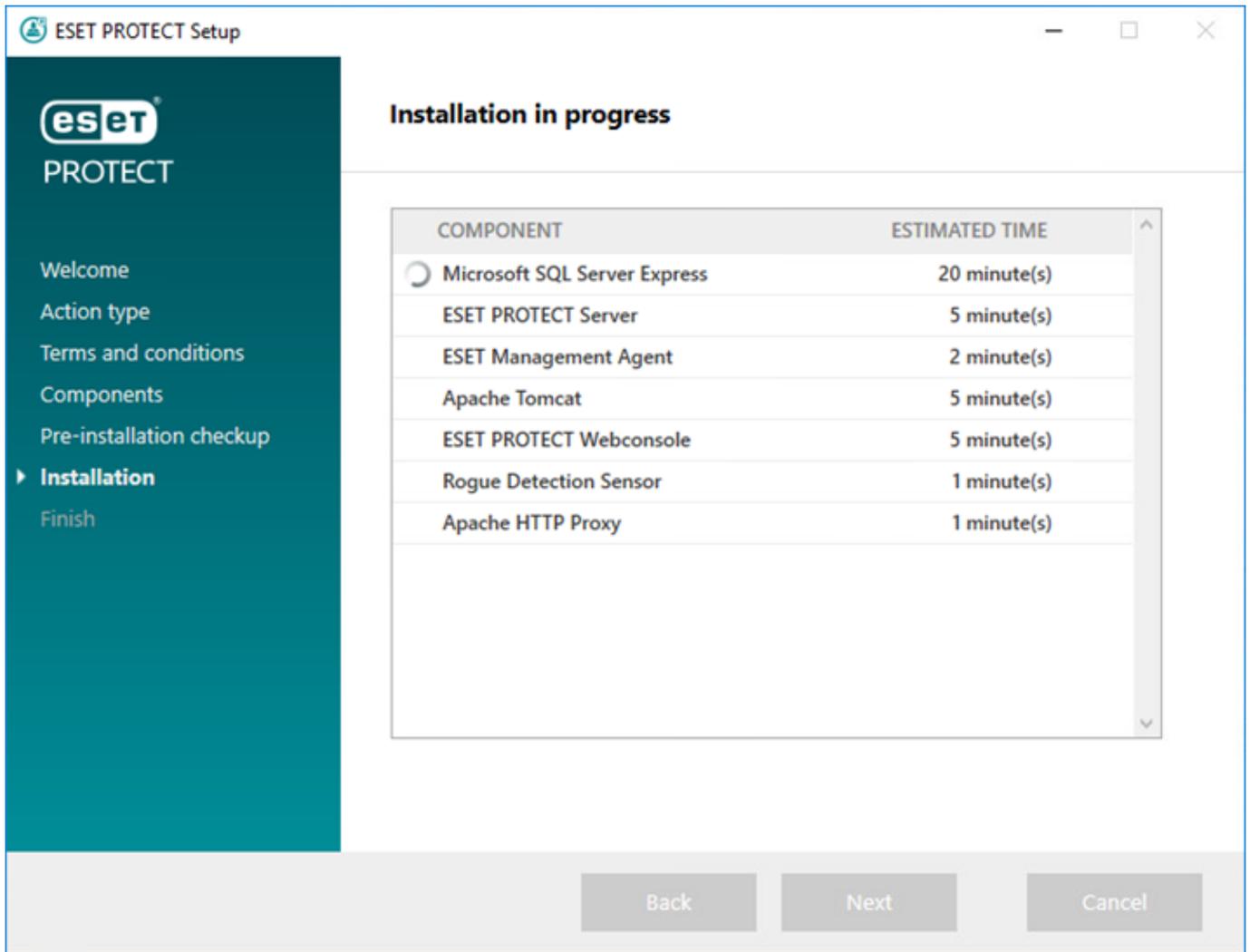
- El instalador podrá mostrar la siguiente notificación si su sistema no tiene suficiente espacio en disco para la instalación de ESET PROTECT.
- Debe contar con al menos 4400 MB de espacio libre en el disco para instalar ESET PROTECT y todos sus componentes.

[ESET Remote Administrator versión 5.x o superior está instalado en el equipo.](#)

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

7. Cuando se complete el control de los requisitos previos y su entorno cumpla con todos los [requisitos](#), se iniciará la instalación. Tenga en cuenta que el proceso de instalación puede llevar más de una hora, dependiendo de su sistema y la configuración de la red.

 Cuando la instalación se encuentra en progreso, el asistente de instalación ESET PROTECT no responde.



8. Si opta por instalar **Microsoft SQL Server Express** en el paso 4, el instalador realizará un control de conexión de base de datos. Si tiene un servidor de base de datos existente, el instalador le indicará que ingrese los detalles de conexión de su base de datos:

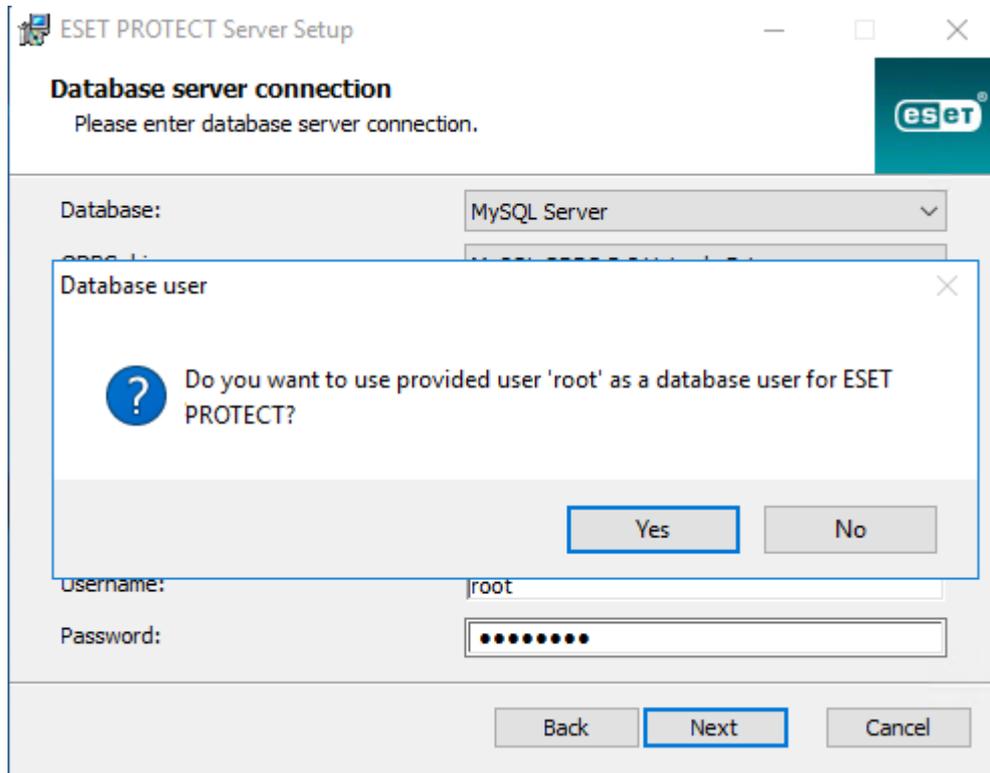
[Configure la conexión a SQL/MySQL Server](#)

Ingrese su **Nombre de base de datos**, **Nombre de host**, número de **Puerto** (podrá encontrar esta información en Microsoft SQL Server Configuration Manager) y los detalles de la **Cuenta de la base de datos (Nombre de usuario y Contraseña)** en los campos adecuados y haga clic en **Siguiente**. El instalador comprobará la conexión de la base de datos. Si tiene una base de datos existente (de una instalación ESMC/ESET PROTECT anterior) en su servidor de base de datos, se detectará. Puede elegir **usar una base de datos existente y aplicar la actualización** o **quitar la base de datos existente e instalar una nueva versión**.

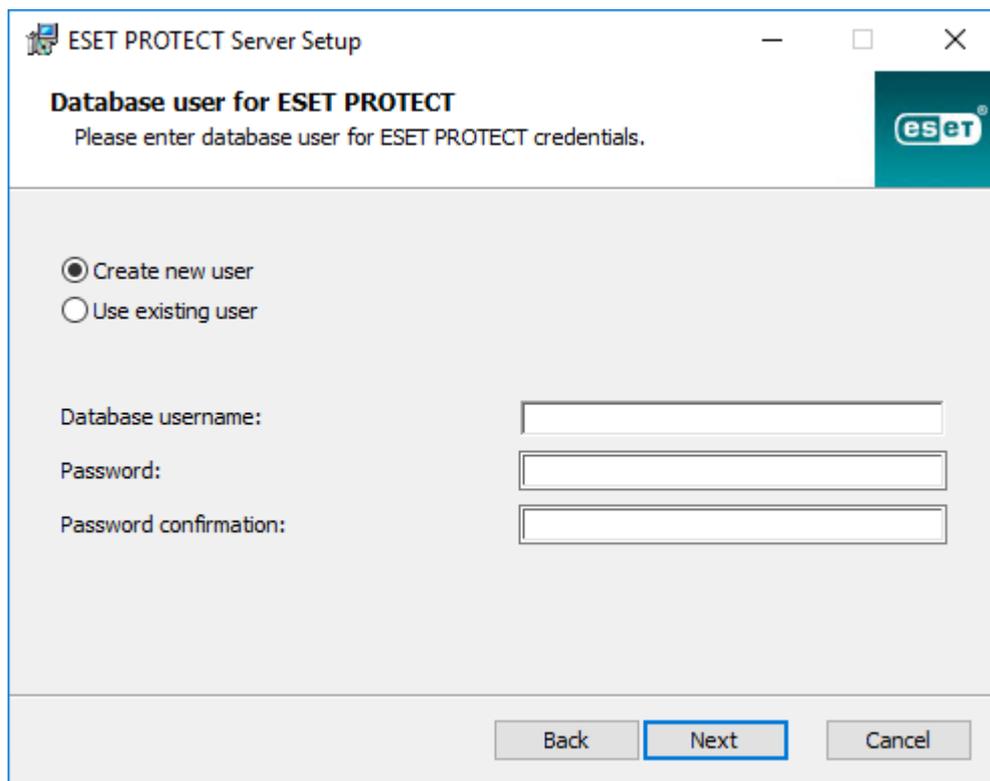
Usar instancia con nombre: si usa la base de datos MS SQL, puede seleccionar la casilla de verificación **Usar instancia con nombre** para usar una instancia de la base de datos con nombre. Puede configurarlo en el campo **Nombre de host** con el formato *HOSTNAME\DB_INSTANCE* (por ejemplo, *192.168.0.10\ESMC7SQL*). Para bases de datos en clúster use únicamente el nombre del clúster. Si selecciona esta opción, no puede cambiar el puerto de conexión a la base de datos; el sistema usará los puertos predeterminados por Microsoft. Para conectar el servidor ESET PROTECT a la base de datos de MS SQL instalada en un clúster de conmutación por error, ingrese el nombre del clúster en el campo **Nombre de host**.

i Hay dos opciones cuando ingresa la información de **cuenta de base de datos**. Puede usar una **cuenta de usuario de base de datos dedicada** que solo tendrá acceso a la base de datos ESET PROTECT o puede usar una **cuenta SA** (MS SQL) o una **cuenta raíz** (MySQL). Si decide usar una cuenta de usuario dedicada, deberá crear la cuenta con privilegios específicos. Para obtener más información, consulte la [cuenta de usuario de base de datos dedicada](#). Si no tiene intenciones de usar una cuenta de usuario dedicada, ingrese la cuenta del administrador (SA o raíz).

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



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



9. El instalador le solicitará que ingrese una contraseña para la cuenta de Administrador de la consola web. Esta contraseña es importante, ya que la usará para iniciar sesión en la [Consola web ESET PROTECT](#). 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: [Masked]

Password confirmation: [Masked]

Agent port: 2222

Console port: 2223

Back Next Cancel

10. Deje los campos intactos o introduzca su información corporativa para que aparezca en los detalles de los certificados del Agente ESET Management y del servidor ESET PROTECT. Si opta por ingresar una contraseña en el campo **contraseña de autoridad**, asegúrese de recordarla. Haga clic en **Siguiente**.

ESET PROTECT Server Setup

Certificate information
Please enter common certificate information below.

Organizational unit: [Empty]

Organization: [Empty]

Locality: [Empty]

State / Country: [Empty] ▼

Certificate validity: * 10 Years ▼

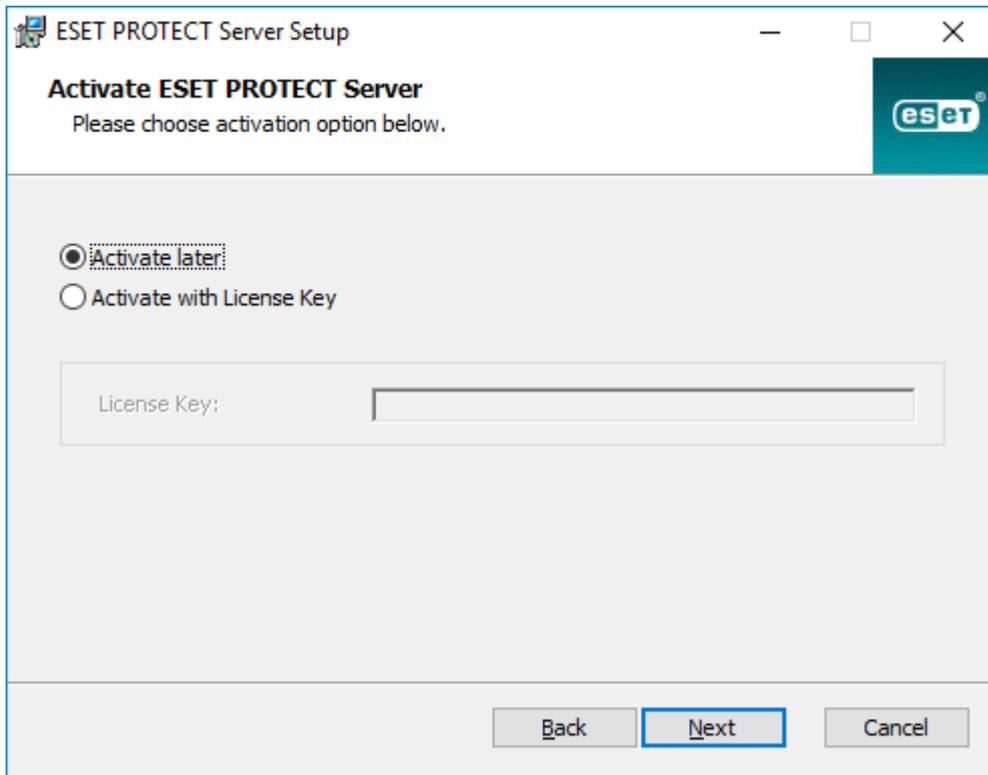
Authority common name: * Server Certification Authority

Authority password: [Empty]

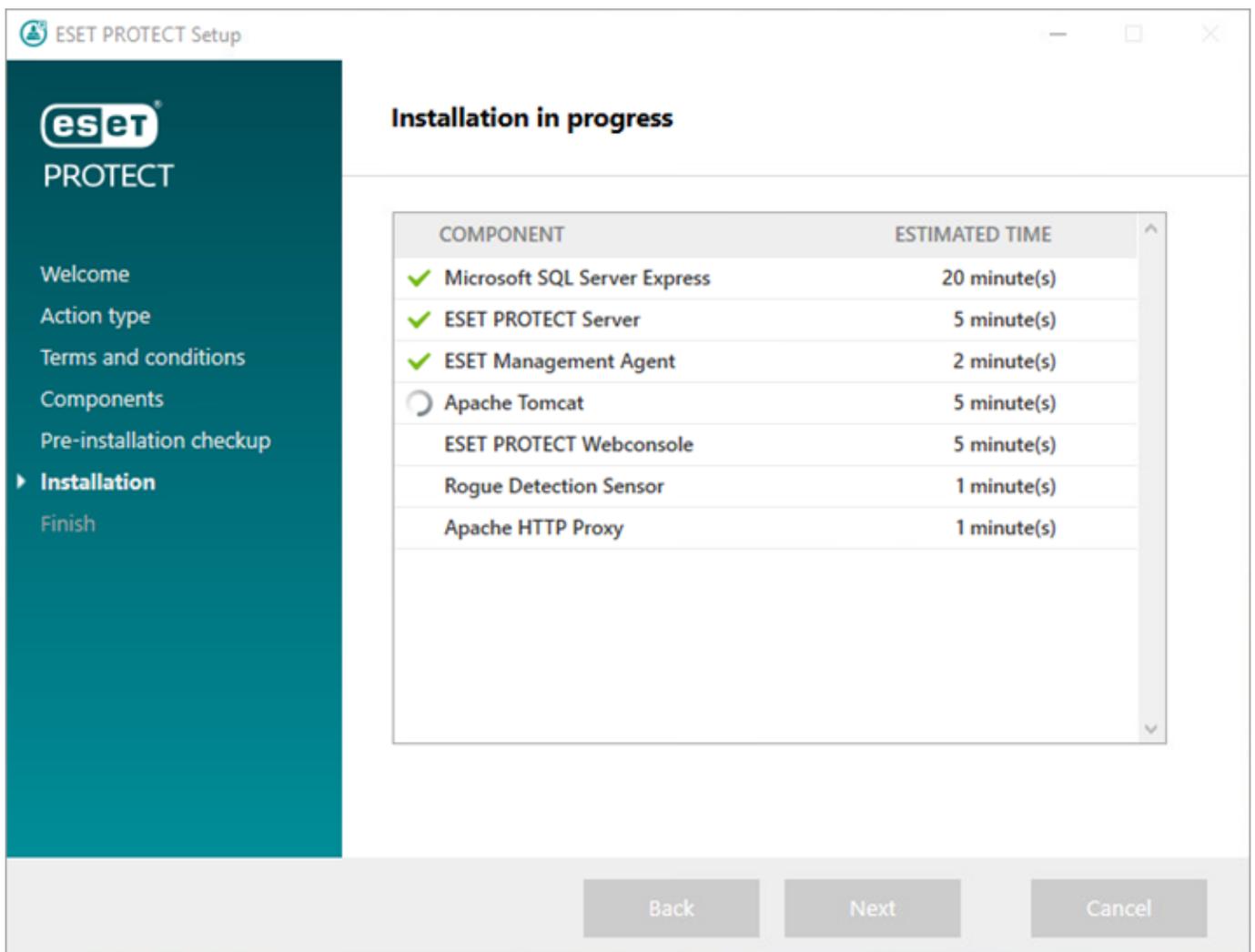
* required fields

Back Next Cancel

11. Ingrese una **Clave de licencia** válida (incluida en el correo electrónico de nueva compra que recibió de ESET) y haga clic en **Siguiente**. Si usa credenciales de la licencia de legado (Nombre de usuario y contraseña), [convierta](#) las credenciales en una clave de licencia. Como alternativa, puede optar por **Activar más tarde** (consulte el capítulo [Activación](#) para obtener instrucciones adicionales).



