ESET PROTECT

Guía de instalación actualización y migración

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

Digital Security
Progress. Protected.

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

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

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

REV. 12/04/2024

Acerca de la ayuda

Esta guía de instalación se redactó para ayudar en el proceso de instalación y actualización de ESET PROTECT y contiene instrucciones para completar el proceso.

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

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

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

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

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

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

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

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

- La Base de conocimiento ESET contiene respuestas a las preguntas más frecuentes, así como soluciones recomendadas para distintos problemas. Esta Base de conocimiento la actualizan periódicamente los especialistas técnicos de ESET, y es la herramienta más potente para resolver diversos tipos de problema.

- El Foro de ESET ofrece a los usuarios de ESET una forma sencilla de obtener ayuda y de ayudar a otras personas. Puede publicar cualquier problema o pregunta que tenga con respecto a sus productos ESET.

Instalación, actualización o migración

ESET PROTECT es una aplicación que le permite gestionar los productos de ESET en estaciones de trabajo cliente, servidores y dispositivos móviles en un entorno de red desde una ubicación central. Con el sistema de administración de tareas integrado de ESET PROTECT, puede instalar soluciones de seguridad de ESET en ordenadores remotos y responder rápidamente a nuevos problemas y detecciones.

ESET PROTECT no ofrece protección frente a código malicioso por sí mismo. La protección de su entorno depende de la presencia de una solución de seguridad de ESET ESET Endpoint Security en estaciones de trabajo y dispositivos móviles o ESET Server Security para Windows en servidores.

ESET PROTECT se basa en dos principios fundamentales:

- **Gestión centralizada**: toda la red se puede configurar, administrar y monitorizar desde un solo lugar.
- **Escalabilidad**: el sistema puede implementarse en una red pequeña, así como en grandes entornos empresariales. ESET PROTECT se ha diseñado para adaptarse al crecimiento de su infraestructura.

ESET PROTECT es compatible con la nueva generación