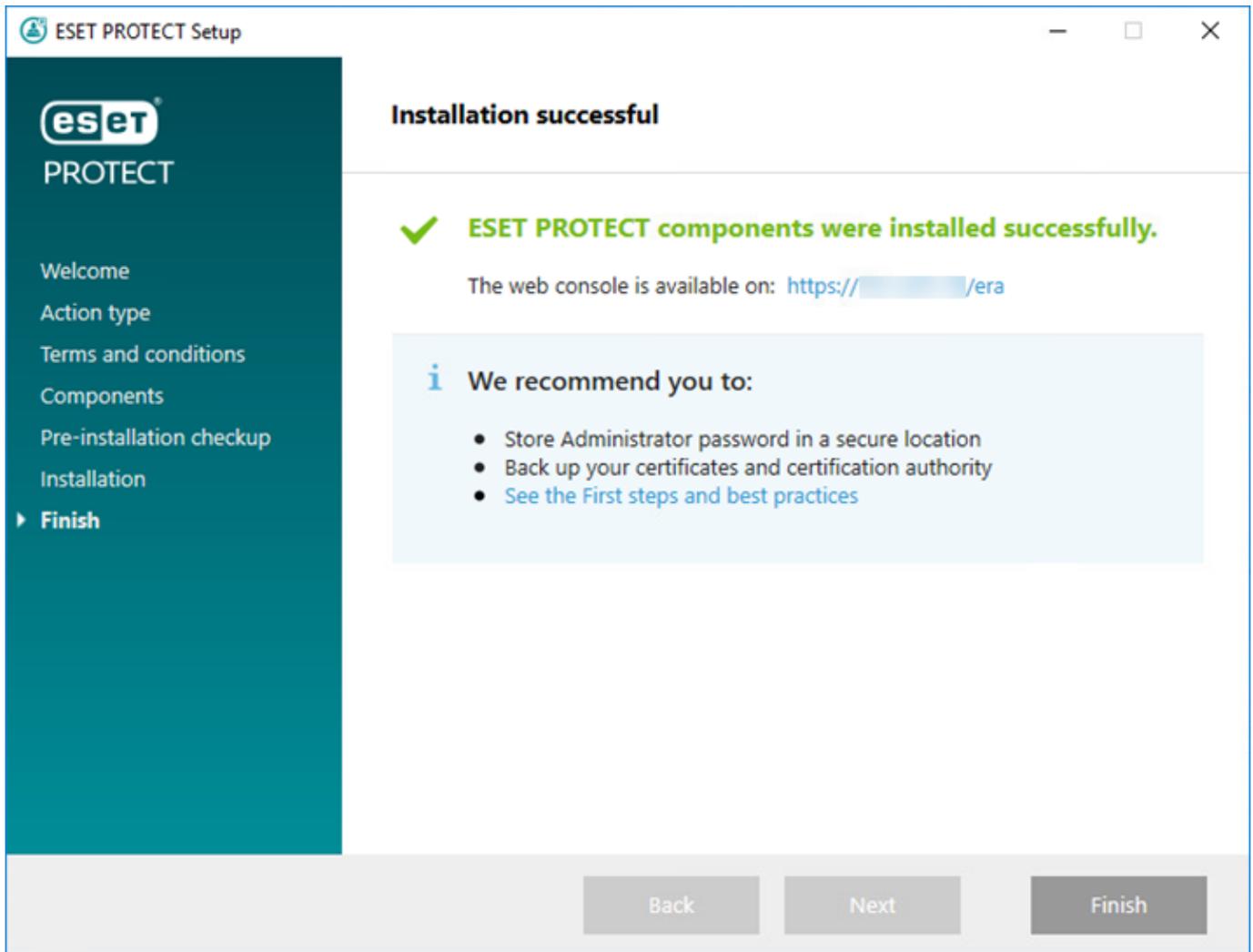
12. Verá el progreso de la instalación.



13. Si seleccionó instalar el **Sensor de Rogue Detection**, verá las ventanas de instalación del controlador

WinPcap. Asegúrese de marcar la casilla de verificación **Iniciar automáticamente el controlador de WinPcap al arrancar**.

14. Cuando finalice la instalación, se mostrará “La instalación de los componentes de ESET PROTECT se realizó correctamente” además de la dirección URL de la consola web de ESET PROTECT . Haga clic en la URL para abrir la [Consola web](#), o haga clic en **Finalizar**.



Si la instalación no se realizó 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 del instalador todo en uno, por ejemplo:
C:\Users\Administrator\Downloads\x64\logs\
- Consulte [Resolución de problemas](#) para obtener los pasos para resolver el problema.

Pasos posteriores a la instalación

Luego de la instalación de ESET PROTECT, puede iniciar la configuración.

Primeros pasos luego de la instalación de ESET PROTECT Server

1. Conéctese a la [consola web de ESET PROTECT](#).

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

3. Agregue sus [licencias](#).

4. [Instale el agente ESET Management y los productos de punto de conexión de ESET](#) en los equipos de su red.

 La [información general de estado](#) puede ayudarlo con la configuración inicial de ESET PROTECT.

Con el servidor ESET PROTECT instalado en su servidor y las soluciones de punto de conexión de ESET instaladas en los clientes, puede comenzar a administrar su red. Consulte la [Guía del administrador](#) para obtener más información sobre cómo puede administrar los productos de punto de conexión de ESET.

Pasos adicionales recomendados

- Utilice [notificaciones](#) e [informes](#) para supervisar el estado de los equipos cliente de su entorno, por ejemplo, si desea recibir una notificación sobre determinados eventos, o bien, ver o descargar un informe.
- Configure una conexión al [servidor SMTP](#). Esta configuración es opcional si desea recibir [notificaciones](#) o [informes](#) por correo electrónico. Puede configurar al servidor ESET PROTECT para enviar Notificaciones a su [servidor Syslog](#).
- Cree un [nuevo usuario de la consola web de ESET PROTECT](#).

Instalar el agente ESET Management y los productos de punto de conexión de ESET

Luego de haber instalado ESET PROTECT con éxito, es necesario implementar el Agente ESET Management y los productos ESET Endpoint para equipos en su red.

La implementación consiste en los siguientes pasos:

1. [Crear el paquete de instalación](#)
2. [Instalar el paquete de instalación](#)

Consulte también [otras opciones de instalación](#). Para redes más grandes, recomendamos usar [ESET Remote Deployment Tool](#).

Creación del paquete de implementación

El procedimiento de crear un paquete instalador todo en uno (que incluye el agente ESET Management y un producto de seguridad ESET) es parecido al [Asistente de inicio](#).

Haga clic en **Otras opciones de implementación** en la sección de **Enlaces Rápidos** de la barra del menú. En la ventana **Implementar Agente**, haga clic **Crear Instalador** en **Crear un instalador completo (solo para Windows)**. Se abrirá la ventana **Crear instalador todo en uno**.



El paquete de instalación es un archivo .exe y solo es válido para sistemas operativos Windows de Microsoft.

Básica

Desmarque la casilla de verificación al lado de **Participar en el programa de mejora del producto** si no está de acuerdo en enviar informes de fallas y datos de telemetría anónimos a ESET (versión y tipo de sistema operativo, versión de producto ESET y otra información específica del producto). Si la casilla de verificación está seleccionada, se enviará informes de fallas y datos de telemetría a ESET.

Contenido del paquete: seleccione la(s) casilla(s) de verificación a partir de las siguientes opciones:

- **Management Agent:** si no selecciona otros elementos en el **contenido del paquete**, el instalador incluirá solo el agente ESET Management. Seleccione esta opción si desea instalar el Producto de seguridad ESET en el equipo cliente más tarde, o si el equipo cliente ya tiene un Producto de seguridad ESET instalado.
- **Producto de seguridad:** incluye el producto de seguridad ESET con el agente ESET Management. Seleccione esta opción si el equipo cliente no tiene ningún Producto de seguridad ESET instalado y desea instalarlo con el agente ESET Management.
- **Cifrado de disco completo:** la opción de cifrado es visible únicamente para licencias activas de [ESET Full Disk Encryption](#).
- **Agente Enterprise Inspector:** incluya el agente ESET Enterprise Inspector en el instalador.

Producto de seguridad

1. **Licencia** (Opcional): puede agregar una licencia a través de uno de los métodos que se describen en [Administración de licencias](#). Si ya tiene licencias existentes en [Administración de licencias](#), simplemente elija la licencia que se usará para activar el producto de seguridad de ESET durante la instalación. Si no elige una licencia, podrá crear un instalador sin esta y [activar el producto más adelante](#). La función Incorporar/Quitar una licencia solo la puede llevar a cabo el administrador cuyo grupo hogar se encuentre configurado con la opción **Todo** y que tenga permiso de **Escribir** en las licencias de dicho grupo.
2. **Producto:** seleccione el producto de seguridad de ESET que se instalará junto con el agente de ESET Management.



Si no visualiza ningún archivo de instalación del producto, asegúrese de tener el repositorio establecido en **AUTOSELECT**. Para más información, consulte la sección de **Configuración avanzada** de la [Configuración del servidor](#).

3. **Idioma:** seleccione la versión de idioma del instalador de productos del producto de seguridad de ESET.
4. De manera opcional, puede seleccionar una **Política** que se aplicará en el producto de ESET Security durante su instalación.
5. **Configuración de protección:** marque la casilla de verificación que se encuentra junto a la configuración para habilitarla para el instalador:

oHabilite el sistema de respuesta ESET LiveGrid® (recomendado)

oHabilite la detección de aplicaciones potencialmente no deseadas: obtenga más información en nuestro [artículo de la base de conocimiento](#).

Seleccione la casilla de verificación junto a **No definir la configuración de protección ahora mismo (no recomendado)** si no desea definir esta configuración de protección para el instalador y, en su lugar, desea establecerla mediante políticas más tarde.

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

Agente Enterprise Inspector

Requisitos del agente ESET Enterprise Inspector:

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

1. **Licencia** (opcional): ESET le recomienda seleccionar la licencia ESET Enterprise Inspector para activar el agente ESET Enterprise Inspector durante la instalación. Si crea el instalador sin la licencia, puede activar el agente ESET Enterprise Inspector más tarde.
2. **Producto o versión:** seleccione la versión del agente ESET Enterprise Inspector. La versión disponible más reciente se encuentra preseleccionada.
3. **Política de configuración** (opcional): seleccione una política de agente ESET Enterprise Inspector existente para aplicar la configuración de la política durante la instalación del agente ESET Enterprise Inspector.
4. Seleccione la casilla de verificación **Acepto los términos del Acuerdo de licencia de usuario de la aplicación y la Política de privacidad**. Consulte el [Acuerdo de licencia de usuario final \(EULA\)](#), [los Términos de uso y la Política de privacidad de los productos ESET](#) para obtener más información.
5. Escriba el **nombre de host del servidor** ESET Enterprise Inspector y el **puerto** de conexión especificado durante la instalación del servidor ESET Enterprise Inspector (el puerto predeterminado es 8093).
6. Seleccione la **autoridad de certificación** para la conexión al servidor ESET Enterprise Inspector.

Certificado

Un certificado de pares y la autoridad de certificación de ESET PROTECT se eligen automáticamente con base en los certificados disponibles. Para usar un certificado diferente al seleccionado automáticamente, haga clic en

Certificado de ESET PROTECT para ver una lista de los certificados disponibles y, luego, elija el que desee usar. Si desea usar su propio [Certificado personalizado](#), haga clic en el botón de selección y cargue un archivo de certificado *.pfx*.

Ingrese la **Frase de contraseña del certificado** si fuera necesario. Por ejemplo, si especificó la frase de contraseña durante la instalación de ESET PROTECT o si usa el certificado personalizado con una frase de contraseña. De lo contrario, deje el campo **Frase de contraseña del certificado** en blanco.

 La frase de contraseña del certificado no debe contener los siguientes caracteres: " \ Estos caracteres provocan un error crítico al iniciar el agente.

 Recuerde que es posible extraer la **Frase de contraseña** del certificado porque está incorporado al archivo *.exe*.

Avanzado

En esta sección puede personalizar el paquete completo del instalador:

1. De forma opcional, puede cambiar el **Nombre** e ingresar una **Descripción** para el paquete instalador.
2. Haga clic en **Seleccionar etiquetas** para [asignar etiquetas](#).
3. **Grupo principal (opcional)**: seleccione el Grupo principal donde se colocará el equipo luego de la instalación. Puede seleccionar un grupo estático existente o crear uno nuevo al que se le asignará el dispositivo luego de implementar el instalador.
4. **ESET AV Remover**: seleccione la casilla de verificación si desea desinstalar o quitar por completo otros programas de antivirus del dispositivo de destino.
5. **Configuración inicial del instalador (opcional)**: use esta opción si desea aplicar una [política de configuración](#) al agente ESET Management. Haga clic en **Seleccionar** dentro de **Configuración del agente (opcional)** y elija entre la lista de políticas disponibles. Si ninguna de las políticas definidas previamente son adecuadas, puede crear [una nueva política](#) o personalizar las existentes.
6. **Nombre de host del servidor (opcional)**: escriba el nombre de host o la dirección IP del servidor de ESET PROTECT. De ser necesario, puede especificar el número de **Puerto** (el predeterminado es 2222).
7. Si usa un proxy HTTP, seleccione la casilla de verificación **Habilitar la configuración del proxy HTTP** y especifique la configuración del proxy (**Host, Puerto, Usuario y Contraseña**) para definir la conexión del agente ESET Management al proxy y habilitar el reenvío de comunicaciones entre el agente ESET Management y el servidor ESET PROTECT. El campo **Host** es la dirección del equipo en el que se ejecuta el [proxy HTTP](#). El proxy HTTP usa el puerto 3128 de manera predeterminada. Puede definir otro puerto, de ser necesario. Asegúrese de configurar el mismo puerto también en la configuración del proxy de HTTP.

 El protocolo de comunicación entre el Agente y el servidor ESET PROTECT no es compatible con la autenticación. Cualquier solución proxy que se use para reenviar la comunicación del agente hacia el servidor ESET PROTECT que requiera autenticación no funcionará.
Si elige usar un puerto no predeterminado para la consola web o el agente, puede requerir un ajuste del firewall. De lo contrario, la instalación puede fallar.

Habilite **Usar una conexión directa si el proxy HTTP no está disponible** si quiere permitir esta opción de respaldo.

8. Haga clic en **Finalizar**.

9. Descargue el paquete de instalación todo en uno generado. Seleccione la versión que desee instalar:

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

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

o Descargar la versión ARM64 (por ejemplo *PROTECT_Installer_arm64.exe*); no puede instalar la versión x86 o x64 del agente ESET Management o el producto de seguridad ESET en Windows ARM64.



Todos los datos descargados del repositorio (repositorio de ESET o réplica del repositorio personalizado) están firmados digitalmente por ESET y el servidor de ESET PROTECT verifica los hashes de los archivos y las firmas PGP. El servidor de ESET PROTECT genera el instalador todo en uno a nivel local. Por lo tanto, el instalador no tiene firma digital, lo que puede generar una advertencia del navegador web durante la descarga del instalador, generar una [advertencia](#) del sistema operativo y evitar la instalación en sistemas en los que los instaladores sin firmar están bloqueados.

10. Ejecute el archivo del paquete de instalación en un equipo del cliente. Se instalará el agente de ESET Management y el producto de ESET Security en el dispositivo, y podrá conectarse el dispositivo a ESET PROTECT. Para obtener instrucciones paso a paso, consulte la [instalación del paquete de instalación](#). Puede [ejecutar el paquete de instalación en un modo silencioso](#) para ocultar la ventana del asistente de configuración.

Instalación del paquete de implementación

Puede crear este paquete de instalación en [ESET PROTECT](#).

El paquete del instalador instala el agente de ESET Management y el paquete también puede instalar estos componentes (si se seleccionan durante la creación del paquete del instalador):

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

- El paquete del instalador es un archivo .exe y solo es compatible con 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 el agente ESET Management, el instalador lo actualizará a la versión del instalador.
- Debe ejecutar el programa de instalación con la cuenta predefinida de administrador o una Cuenta de administrador de dominio (en caso de que tenga la cuenta predefinida de administrador deshabilitada). Cualquier otro usuario, sin importar si es miembro del grupo de Administradores, no tendrá derechos de acceso suficientes. Por consiguiente, necesita usar la cuenta predefinida de administrador, ya que no podrá completar la instalación con éxito en ninguna otra cuenta de usuario que no sea el administrador local o de dominio.
- Todos los datos descargados desde el repositorio (repositorio de ESET o replicación del repositorio personalizado) están firmados digitalmente por ESET y el servidor ESET PROTECT verifica los hashes de los archivos y las firmas PGP. El servidor de ESET PROTECT genera el instalador todo en uno a nivel local. Por lo tanto, el instalador todo en uno no está firmado digitalmente, lo que podría generar una advertencia del navegador web durante la descarga del instalador o generar una [alerta](#) del sistema operativo y evitar la instalación en sistemas en los que los instaladores no firmados están bloqueados.
- Recuerde que es posible extraer datos confidenciales (por ejemplo, la frase de contraseña del certificado) porque está incorporado al instalador.
- El instalador de ESET Endpoint Antivirus/Security creado en ESET PROTECT 8.1, y versiones posteriores, es compatible con el modo de varias sesiones de Windows 10 y Windows 10 Enterprise for Virtual Desktops.

Proceso de instalación

- Si desea ejecutar el instalador sin visualizar una ventana de diálogo, siga las [instrucciones de instalación silenciosa](#).
- Si ocurrió un error en el proceso de instalación, consulte la [sección de Resolución de problemas](#) para ver los errores de instalación más comunes.

1. Ejecute el paquete del instalador.

Asegúrese de desinstalar del equipo cualquier producto de seguridad de terceros antes de instalar el producto de seguridad de ESET.

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

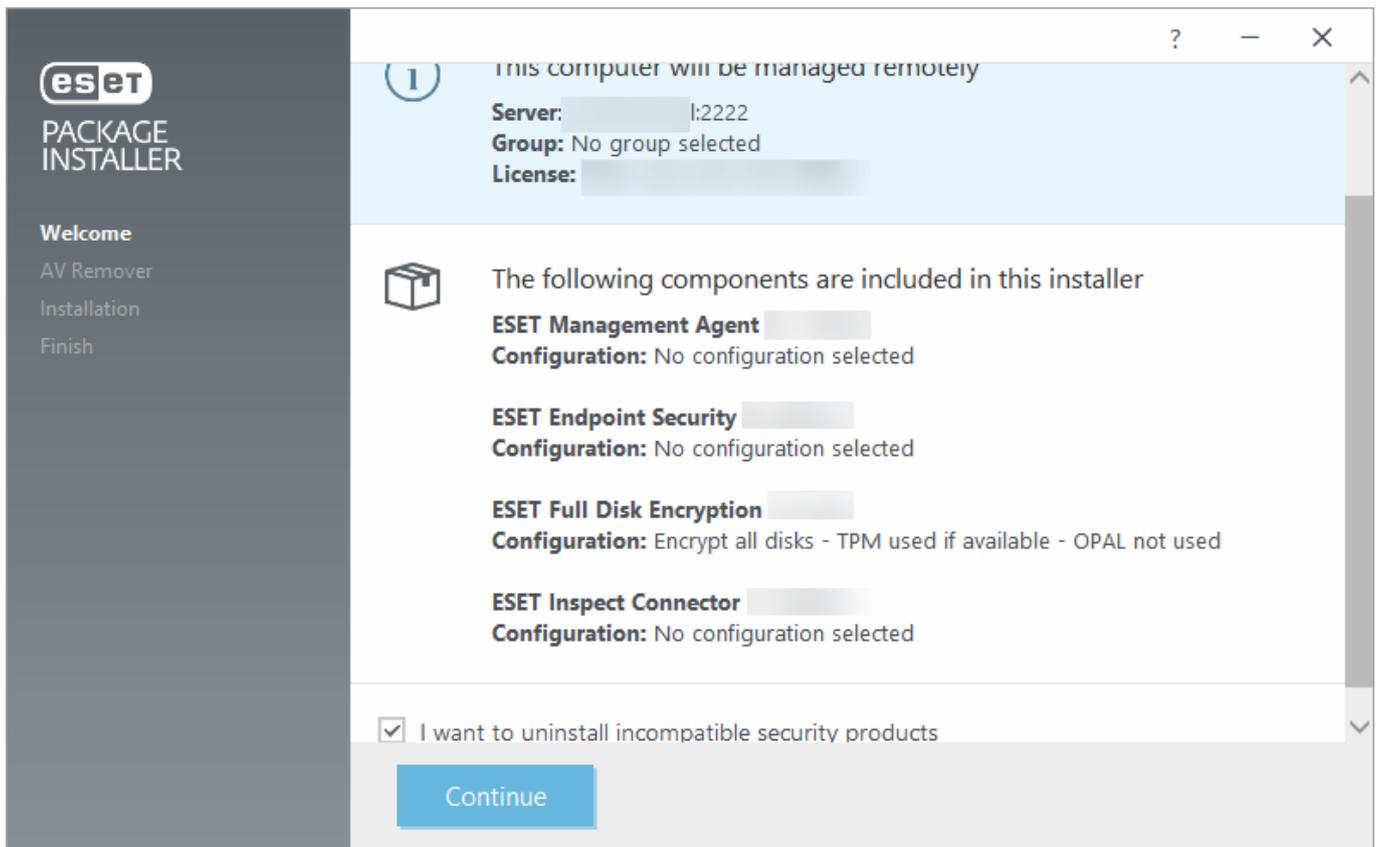
a) Marque la casilla de verificación **Quiero desinstalar los productos de seguridad no compatibles** para quitar o desinstalar software de seguridad de terceros que se ejecute o instale en su equipo. Consulte la [lista de software compatible](#).

b) Haga clic en **Continuar**.

c) Luego de explorar las aplicaciones instaladas, seleccione la casilla de verificación junto a las aplicaciones que desea eliminar y haga clic en **Eliminar**. Para obtener más detalles, consulte nuestro [artículo de la Base de conocimiento](#) sobre ESET AV Remover.

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

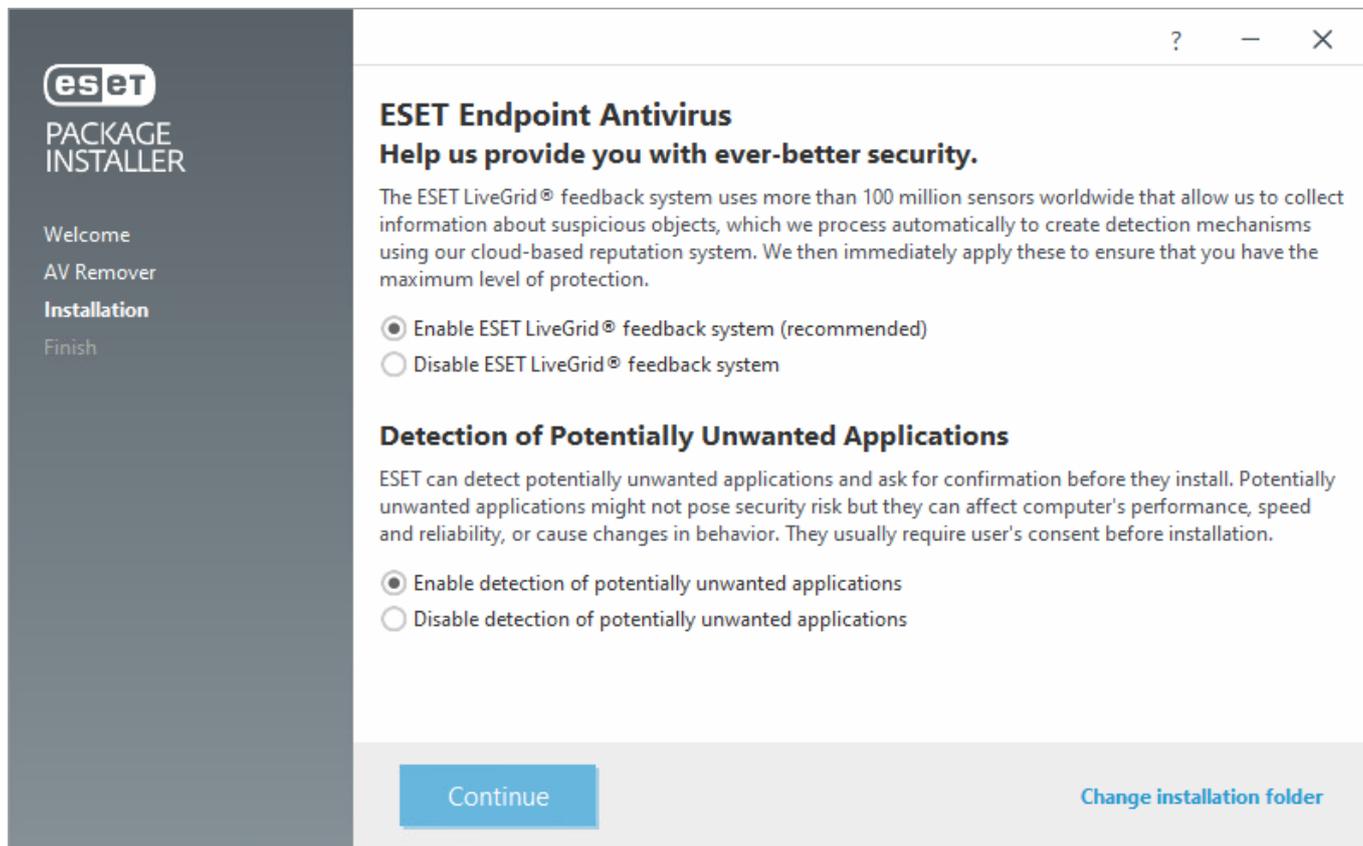
- Si no utiliza ningún producto de seguridad de terceros en su equipo local, haga clic en **Continuar**.



2. **Configuración de protección:** marque la casilla de verificación que se encuentra junto a la configuración para habilitarla para el instalador:

oHabilite el sistema de respuesta ESET LiveGrid® (recomendado)

oHabilite la detección de aplicaciones potencialmente no deseadas: obtenga más información en nuestro [artículo de la base de conocimiento](#).



3. Una vez finalizada la instalación, haga clic en **Listo**. El producto de Seguridad de ESET se abrirá automáticamente. Puede verificar el registro de estado (`C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.html` esta ubicación se encuentra oculta de manera predeterminada) en la máquina del cliente para asegurarse de que el Agente ESET Management funcione correctamente. En caso de que hubiera problemas con el agente ESET Management instalado (por ejemplo, si no se conecta al servidor ESET PROTECT), consulte [Resolución de problemas de conexión del agente](#).

Solución de problemas

Si ocurrió un error en el proceso de instalación, consulte la [sección de Resolución de problemas](#) para ver los errores de instalación más comunes.

Otros métodos de implementación

Puede instalar los productos de puntos de conexión de ESET o el agente ESET Management de forma independiente y de varias maneras.

Instalar el agente ESET Management

Implementación local:

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

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

Instalación remota (recomendada 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 de instalación del agente](#)

Instalar productos de punto de conexión de ESET

Una vez que se instala el agente ESET Management, puede instalar el producto de punto de conexión de ESET directamente desde ESET PROTECT de dos maneras:

- Usando la [Tarea de instalación de software](#)
- Localmente, mediante el uso de la instalación estándar del producto ESET

ESET Remote Deployment Tool

La ESET Remote Deployment Tool es una manera conveniente de distribuir el [paquete del instalador](#) creado por ESET PROTECT para implementar el agente de ESET Management y productos de seguridad de ESET de manera remota en equipos que pertenecen a una red.

ESET Remote Deployment Tool se encuentra disponible de forma gratuita en el [sitio web](#) de ESET como un componente independiente de ESET PROTECT. La herramienta de instalación está pensada principalmente para la instalación en redes pequeñas o medianas, y se ejecuta conforme a los privilegios de administración.

 ESET Remote Deployment Tool se diseñó para implementar el Agente ESET Management en equipos cliente con sistemas operativos Microsoft Windows [compatibles](#), únicamente.

Requisitos previos de la herramienta de implementación remota de ESET

 Para implementaciones remotas, verifique que todos los equipos clientes estén conectados a Internet.

Los siguientes prerrequisitos deben cumplirse para usar ESET Remote Deployment Tool en Windows:

- Debe instalar el Servidor ESET PROTECT y la Consola web ESET PROTECT (en un equipo del Servidor).
- Se deben abrir los puertos adecuados. Consulte los [puertos usados para la implementación remota del Agente ESET Management en un equipo de destino con sistema operativo Windows](#).
- Los nombres de paquetes de instalación deben incluir la cadena "x86" o "x64". De lo contrario, no funcionará la implementación.
- Se debe [crear](#) y [descargar](#) un paquete instalador todo en uno en su unidad local.
- Es necesario contar con permisos para [crear un instalador todo en uno](#).

i La implementación puede fallar por varios motivos. En caso de problemas con la implementación, lea el [capítulo sobre Resolución de problemas](#) o [los escenarios de ejemplo verificados de la implementación del Agente ESET Management](#).

Para implementar Agentes de ESET Management en equipos cliente, siga estos pasos:

1. [Descargue](#) ESET Remote Deployment Tool desde el sitio Web de ESET.
2. Asegurarse de que se cumplan todos los [prerrequisitos](#).
3. Ejecutar ESET Remote Deployment Tool en el equipo del cliente.
4. Seleccione **Agregar equipos manualmente**. Necesitará ingresar una lista de nombres de host o direcciones IP manualmente.
5. Ingrese los nombres de host o las direcciones IP y haga clic en **Siguiente**. Cada dirección IP o nombre de host debe estar en una línea nueva.

! Asegúrese de que los equipos seleccionados tengan la misma plataforma (sistemas operativos de 64 bits o 32 bits).

6. Se mostrarán equipos seleccionados para implementación remota. Asegúrese de que se hayan agregado todos los equipos y luego haga clic en **Siguiente**.
7. Haga clic en **Buscar** y seleccione el paquete de instalación que creó en la consola web [ESET PROTECT](#) o [en ESET PROTECT Cloud](#). También puede seleccionar **Usar el paquete de instalación sin conexión de ESET** (archivo *.dat*) creado a partir del ESET PROTECT Live Installer. Si no tiene ninguna aplicación de seguridad adicional instalada en su equipo local, quite la selección de la casilla de verificación junto a **Usar ESET AV Remover**. ESET AV Remover puede quitar [ciertas aplicaciones](#).
8. Ingrese las credenciales de inicio de sesión para los equipos objetivos. Si los equipos son miembros de un dominio, ingrese las **credenciales de administrador de dominio**. Si inicia sesión con **credenciales de administrador de dominio**, es necesario [desactivar UAC remoto en los equipos objetivos](#). De manera opcional, puede seleccionar la casilla de verificación junto a **Usar credenciales de usuario actuales**.
9. Se utiliza el **método de instalación** para ejecutar programas en máquinas remotas. El método **Incorporado** es una configuración predeterminada que admite mensajes de error de Windows. **PsExec** es una herramienta de terceros y una alternativa al método Incorporado. Seleccione una de estas opciones y haga clic en **Siguiente**.



Si ha seleccionado **PsExec**, la instalación fallará debido a que la herramienta no puede aceptar el Acuerdo de licencia de usuario final de **PsExec**. Para una instalación correcta, abra la línea de comandos y ejecute el comando **PsExec** manualmente.

10. Cuando se inicia la instalación, se mostrará "Éxito". Haga clic en **Finalizar** para completar la implementación. Si falla la implementación, puede exportar una lista de equipos fallidos. Haga clic en **Buscar** junto al campo **Exportar equipos fallidos**, seleccione un archivo **.txt** en el que quiere guardar la lista y haga clic en **Exportar equipo fallido**.

Progress	
COMPUTER	STATUS
✓ [blurred]	Success

Puede verificar el registro de estado (*C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.htm*) en la máquina cliente para asegurarse de que el Agente ESET Management funcione de manera correcta.

Otros métodos para instalar los agentes ESET Management con ESET Remote Deployment Tool

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

- [Red de escaneo](#): proporcione rangos de IP para explorar equipos en la red.
- [Importar lista](#): proporcione una lista de nombres de host o direcciones IP.

Solución de problemas

i La implementación puede fallar por varios motivos. En caso de problemas con la implementación, lea el [capítulo sobre Resolución de problemas](#) o [los escenarios de ejemplo verificados de la implementación del Agente ESET Management](#).

Consola web ESET PROTECT

Ingrese a la Consola Web ESET PROTECT

- En su servidor Windows local (el equipo en el que se aloja su consola web):

Haga clic en **Iniciar > Todos los programas > ESET > Consola web de ESET PROTECT**.

- Desde cualquier lugar con acceso a Internet a su servidor web, escriba la URL con 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 en su navegador web.

i Use un [navegador web compatible](#) para conectarse a la consola web de ESET PROTECT.

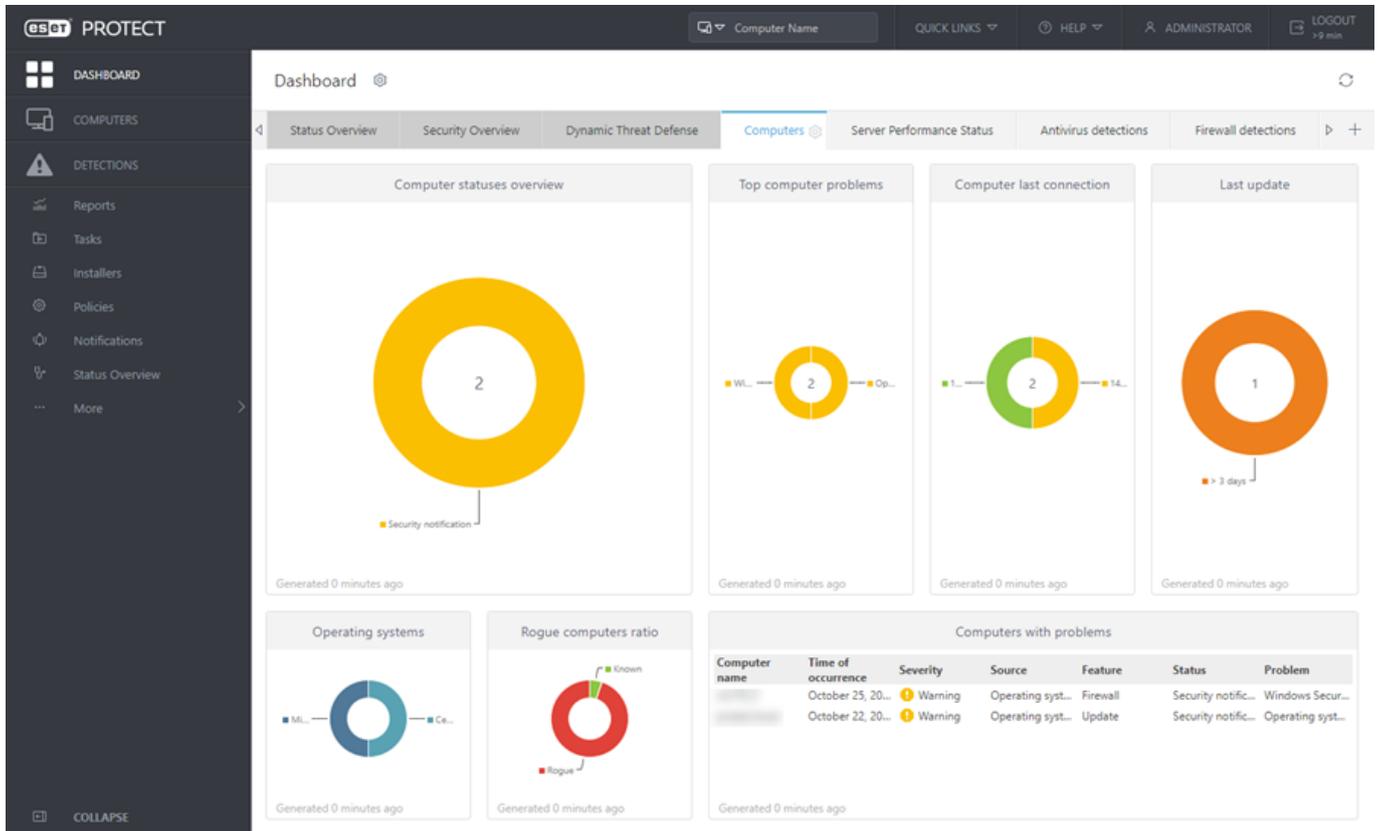
Cuando inicia sesión en la consola web por primera vez, se muestra un [Asistente de inicio](#) para ESET PROTECT. Puede usarlo para instalar los agentes de ESET Management en equipos de su red.

Interfaz del usuario de la consola web de ESET PROTECT

La interfaz del usuario de la consola web de ESET PROTECT consta de varias partes:

- Puede usar la herramienta **Búsqueda** en la parte superior de la consola web de ESET PROTECT.
- Haga clic en **Enlaces rápidos** para realizar algunas de las acciones de la consola web más usadas.
- Si necesita ayudar al trabajar con ESET PROTECT, haga clic en el ícono  **Ayuda** en la esquina superior derecha y haga clic en **<Current topic> - Ayuda**. Se visualizará la ventana de ayuda correspondiente a la página actual.
- En la esquina superior derecha se muestra el [usuario](#) actual con la cuenta regresiva del tiempo de espera de la sesión del usuario. Puede hacer clic en **Cerrar sesión** para cerrar sesión en cualquier momento. Cuando expira una sesión (por la inactividad del usuario), debe iniciar sesión nuevamente.

- El menú principal a la izquierda de la consola web contiene herramientas que los administradores pueden usar para administrar las soluciones de seguridad del cliente y para la configuración del servidor ESET PROTECT. Puede usar las herramientas en **Más** para configurar el entorno de red y minimizar las necesidades de mantenimiento. También puede configurar [notificaciones](#) y [dashboards](#) para estar al tanto del estado de la red.

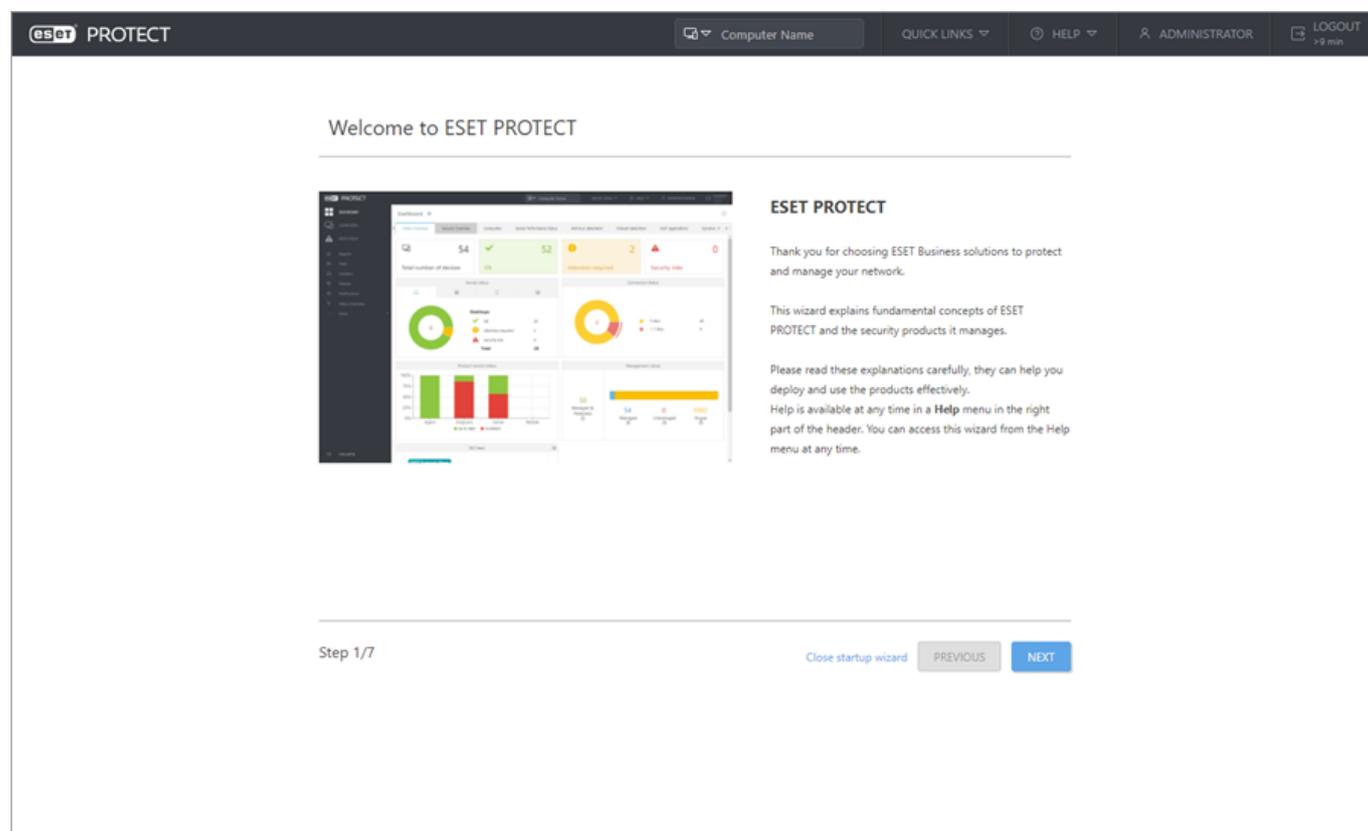


En los temas que se indican a continuación se describen los elementos principales del menú:

 Dashboard
 Equipos y grupos
 Detecciones
 Informes
 Tareas
 Políticas
 Notificaciones
 Información general de estado
*** Más > Exclusiones
*** Más > Cuarentena
*** Más > Usuarios y conjuntos de permisos
*** Más > Administración de licencias
*** Más > Certificados

Asistente de inicio

Cuando inicia sesión en la consola web por primera vez, aparecerá un **Asistente de inicio** para ESET PROTECT. Puede usarlo para implementar los agentes de ESET Management en equipos de su red. El asistente le dará una explicación básica de las secciones importantes de la consola web de ESET PROTECT.



The screenshot displays the ESET PROTECT web console interface. At the top, there is a dark header with the ESET PROTECT logo on the left and navigation links for 'Computer Name', 'QUICK LINKS', 'HELP', 'ADMINISTRATOR', and 'LOGOUT >9 min' on the right. The main content area is titled 'Welcome to ESET PROTECT'. On the left, there is a preview of the dashboard showing various metrics and charts. On the right, there is a section titled 'ESET PROTECT' with the following text: '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.' At the bottom of the wizard, it shows 'Step 1/7' and navigation buttons for 'Close startup wizard', 'PREVIOUS', and 'NEXT'.

El último paso del Asistente de inicio llamado **Instalación** lo ayudará a crear un paquete instalador todo en uno (que contiene al agente ESET Management y el producto de seguridad ESET). También puede [crear un instalador de agente todo en uno](#) sin usar el asistente al hacer clic en **Otras opciones de instalación** en la sección **Enlaces 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

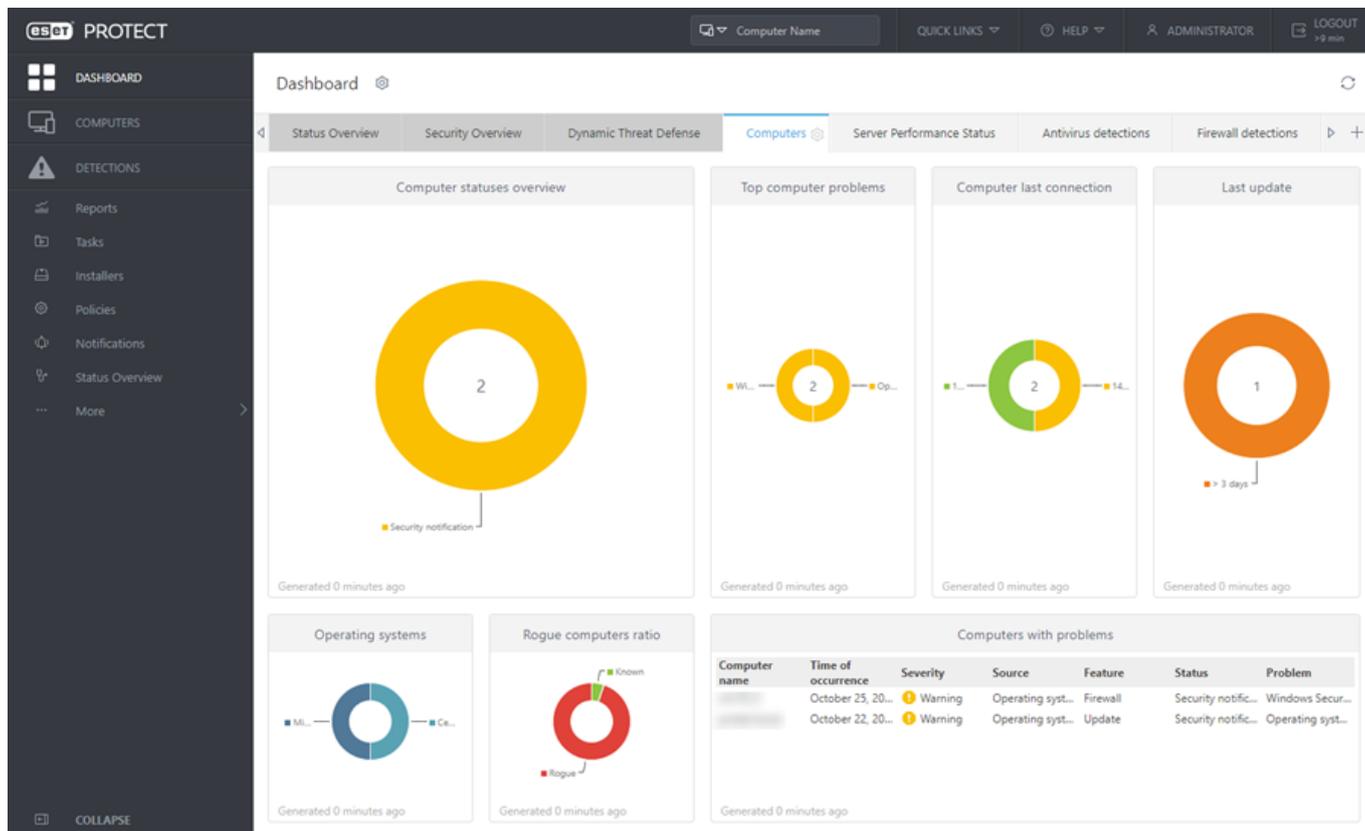
Enterprise Inspector Agent
 Show ESET Enterprise Inspector Agent settings

Step 7/7 Close startup wizard

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

Tablero

Dashboard es la pantalla predeterminada que se muestra cuando el usuario inicia sesión en la consola web de ESET PROTECT. Muestra los informes predefinidos sobre su red. Puede alternar entre los dashboards por medio de las pestañas que se encuentran en la barra superior del menú. Cada tablero consta de varios informes.



Puede personalizar sus dashboards (excepto **Información general de estado**, **Información general de seguridad** y **Dynamic Threat Defense**) al agregar [informes](#), modificar informes existentes, cambiarles el tamaño, moverlos o reorganizarlos. Esta versatilidad le permite crear una visión general exhaustiva de ESET PROTECT y sus objetos ([equipos](#), [grupos](#), [tareas](#), [políticas](#), [usuarios](#), etc.).

Los siguientes tableros vienen preconfigurados en ESET PROTECT:

- **Información general de estado:** ventana básica del dashboard con la información clave sobre la red de ESET PROTECT. Este dashboard no puede modificarse.
- **Información general de seguridad:** este dashboard provee una vista general de detecciones sin resolver que se informaron en los 7 días anteriores, que incluye la gravedad, el método de detección, el estado de resolución y los 10 equipos/usuarios principales con detecciones. Este dashboard no puede modificarse.
- **Dynamic Threat Defense:** si usa [ESET Dynamic Threat Defense](#), aquí encontrará una descripción general de informes útiles ESET Dynamic Threat Defense.
- **Equipos:** Este tablero le proporciona una visión general de los equipos cliente; su estado de protección, sistemas operativos, estado de actualización, etc.
- **Estado del rendimiento del servidor:** En este tablero, puede visualizar la información acerca del servidor de ESET PROTECT en sí; carga del servidor, clientes con problemas, carga de la CPU, conexiones de la base de datos, etc.
- **Detecciones del antivirus:** aquí, puede ver los informes del módulo antivirus de los productos de seguridad del cliente; detecciones activas, detecciones en los últimos 7/30 días, etc.
- **Detecciones del Firewall:** los eventos de firewall de los clientes conectados; según su gravedad, tiempo de generación de informes, etc.

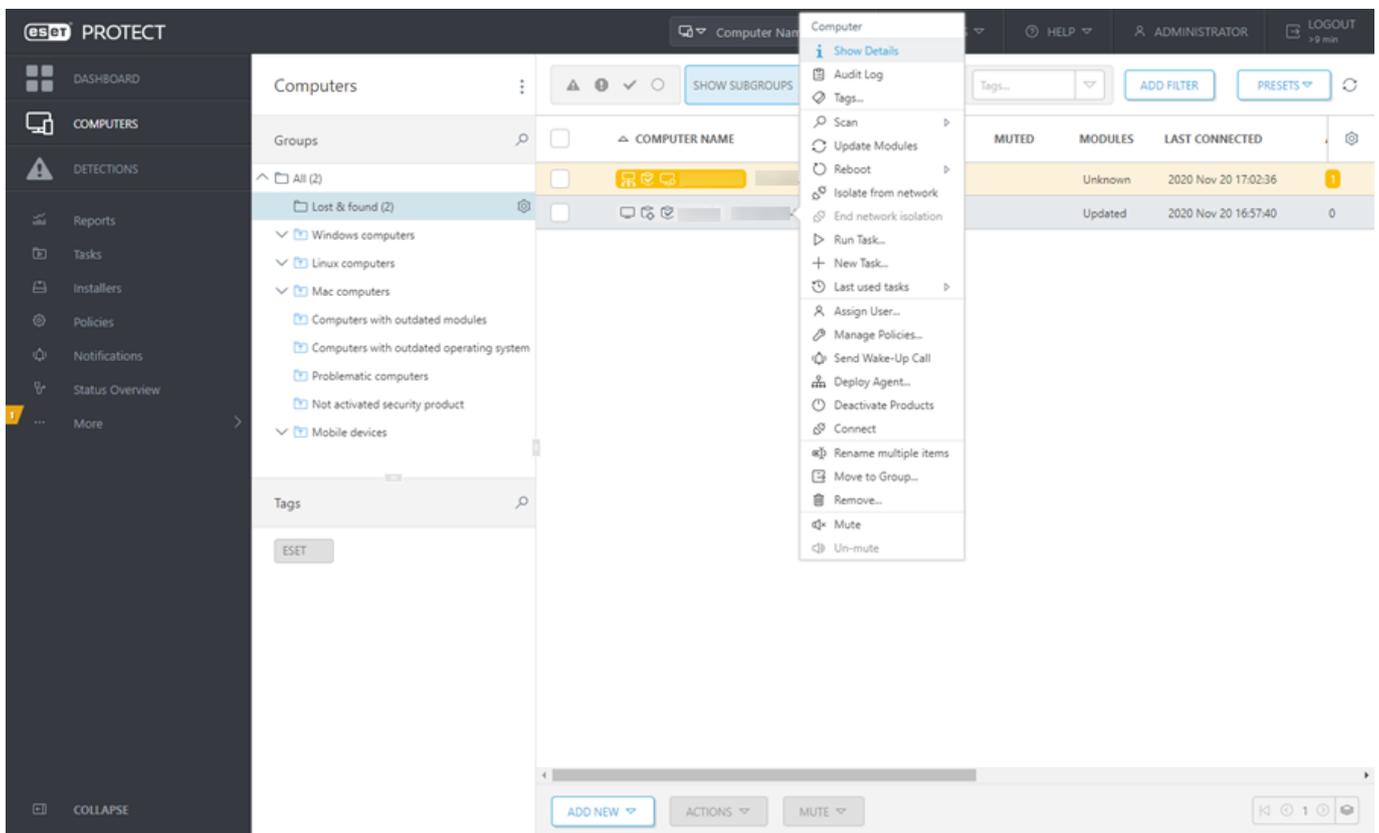
- **Aplicaciones de ESET:** este tablero le permite ver información sobre aplicaciones de ESET instaladas.
- **Protección basada en la nube:** este dashboard le ofrece una visión general de los informes de protección basados en la nube (ESET LiveGrid® y, si tiene la licencia válida, también ESET Dynamic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

Equipos

Todos los equipos cliente que alcanza ESET PROTECT se muestran en  **Equipos** y se organizan por [grupos](#). Al hacer clic en un grupo de la lista (panel izquierdo) se visualizarán los miembros (clientes) de este grupo en el panel derecho. Puede arrastrar y soltar clientes para moverlos entre los grupos.

Administrar equipos

Haga clic en un dispositivo para abrir un nuevo menú con acciones disponible para ese dispositivo. También puede seleccionar la casilla de verificación junto a un dispositivo y hacer clic en el botón **Acciones** en la barra inferior. El menú **Acciones** muestra diferentes opciones según el tipo de dispositivo.



Filtrar equipos

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

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

- Seleccione la casilla de verificación **Mostrar subgrupos** para mostrar los subgrupos del grupo seleccionado actualmente.

- Al hacer clic en **Agregar filtro**, se muestran los criterios de filtrado disponibles. Algunos filtros predefinidos también están disponibles y se puede acceder a ellos rápidamente.

- Puede hacer clic en **Agregar filtro > Categoría de productos** y seleccionar entre las categorías disponibles:

OTodos los dispositivos: muestra todos los equipos cliente sin filtrar. Cuando se limita la vista, puede usar una combinación de todas las opciones de filtrado anteriores.

OProtegido por ESET: muestra los clientes con protección de un producto ESET.

O ESET PROTECT: muestra los componentes individuales de ESET PROTECT como el agente, RD Sensor y Proxy.

O Otros: muestra solo los equipos cliente que ejecuten el producto seleccionado (Shared Local Cache, Virtual Security Appliance o Enterprise Inspector).

- Puede usar los íconos de estado para filtrar clientes por la gravedad de los problemas detectados ( rojo para errores,  amarillo para advertencias,  verde para avisos y  gris para equipos no administrados). El ícono de estado representa el estado actual de un equipo cliente específico y la solución de ESET instalada en el mismo. Puede ocultar o mostrar los íconos de estado de diferente gravedad para evaluar los clientes de su red en función del estado. Por ejemplo, para ver solamente los equipos con advertencias, active solo el ícono amarillo (el resto de los íconos deben estar inactivos). Para ver tanto advertencias como errores, active los íconos de estado rojos y amarillos. Los equipos no administrados  (clientes en la red que no tienen instalado el agente ESET Management o un producto de seguridad de ESET) suelen aparecer en el grupo estático **Perdidos y Encontrados**.

- También puede hacer clic en el encabezado de una columna para ordenar los equipos según ese atributo.

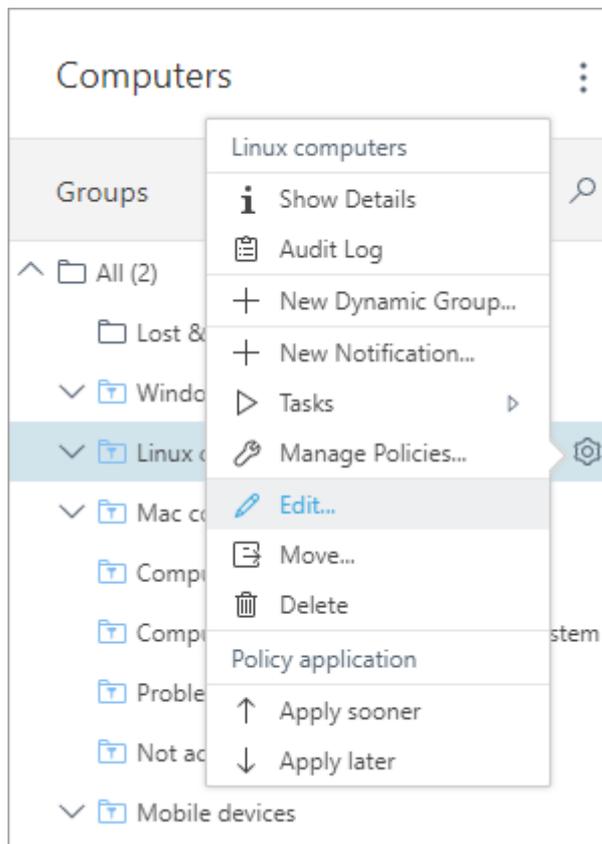
Última conexión muestra la fecha y la hora de la última conexión del dispositivo administrado. Un punto verde indica que el equipo se conectó hace menos de 10 minutos. Se resalta la información sobre la **Última conexión** para indicar que el equipo no se está conectando:

oAmarillo (error): hace de 2 a 14 días que el equipo no se conecta.

oRojo (advertencia): hace más de 14 días que no se conecta el equipo.

Grupos

Puede administrar grupos desde  [Equipos](#). Los grupos le permiten organizar los puntos de conexión en la red para poder asignarles [políticas](#) y [tareas](#) de forma sistemática. La configuración se aplica a todos los miembros del grupo. Los equipos que son miembros del grupo se mencionan en el panel derecho. Haga clic en el ícono del engranaje , ubicado junto al nombre del grupo, para ver las acciones de grupo y los detalles del grupo disponibles.



Existen dos tipos de grupos: grupos estáticos y dinámicos.

Grupos estáticos

- Los Grupos estáticos son grupos de equipos de clientes seleccionados y otros objetos.
- Todos los dispositivos móviles e informáticos se encuentran en un grupo estático.
- Puede seleccionar manualmente qué puntos de conexión pertenecen a un grupo estático.
- Un objeto puede pertenecer a un solo Grupo estático.
- Los grupos estáticos juegan un papel importante en el [modelo de seguridad de ESET PROTECT](#).

Grupos dinámicos

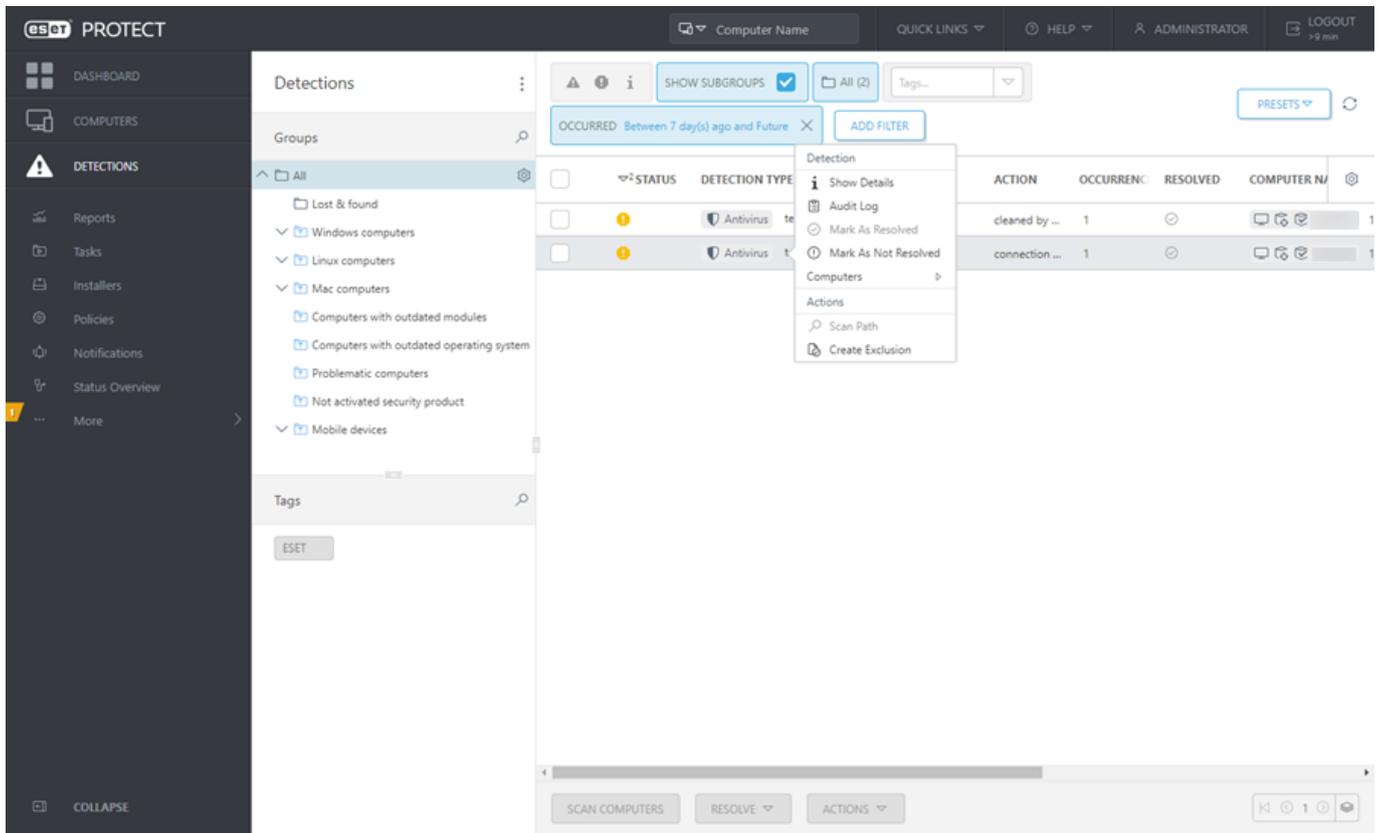
- Puede comprender los grupos dinámicos como filtros personalizados en los que se pueden definir reglas para filtrar los equipos según corresponda.
- Los grupos dinámicos se basan en plantillas y automáticamente incluyen puntos de conexión que cumplen con los requisitos establecidos en la plantilla.
- Si el dispositivo cliente no cumple los criterios, se quita automáticamente del grupo dinámico.
- Un equipo puede estar en varios grupos dinámicos al mismo tiempo o no estar en ninguno de ellos.

Hay artículos de la base de conocimiento disponibles que lo ayudarán a [agregar equipos a grupos estáticos](#), [crear nuevas plantillas de grupos dinámicos](#) y [asignar una política a un grupo](#).

Puede encontrar información adicional sobre los grupos en [Grupos](#).

Detecciones

Para acceder a los informes de detección, haga clic en **Detecciones** en el menú de la consola web a la izquierda. El panel **Detecciones** le ofrece una visión general de todas las detecciones encontradas en los equipos de su red.



Puede explorar los grupos y ver las detecciones en los miembros de un grupo determinado. La vista puede filtrarse, pero de forma predeterminada se muestran todos los tipos de detecciones de los últimos siete días. Las detecciones se pueden **Marcar como resueltas** en la sección **Detecciones** o debajo de los detalles de un cliente específico.

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

Puede encontrar las detecciones en cuarentena en **Más > Cuarentena**.

Exclusión

Puede excluir el(los) elemento(s) seleccionado(s) para evitar que se los **detecte** en el futuro. Haga clic en una detección y seleccione **Crear exclusión**. Puede excluir únicamente las detecciones del **Antivirus** y del **Firewall - Reglas IDS**. Puede crear una exclusión y aplicarla a más equipos y grupos.

⚠ Utilice las exclusiones con precaución. Pueden dar lugar a un equipo infectado.

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

Detecciones en archivos

Si se encuentran una o más detecciones en un archivo, el archivo y la detección dentro de este se informan en **Detecciones**.

 Al excluir un archivo que contiene una detección no se excluye la detección. Debe excluir las detecciones individuales dentro del archivo. El tamaño máximo de archivo de los archivos contenidos en archivos es 3 GB.

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

Protección Anti-Ransomware

Los productos para negocios de ESET (versión 7 y posterior) incluyen **Protección Anti-Ransomware**. Esta nueva característica de seguridad forma parte de HIPS y protege a los ordenadores de ransomware. Cuando se detecta ransomware en el equipo del cliente, puede ver los detalles de la detección en la consola web de ESET PROTECT en la sección **Detecciones**. Para filtrar solo detecciones de ransomware, haga clic en **Agregar filtro > Escáner > Explorador antiransomware**. Para obtener más información acerca de la Protección contra Ransomware, consulte el [glosario de ESET](#).

Puede configurar de forma remota la **Protección Anti-Ransomware** desde la consola web ESET PROTECT con la configuración de la **Política** para su producto comercial de ESET:

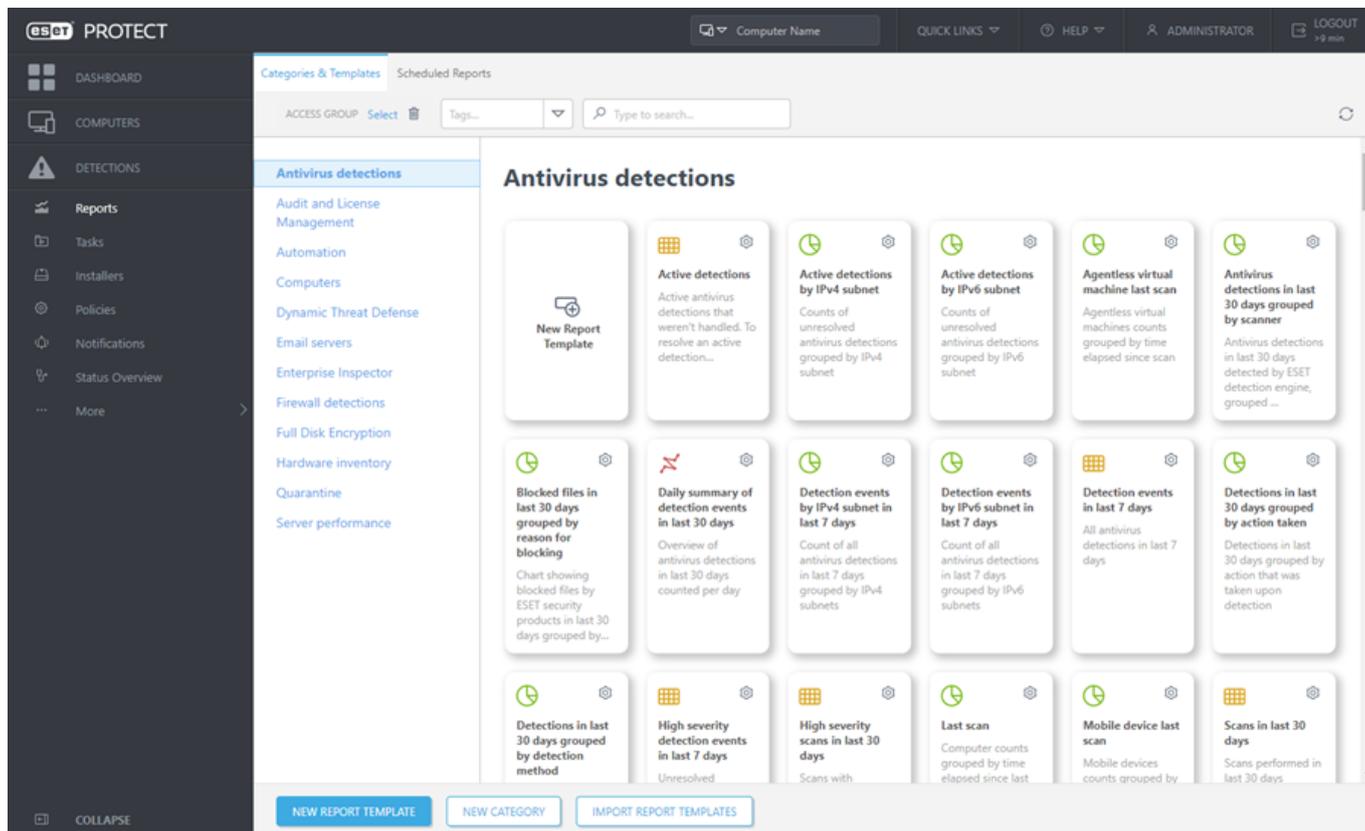
- **Habilitar la Protección contra Ransomware:** el producto comercial de ESET bloquea de manera automática todas las aplicaciones sospechosas que se comportan como ransomware.
- **Habilitar el modo de auditoría:** cuando habilita el modo de auditoría, las detecciones que identifica la Protección contra Ransomware se informan en la consola web de ESET PROTECT, pero el producto de seguridad de ESET no las bloquea. El administrador puede decidir bloquear la detección informada o excluirla al seleccionar [Crear exclusión](#). La configuración de esta Política está disponible solo mediante la Consola web ESET PROTECT.

 De forma predeterminada, la Protección Anti-Ransomware bloquea todas las aplicaciones que tienen un posible comportamiento de ransomware, incluso las aplicaciones legítimas. Le recomendamos **Habilitar el modo de auditoría** durante un período corto en un equipo administrado nuevo, de modo que pueda excluir aplicaciones legítimas que se detectan como ransomware según su comportamiento (falsos positivos). No recomendamos que use el modo de auditoría de forma permanente, ya que el ransomware en los equipos administrados no se bloquea automáticamente cuando el modo de auditoría está habilitado.

Informes

Los informes le permiten acceder a los datos y filtrarlos desde la base de datos en forma conveniente. Los informes tienen categorías y cada categoría incluye una breve descripción.

Para acceder a los informes, haga clic en **Informes** en el menú de la consola web a la izquierda, seleccione la plantilla de informes deseada (un mosaico con descripción y acción) sobre la cual desea ver el informe y haga clic en  (ícono de engranaje) > **Generar ahora**.



i De forma predeterminada, solo el administrador puede acceder a todas las plantillas de informes. Los demás [usuarios](#) no pueden ver ni usar estas plantillas salvo que se les haya asignado un permiso adecuado (o que las plantillas se encuentren en otra ubicación).

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

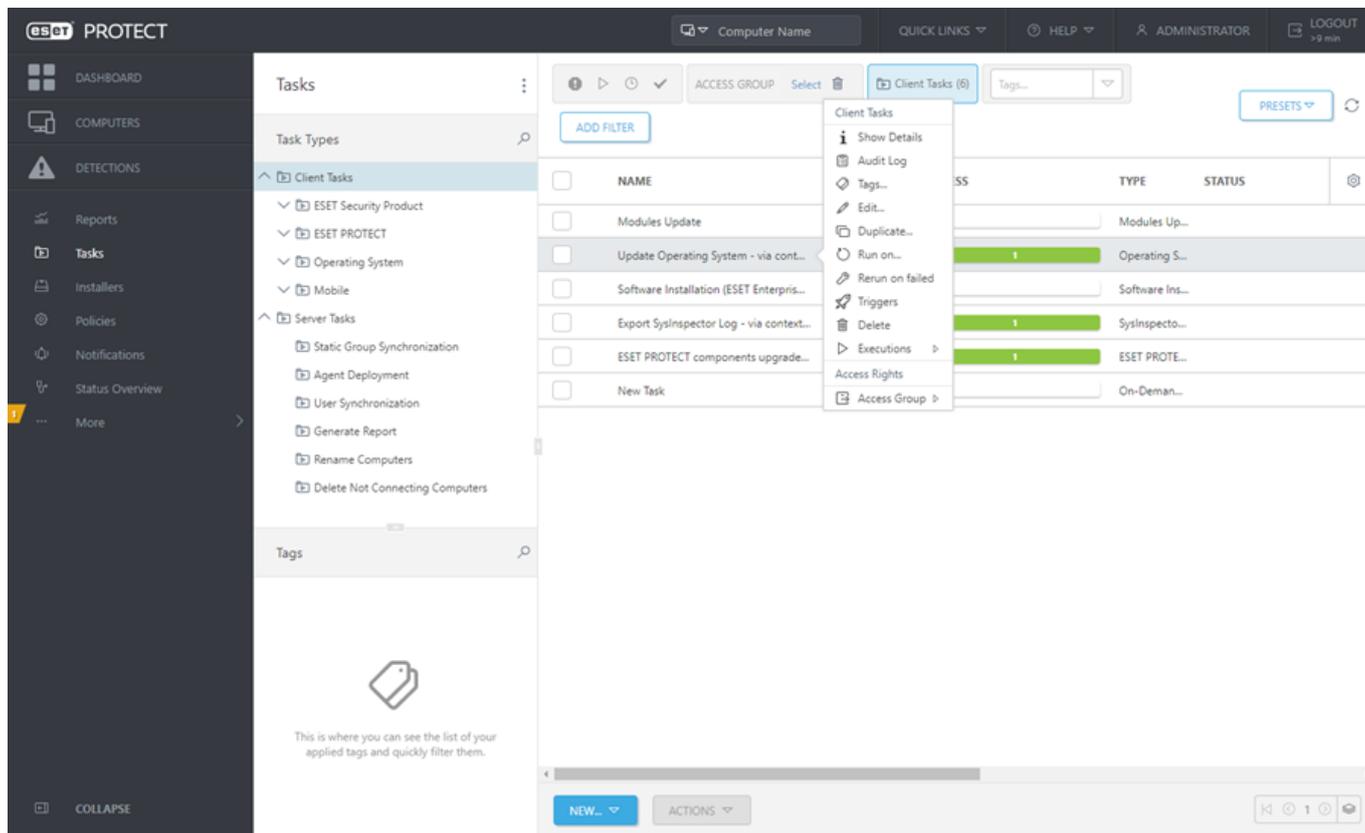
Consulte el [artículo de la base de conocimiento](#) de ESET para obtener instrucciones paso a paso sobre cómo configurar los informes automatizados en ESET PROTECT.

Tareas

Puede usar tareas para administrar el servidor ESET PROTECT, los equipos cliente y sus productos ESET. Las Tareas pueden automatizar trabajos de rutina. Los destinos de la tarea pueden ser [equipos](#) y [grupos](#) individuales.

Las tareas le permiten asignar procedimientos específicos a clientes individuales o grupos de clientes.

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



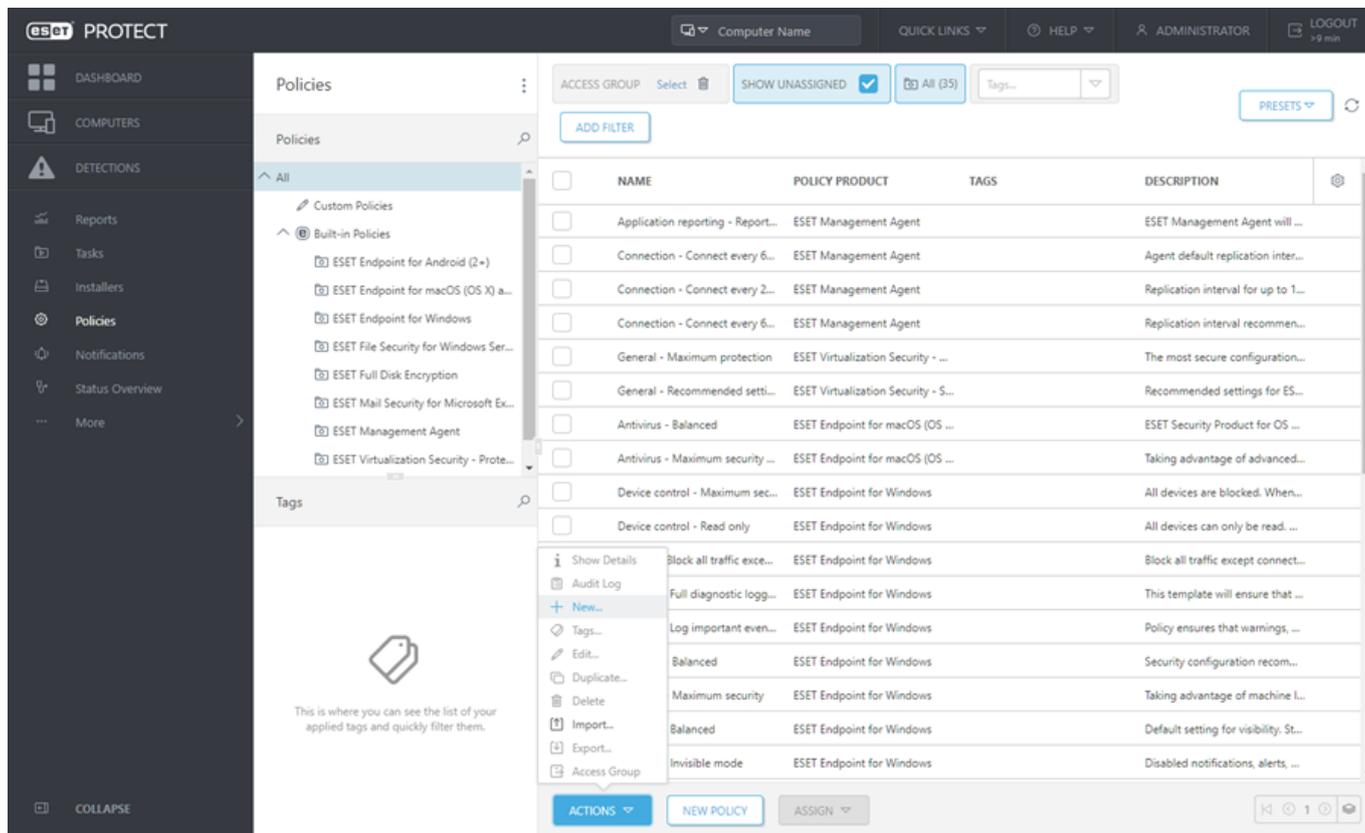
La sección [Tareas](#) de la Guía del administrador de ESET PROTECT contiene información sobre cómo crear, asignar y programar tareas nuevas.

En la base de conocimiento de ESET, encontrará ejemplos de procedimientos para configurar tareas específicas, tales como:

- [Enviar una llamada de activación a los equipos cliente para ejecutar una tarea inmediatamente en ESET PROTECT.](#)
- [Cambiar el intervalo de conexión del agente para los equipos cliente en ESET PROTECT.](#)
- [Usar una tarea del cliente Instalación de software para instalar o actualizar productos de punto de conexión de ESET.](#)
- [Sincronizar ESET PROTECT con Active Directory.](#)

Políticas

Puede usar políticas para administrar los equipos cliente. Las políticas son conjuntos de reglas de configuración que usted puede aplicar a los productos ESET que se ejecutan en equipos cliente para evitar la configuración manual del producto ESET de cada cliente. Puede aplicar una política directamente a [equipos](#) y [grupos](#) individuales. Además, puede asignar políticas múltiples a un equipo o a un grupo.



Siga los pasos de nuestro [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 en que se acomodan los Grupos estáticos. Esta regla no es válida para los grupos dinámicos, ya que se aplican primero a los grupos dinámicos secundarios para poder aplicar políticas con mayor impacto en la parte superior del árbol del grupo y políticas más específicas para los subgrupos.

i ESET recomienda que asigne políticas más genéricas (por ejemplo, el servidor de actualización) a los grupos que se ubiquen en la parte superior del árbol de grupos. Debe asignar políticas más específicas (por ejemplo, configuración del control del dispositivo) en la parte inferior 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 específicos, como detecciones informadas, puntos de conexión desactualizados y más. Consulte la sección [Notificaciones](#) de la Guía del administrador de ESET PROTECT o nuestro [artículo de la base de conocimiento](#) si desea obtener más información sobre cómo configurar y administrar notificaciones.

NAME	TAGS	ENABLED	STATUS	NOTIFICATION DESCRIPTION	LAST M
<input type="checkbox"/> Malware outbreak alert (count per time criteria)		<input type="radio"/> Disabled		Notification is sent when count of antivirus detection events in d...	Administrator
<input type="checkbox"/> Network attack alert		<input checked="" type="radio"/> Enabled	✓	Notification is sent when count of firewall events in defined perio...	Administrator
<input type="checkbox"/> Computers report problems alert		<input type="radio"/> Disabled		Notification is sent when at least 5% of managed computers hav...	Administrator
<input type="checkbox"/> Outdated modules alert		<input checked="" type="radio"/> Enabled	✓	Notification is sent when at least 5% of managed computers hav...	Administrator
<input type="checkbox"/> Managed clients not connecting alert		<input type="radio"/> Disabled		Notification is sent when at least 5% of all managed clients have ...	Administrator
<input type="checkbox"/> Outdated ESET software alert		<input type="radio"/> Disabled		Notification is sent when outdated ESET software is detected on ...	Administrator
<input type="checkbox"/> Malicious file detected (trojan / worm / virus / application)		<input type="radio"/> Disabled		Notification is sent when a malicious file is detected (trojan / wor...	Administrator
<input type="checkbox"/> Notification has invalid configuration and will not be triggered		<input type="radio"/> Disabled		At least one of the enabled notifications became invalid and will ...	Administrator
<input type="checkbox"/> Outdated version of ESET Endpoint Antivirus detected		<input checked="" type="radio"/> Enabled	✓	Notification is sent every day when at least one outdated instanc...	Administrator
<input type="checkbox"/> At least one computer has not connected for more than 14 ...		<input type="radio"/> Disabled		Notification is sent, when at least one computer has not been co...	Administrator
<input type="checkbox"/> Potentially unsafe application detected		<input type="radio"/> Disabled		Notification is sent when a potentially unsafe application is detec...	Administrator
<input type="checkbox"/> At least one infected file that was not cleaned automatically ...		<input type="radio"/> Disabled		Executed computer scan has detected at least one infected file th...	Administrator
<input type="checkbox"/> Detection occurred in memory		<input type="radio"/> Disabled		Notification is sent, when a detection event is detected by advan...	Administrator
<input type="checkbox"/> Potentially unwanted application (PUA) detected		<input type="radio"/> Disabled		Notification is sent when PUA (potentially unwanted application) ...	Administrator
<input type="checkbox"/> High severity alert detected by HIPS occurred		<input type="radio"/> Disabled		Notification is sent when a high severity detection triggered by H...	Administrator
<input type="checkbox"/> Suspicious application detected		<input checked="" type="radio"/> Enabled	✓	Notification is sent when a suspicious application is detected in y...	Administrator
<input type="checkbox"/> Client task has invalid configuration and therefore will fail		<input type="radio"/> Disabled		At least one of the created client tasks has invalid configuration a...	Administrator
<input type="checkbox"/> New computer connected for the first time		<input type="radio"/> 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 informes y notificaciones por correo electrónico. Habilite **Usar servidor SMTP**, haga clic en **Más > Configuración del servidor > Configuración avanzada > Servidor SMTP** y especifique lo siguiente:

- **Host:** nombre de host o dirección de IP de su servidor SMTP.
- **Port:** SMTP usa el puerto 25 como predeterminado, pero lo puede cambiar si su servidor SMTP usa un puerto diferente.
- **Nombre de usuario:** si su servidor SMTP requiere autenticación, especifique el nombre de la cuenta del usuario SMTP (no incluya el dominio ya que no funcionará).
- **Contraseña:** contraseña asociada con la cuenta de usuario SMTP.
- **Tipo de seguridad de conexión:** especifique el tipo de conexión, el predeterminado es **No asegurado**, pero si su servidor SMTP admite conexiones seguras, elija TLS o STARTTLS. Si desea hacer que su conexión sea más segura, use una extensión STARTTLS o SSL/TLS, ya que emplea un puerto independiente para la comunicación cifrada.
- **Tipo de autenticación:** el valor predeterminado está configurado en **Sin autenticación**. Sin embargo, puede seleccionar el tipo de autenticación adecuado de la lista desplegable (por ejemplo, inicio de sesión, CRAM-MD5, CRAM-SHA1, SCRAM-SHA1, NTLM o Automático)
- **Dirección del remitente:** este campo especifica la dirección del remitente que se mostrará en el encabezado de los correos electrónicos de notificación (De:)
- **Servidor de prueba SMTP:** se usa para asegurarse de que la configuración de SMTP sea la correcta. Haga clic en **Enviar correo electrónico de prueba** para abrir una ventana emergente. Ingrese la dirección de correo

electrónico del destinatario y el mensaje de correo electrónico de prueba se enviará por el servidor SMTP a esta dirección. Compruebe el buzón de correo del destinatario para verificar que se entregó el correo electrónico de prueba.

Si tiene cuenta de Gmail, puede usar Gmail como servidor SMTP. Use las configuraciones a continuación:

Configuración	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 conexión	TLS o STARTTLS
Tipo de autenticación	Automatic
Dirección del remitente	<i>su dirección de Gmail</i>

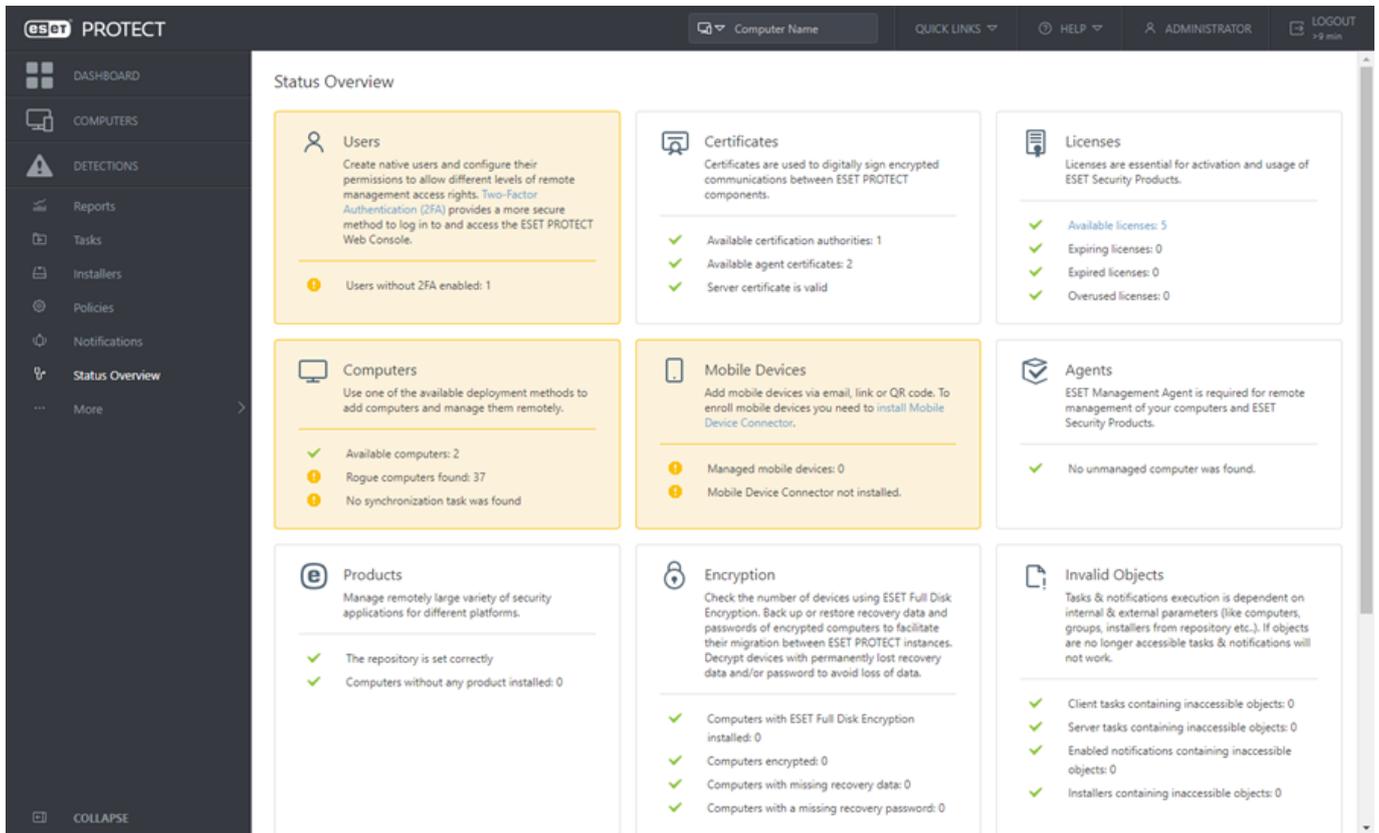
Si el envío de correos electrónicos falla, es posible que deba [permitir aplicaciones de menos seguridad](#) en su cuenta de Gmail o [desbloquear](#) su cuenta de Gmail.

Información general de estado

ESET PROTECT Server realiza verificaciones de diagnóstico periódicas.

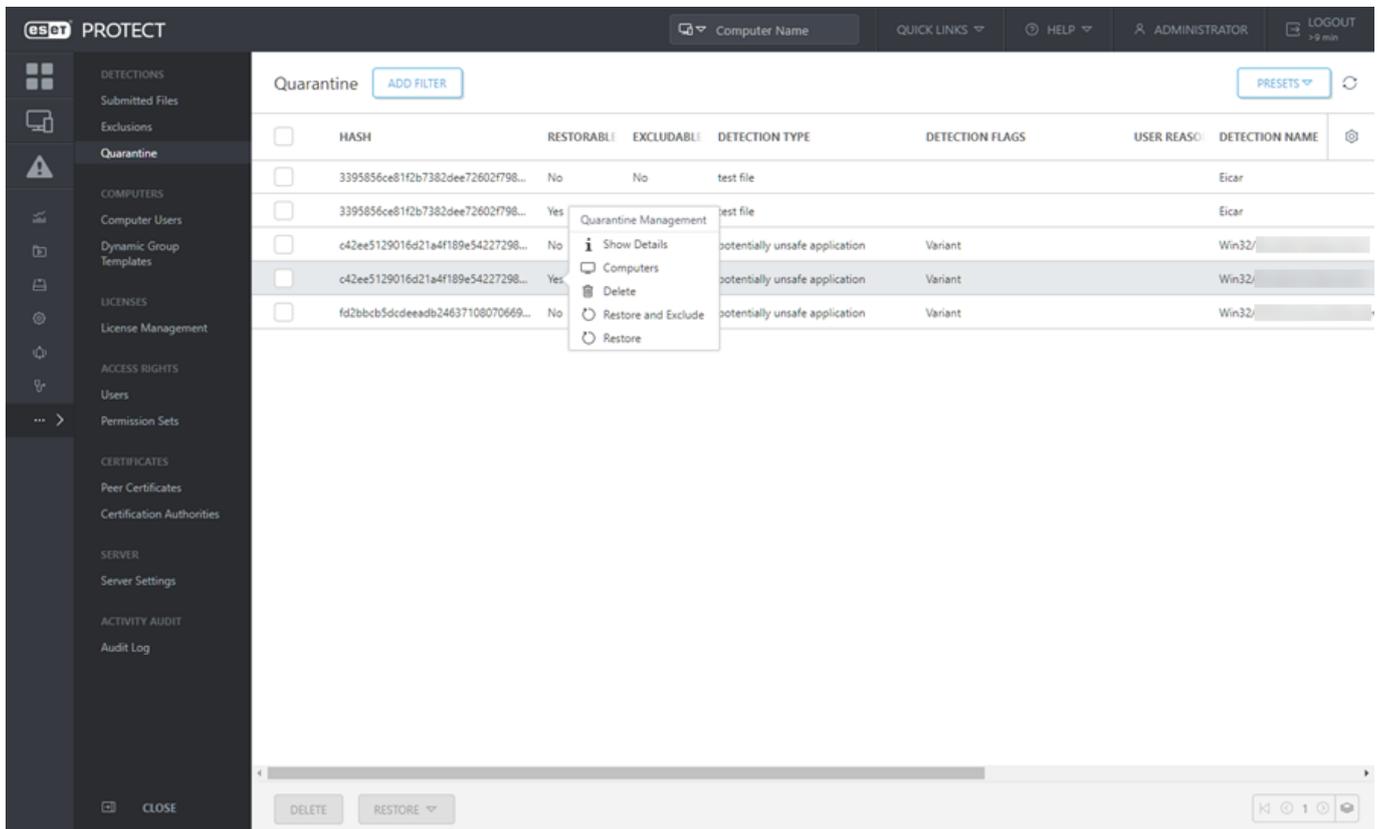
1.Haga clic en **Información general de estado** para ver la información de estado detallada de ESET PROTECT. Use la  **información general de estado** para ver las estadísticas de uso y el estado general de ESET PROTECT. También puede ayudarlo con la configuración inicial de ESET PROTECT.

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



Cuarentena

La sección Cuarentena se encuentra en la consola web en **Más > Cuarentena**. Esta sección muestra todos los archivos puestos en cuarentena en dispositivos del cliente.



Debe poner los archivos en cuarentena si no puede limpiarlos, si no es seguro ni aconsejable quitarlos o si un producto ESET los detecta en forma errónea.

No todas las detecciones encontradas en los dispositivos de los clientes se ponen en cuarentena. Las detecciones que no se ponen en cuarentena incluyen:

- Detecciones que no pueden eliminarse
- Detecciones que son sospechosas por su comportamiento, pero no se detectan 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 displays the ESET PROTECT web interface for License Management. The left sidebar includes navigation items: 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 last row showing 'ESET Security Manag'. A dropdown menu is open, showing options: Tags..., Add Licenses, Remove Licenses, Access Group (with a sub-menu containing Move), Synchronize Licenses, Open EBA, and Open EMA. At the bottom, there is an 'ACTIONS' button and a green status message: 'Synchronization successful (2020 Nov 30 14:00:41)'.

Para agregar una licencia nueva a ESET PROTECT:

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

2. Seleccione el método que desea usar para agregar sus licencias nuevas:

a. **ESET Business Account o ESET MSP Administrator:** sincronice las licencias desde su cuenta [ESET Business Account](#) o [ESET MSP Administrator](#) con la consola web de ESET PROTECT. Ahora puede importar la estructura completa de su ESET Business Account, incluida la distribución de puestos de licencias entre [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 es compatible con la gestión de licencias de suscripción. Puede agregar una licencia con ESET Business Account, ESET MSP Administrator o una clave de licencia. Puede verificar la validez de su suscripción en **Gestión de licencias** en la columna **Validez** o al hacer clic en **Equipos** > [Mostrar detalles](#).

Usuarios y conjuntos de permisos

ESET PROTECT modelo de seguridad

Estos son los términos clave que se usan en el modelo de seguridad:

Término	Explicación
Grupo de pertenencia	El grupo de pertenencia es donde se almacenan automáticamente todos los objetos (dispositivos, tareas, plantillas, entre otros) que crea un usuario. Cada usuario debe contar con solo con un grupo hogar.
Objeto	Cada objeto (equipo, tarea, política, informe o notificación) está en un grupo estático . El acceso a los objetos se realiza por grupos, no usuarios (al proporcionar acceso por grupo, es más fácil acomodar varios usuarios, por ejemplo, si 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 los derechos de acceso.
Administrador	Un administrador es un usuario con el grupo de pertenencia Todo y un conjunto completo de permisos sobre el grupo.
Derecho de acceso	El derecho de acceder a un objeto o de ejecutar una tarea se asigna con un conjunto de permisos.
Conjunto de permisos	Un conjunto de permisos representa los permisos para usuarios que acceden a la consola web de ESET PROTECT. Un conjunto de permisos define lo que un usuario puede ver o hacer en la consola web de ESET PROTECT. Se le puede asignar diferentes conjuntos de permisos a un mismo usuario. Los conjuntos de permisos solo se aplican a objetos de grupos estáticos definidos.
Funcionalidad	Una funcionalidad es un tipo de objeto o acción. Normalmente, la funcionalidad obtiene estos valores: Lectura , Escritura o Uso . La combinación de funcionalidades aplicadas a un grupo de acceso se denomina conjunto de permisos.

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

Crear un nuevo usuario de la consola web de ESET PROTECT

Una [configuración de ESET PROTECT nueva](#) tiene inicialmente un **administrador** predeterminado (un usuario con el grupo de pertenencia **Todo** y acceso a todo) como único usuario.

 ESET no recomienda usar la cuenta de usuario administrador predeterminada. Debe [crear otra cuenta de administrador](#). Además, puede crear usuarios adicionales con derechos de acceso más estrechos basados en sus competencias deseadas.

Certificados

Certificados

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

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

Autoridades de certificación

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



Todos los certificados de pares deben ser válidos y estar firmados por la misma autoridad de certificación para asegurarse de que todos los componentes se puedan comunicar correctamente.

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

Ayuda y soporte

ESET trabaja continuamente para actualizar y mejorar los productos de terminales ESET y ESET PROTECT.

o La [base de conocimiento de ESET](#) es un repositorio de artículos de soporte que permite hacer búsquedas, diseñada para ayudarlo a resolver problemas y responder preguntas.

o El [foro de usuarios de ESET](#) está controlado por personal de ESET y permite que los usuarios de ESET compartan problemas que tienen y encuentren soluciones.

o El [canal de videos de la base de conocimiento de ESET](#) incluye recorridos en video por procedimientos comunes de productos ESET.

o Visite [noticias de soporte de ESET](#) y asesoramiento al cliente para consultar los anuncios más recientes sobre actualizaciones y características de los productos ESET.

o Puede [abrir un caso con atención al cliente de ESET](#) en cualquier momento si no puede resolver un problema o encontrar la respuesta a una pregunta.

También puede consultar la [Guía de instalación](#) de ESET PROTECT (que incluye actualización, migración y resolución de problemas), la [Guía del administrador](#) (cómo administrar ESET PROTECT con la consola web de ESET PROTECT) y la [Guía del aparato virtual](#) (ESET PROTECT en un hipervisor) para obtener información más detallada.

Acuerdo de licencia de usuario final

Vigente a partir del 19 de octubre de 2021.

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

Acuerdo de Licencia de Usuario Final

Los términos de este Acuerdo de licencia para el usuario final ("Acuerdo") ejecutado por y entre ESET, spol. s r. o., con domicilio social en Einsteinova 24, 85101 Bratislava, Slovak Republic, registrado en el Registro Mercantil

administrado por el tribunal de distrito de Bratislava I, sección Sro, n.º de entrada 3586/B, número de registro de negocio: 31333532 ("ESET" o el "Proveedor") y usted, una persona física o jurídica ("Usted" o el "Usuario final"), tienen derecho a usar el Software definido en el Artículo 1 de este Acuerdo. El Software definido en este artículo puede almacenarse en un soporte digital, enviarse mediante correo electrónico, descargarse de Internet, descargarse de servidores del Proveedor u obtenerse de otras fuentes bajo los términos y condiciones mencionados más adelante.

ESTO ES UN ACUERDO SOBRE LOS DERECHOS DEL USUARIO FINAL; NO UN CONTRATO DE COMPRA PARA ARGENTINA. El Proveedor sigue siendo el propietario de la copia del Software y del soporte físico en el que el Software se suministra en paquete comercial, así como de todas las demás copias a las que el Usuario final está autorizado a hacer en virtud de este Acuerdo.

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

USTED ACEPTA QUE LA UTILIZACIÓN DEL SOFTWARE INDICA QUE HA LEÍDO ESTE ACUERDO, QUE LO COMPRENDE Y QUE CONSIENTE OBLIGARSE POR SUS TÉRMINOS Y CONDICIONES.

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

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

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

a) **Instalación y uso.** Usted tendrá el derecho no exclusivo y no transferible de instalar el Software en el disco rígido de un equipo o soporte similar para un almacenamiento permanente de datos, instalar y almacenar el

Software en la memoria de un sistema informático e implementar, almacenar y mostrar el Software.

b) Disposición sobre la cantidad de licencias. El derecho a utilizar el Software estará sujeto a la cantidad de Usuarios finales. Un "Usuario final" se refiere a lo siguiente: (i) instalación del Software en un sistema informático, o (ii) si el alcance de una licencia está vinculado a la cantidad de buzones de correo, un Usuario final se referirá a un usuario informático que acepta correo electrónico a través de un Agente de usuario de correo ("AUC"). Si un AUC acepta el correo electrónico y lo distribuye posteriormente en forma automática a varios usuarios, la cantidad de Usuarios finales se determinará conforme a la cantidad real de usuarios para los que se distribuyó el correo electrónico. Si un servidor de correo cumple la función de una pasarela de correo, la cantidad de Usuarios finales será equivalente a la cantidad de usuarios de servidores de correo a los que dicha pasarela presta servicios. Si se envía una cantidad no especificada de direcciones de correo electrónico (por ejemplo, con alias) a un usuario y el usuario las acepta, y el cliente no distribuye automáticamente los mensajes a más usuarios, se requiere la Licencia únicamente para un equipo. No debe usar la misma Licencia en más de un equipo al mismo tiempo. El Usuario final solo tiene derecho a introducir la Clave de licencia en el Software en la medida en que el Usuario final tenga derecho a usar el Software de acuerdo con la limitación derivada del número de Licencias otorgadas por el Proveedor. Se considera que la clave de Licencia es confidencial. No puede compartirla con terceros ni puede permitirles que la utilicen a menos que el presente Acuerdo o el Proveedor indique lo contrario. Si su clave de Licencia se encuentra en riesgo notifique al Proveedor de inmediato.

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

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

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

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

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

4. Funciones con recopilación de información y requisitos para la conexión a Internet. Para que funcione de manera correcta, el Software requiere conexión a Internet y debe conectarse a intervalos regulares a los servidores del Proveedor o de terceros y debe recopilar información en conformidad con la Política de Privacidad. La conexión a Internet y la recopilación de datos son necesarias para el funcionamiento y la actualización del Software. El Proveedor podrá publicar actualizaciones o actualizar el Software ("Actualizaciones"), aunque no está obligado a proporcionarlas. Esta función se activa en la sección de configuración estándar del Software y las Actualizaciones se instalan automáticamente, a menos que el Usuario final haya desactivado la instalación automática de Actualizaciones. Para aprovisionar Actualizaciones, es necesario verificar la autenticidad de la Licencia, lo que incluye información sobre el equipo o la plataforma en los que está instalado el Software, de acuerdo con la Política de Privacidad.

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

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

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

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

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

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

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

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

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

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

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

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

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

7. Copyright. El Software y todos los derechos, incluyendo, pero sin limitarse a, los derechos de propiedad y los derechos de propiedad intelectual, son propiedad de ESET y/o sus licenciatarios. Están protegidos por las disposiciones de tratados internacionales y por todas las demás leyes nacionales aplicables del país en el que se utiliza el Software. La estructura, la organización y el código del Software son valiosos secretos comerciales e información confidencial de ESET y/o sus licenciatarios. No puede copiar el Software, a excepción de lo especificado en el artículo 6 (a). Todas las copias que este Acuerdo le permita hacer deberán incluir el mismo copyright y los demás avisos legales de propiedad que aparezcan en el Software. Si aplica técnicas de ingeniería inversa, descompila o desmonta el Software, o intenta obtener el código fuente del Software de alguna otra forma, en incumplimiento de las disposiciones de este Acuerdo, por este medio Usted acepta que toda la información obtenida de ese modo se considerará automática e irrevocablemente transferida al Proveedor o poseída por el Proveedor de forma completa desde el momento de su origen, más allá de los derechos del Proveedor en relación con el incumplimiento de este Acuerdo.

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

9. Versiones en varios idiomas, software en medios duales, varias copias. En caso de que el Software sea compatible con varias plataformas o idiomas, o si Usted obtuvo varias copias del Software, solo puede usar el Software para la cantidad de sistemas informáticos y para las versiones correspondientes a la Licencia adquirida. No puede vender, arrendar, alquilar, sublicenciar, prestar o transferir ninguna versión o copias del Software no utilizado por Usted.

10. Comienzo y rescisión del Acuerdo. Este Acuerdo es efectivo desde la fecha en que Usted acepta los términos de la Licencia. Puede poner fin a este Acuerdo en cualquier momento. Para ello, desinstale, destruya o devuelva permanentemente y por cuenta propia el Software, todas las copias de seguridad, y todos los materiales relacionados suministrados por el Proveedor o sus socios comerciales. Su derecho a usar el Software y cualquiera de sus funciones puede estar sujeto a la Política EOL. Cuando el Software o cualquiera de sus funciones lleguen a la fecha de fin de su vida útil definida en la Política EOL, se terminará su derecho a usar el Software. Más allá de la forma de rescisión de este Acuerdo, las disposiciones de los artículos 7, 8, 11, 13, 19 y 21 seguirán siendo aplicables por tiempo ilimitado.

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

12. Sin más obligaciones. Este Acuerdo no crea obligaciones del lado del Proveedor y sus licenciatarios, excepto

las obligaciones específicamente indicadas en este Acuerdo.

13. LIMITACIÓN DE RESPONSABILIDAD. EN LA MEDIDA EN QUE LO PERMITA LA LEGISLACIÓN APLICABLE, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O LICENCIADORES SERÁN RESPONSABLES DE PÉRDIDAS DE INGRESOS, GANANCIAS, VENTAS, DATOS O COSTOS DE ADQUISICIÓN DE BIENES O SERVICIOS SUSTITUIDOS, DAÑOS A LA PROPIEDAD, DAÑOS PERSONALES, INTERRUPCIÓN DEL NEGOCIO, PÉRDIDA DE INFORMACIÓN COMERCIAL O DE CUALQUIER VALOR ESPECIAL, DIRECTO, INSONDADO, ACCIDENTAL, ECONÓMICO, DE COBERTURA, DAÑOS PUNITIVOS, ESPECIALES O CONSECUENCIALES, QUE SIN EMBARGO DERIVEN O SURJAN POR CONTRATO, AGRAVIOS, NEGLIGENCIA U OTRA TEORÍA DE RESPONSABILIDAD QUE DERIVE DE LA INSTALACIÓN, EL USO O LA INCAPACIDAD DE USAR EL SOFTWARE, AUNQUE EL PROVEEDOR, SUS LICENCIADORES O FILIALES RECIBAN INFORMACIÓN DE LA POSIBILIDAD DE DICHOS DAÑOS. DADO QUE DETERMINADOS PAÍSES Y JURISDICIONES NO PERMITEN LA EXCLUSIÓN DE RESPONSABILIDAD, PERO PUEDEN PERMITIR LA LIMITACIÓN DE RESPONSABILIDAD, EN DICHOS CASOS, LA RESPONSABILIDAD DEL PROVEEDOR, SUS EMPLEADOS, LICENCIATARIOS O AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR LA LICENCIA.

14. Nada de lo contenido en este Acuerdo perjudicará los derechos estatutarios de ninguna parte que actúe en calidad de consumidor si infringe dicho Acuerdo.

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

16. Transferencia de la Licencia. El Software puede transferirse de un sistema informático a otro, a menos que esta acción infrinja los términos del presente Acuerdo. Si no infringe los términos del Acuerdo, el Usuario final solamente tendrá derecho a transferir en forma permanente la Licencia y todos los derechos derivados de este Acuerdo a otro Usuario final con el consentimiento del Proveedor, sujeto a las siguientes condiciones: (i) que el Usuario final original no se quede con ninguna copia del Software; (ii) que la transferencia de los derechos sea directa, es decir, del Usuario final original al nuevo Usuario final; (iii) que el nuevo Usuario final asuma todos los derechos y obligaciones pertinentes al Usuario final original bajo los términos de este Acuerdo; (iv) que el Usuario final original le proporcione al nuevo Usuario final la Documentación que habilita la verificación de la autenticidad del Software, como se especifica en el artículo 17.

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

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

19. Cumplimiento del control comercial.

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

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

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

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

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

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

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

c) Ninguna de las estipulaciones del Acuerdo tiene por objeto inducir o exigir, ni debe interpretarse como una intención de inducir o exigir a ninguna de las partes actuar o abstenerse de actuar (o acordar actuar o abstenerse de actuar) de ninguna manera que resulte inconsistente con las Leyes de Control Comercial aplicables, o se encuentre penalizada o prohibida por estas.

20. Avisos. Todos los avisos y devoluciones de software o documentación deben entregarse a: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, sin perjuicio del derecho de ESET a comunicarle cualquier cambio de este Acuerdo, las Políticas de privacidad, la Política de EOL y la Documentación de acuerdo con el artículo. 22 del Acuerdo. ESET puede enviarle correos electrónicos, notificaciones en la aplicación a través del Software o publicar la comunicación en nuestro sitio web. Acepta recibir comunicaciones legales de ESET de forma electrónica, lo que incluye comunicaciones sobre cambios de Términos, Términos especiales o Políticas de privacidad, cualquier contrato de trabajo o aceptación o invitación a tratar, avisos u otras comunicaciones legales. Dicha comunicación electrónica se considerará recibida por escrito, a menos que la legislación aplicable requiera específicamente una forma de comunicación diferente.

21. Legislación aplicable. Este Acuerdo se registrará e interpretará conforme a la legislación de la República Eslovaca. En el presente Acuerdo, el Usuario final y el Proveedor aceptan que los principios del conflicto de leyes y la Convención de las Naciones Unidas sobre los Contratos de Venta Internacional de Bienes no serán aplicables. Acepta expresamente que cualquier disputa o demanda derivada del presente Acuerdo con respecto al Proveedor o relativa al uso del Software deberá resolverse por el Tribunal del Distrito de Bratislava I., Eslovaquia; asimismo,

Usted acepta expresamente el ejercicio de la jurisdicción del Tribunal mencionado.

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

ESET se reserva el derecho de realizar cambios en el Software, así como de revisar los términos de este Acuerdo, sus Anexos, la Política de privacidad, la Política y la Documentación de EOL o cualquier parte de ellos, en cualquier momento mediante la actualización del documento pertinente (i) para reflejar cambios del Software o el comportamiento comercial de ESET, (ii) por cuestiones legales, normativas o de seguridad; o (iii) para evitar abusos o daños. Se le notificará cualquier revisión del Acuerdo por correo electrónico, notificación en la aplicación o por otros medios electrónicos. Si no está de acuerdo con los cambios de texto del Acuerdo, puede rescindir el acuerdo con el Artículo 10 en el plazo de 30 días después de recibir un aviso del cambio. A menos que rescinda el Acuerdo dentro de este límite de tiempo, los cambios de texto se considerarán aceptados y estarán vigentes para Usted a partir de la fecha en que reciba un aviso del cambio.

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

ANEXO AL ACUERDO

Reenvío de información al proveedor. Se aplican disposiciones adicionales al reenvío de información al proveedor como se muestra a continuación:

El Software contiene funciones que reúnen datos sobre el proceso de instalación, el equipo o la plataforma en el que se instala el Software, o la información sobre las operaciones y la funcionalidad del Software y sobre equipos administrados (en adelante, referida como «Información») y luego los envía al Proveedor. Esta información contiene datos relacionados con dispositivos administrados (que incluyen información personal obtenida al azar o por accidente). Si se activa esta función del Software, el Proveedor podrá recopilar y procesar la información tal como se especifica en la Política de Privacidad y de conformidad con las normas legales vigentes.

El Software requiere que se instale un componente en el equipo administrado, lo que permite la transferencia de información entre un equipo administrado y un software de administración remota. La información, que está sujeta a la transferencia, contiene datos de administración tal como información sobre el Hardware y el Software de un ordenador administrado así como sobre las instrucciones de administración provenientes de un Software de administración remota. Cualquier otro tipo de datos que transfiera el equipo administrado debe estar determinado por la configuración del Software instalado en ese equipo. Las instrucciones del Software de administración deben estar determinadas por 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, inscrita en el Registro comercial del Tribunal de distrito de Bratislava I, Sección Sro, Registro No 3586/B, Número de registro de empresa: 31333532 como Controlador de datos (“ESET” o “Nosotros”) desea ser transparente con el procesamiento de datos personales y la privacidad de nuestros clientes. A fin de cumplir con el objetivo, publicamos la presente Política de privacidad con el único propósito de informar a nuestros clientes (“Usuario final” o “Usted”) acerca de los siguientes temas:

- Procesamiento de datos personales,
- Confidencialidad de datos,
- Datos de la persona registrada.

Procesamiento de datos personales

Los servicios prestados por ESET implementados en nuestro producto se prestan de acuerdo con los términos del Acuerdo de licencia de usuario final (“EULA”), pero algunos pueden requerir atención especial. Quisiéramos brindarle más detalles sobre la recolección de datos relacionada a la provisión de nuestros servicios. Prestamos distintos servicios descritos en el EULA y la documentación del producto, como el servicio de actualización, ESET LiveGrid®, la protección contra el mal uso de los datos, la asistencia, etc. Para hacer que todo funcione, necesitamos recolectar la siguiente información:

- La administración de productos de seguridad ESET requiere y almacena localmente información como ID y nombre de puesto, nombre de producto, información de licencia, información de activación y expiración, información de hardware y software en relación al equipo administrado con el producto ESET Security instalado. Los registros relacionados con actividades de dispositivos y productos de ESET Security administrados se recolectan y están disponibles para facilitar las funciones y servicios de administración y supervisión sin envío automatizado a ESET.
- Información relacionada con el proceso de instalación, incluida la plataforma en la que se instala nuestro producto e información acerca de las operaciones y la funcionalidad de nuestros productos, como la huella digital del hardware, la ID de instalación, el volcado de memoria, la ID de licencia, la dirección IP, la dirección MAC, los ajustes de configuración de productos que además pueden incluir dispositivos administrados.
- Para fines de facturación, verificación de autenticidad de la licencia y prestación de nuestros servicios, se requiere información de licencia como identificación de licencia y datos personales, como nombre, apellido, dirección y dirección de correo electrónico.
- Pueden ser necesarios datos de contacto y datos contenidos en sus solicitudes de soporte para el servicio técnico. Basados en el medio que Usted eligió para comunicarse con Nosotros, podemos recopilar su correo electrónico, número de teléfono, información de licencia, descripción y detalles de producto del caso de asistencia. Podemos solicitarle que proporcione información adicional para facilitar la prestación del servicio de soporte como archivos de registro o volcados generados.
- Los datos relacionados con el uso de nuestro servicio son completamente anónimos al finalizar la sesión. No se almacena ninguna información de identificación personal una vez que finaliza la sesión.

Confidencialidad de los datos

ESET es una compañía que opera globalmente a través de entidades o socios afiliados como parte de nuestra red de distribución, servicio y soporte. Los datos procesados por ESET pueden ser transferidos desde y hasta las entidades afiliadas o socios para ejecutar EULA, como por ejemplo la prestación de servicios o soporte o facturación. Según la ubicación y servicio que Usted decida utilizar, Nosotros podemos solicitarle que transfiera sus datos a un país sin una decisión adecuada de la Comisión Europea. Incluso en tal situación, cada transferencia de datos se encuentra sujeta a la regulación de la protección de datos y se realiza solo si es necesaria. Se deben establecer cláusulas contractuales estándar, normas corporativas vinculantes u otra forma de protección adecuada sin excepción.

Nosotros 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 la validez de su licencia para que tenga tiempo de renovarla de una forma sencilla y cómoda. Pueden continuar procesándose

estadísticas y otros datos minimizados y seudonimizados de ESET LiveGrid® con fines estadísticos.

ESET implementa medidas técnicas y de organización para asegurar un nivel de seguridad apropiado ante riesgos potenciales. Hacemos todo lo posible para garantizar una continua confiabilidad, integridad, disponibilidad y capacidad de recuperación de los sistemas operativos y servicios. Sin embargo, si ocurre una filtración de datos que resulta en un riesgo para sus derechos y libertades, Nosotros estamos preparados para notificar a la autoridad supervisora así como también a las personas registradas. Como persona registrada, Usted tiene el derecho de presentar una queja con una autoridad supervisora.

Derechos de la persona registrada

ESET se encuentra sujeto a la regulación de las leyes eslovacas y Nosotros cumplimos con la ley de protección de datos como parte de la Unión Europea. De conformidad con las condiciones establecidas por las leyes aplicables de protección de los datos, usted tiene los siguientes derechos como sujeto de datos:

- derecho a que ESET le solicite acceso a sus datos personales,
- derecho a rectificación de datos personales de ser erróneos (Usted también tiene el derecho a completar los datos personales que estén incompletos),
- derecho a solicitar la eliminación de sus datos personales,
- derecho a solicitar una restricción al procesamiento de sus datos personales
- derecho a oponerse al procesamiento
- derecho a presentar un reclamo así como
- derecho a la portabilidad de datos.

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

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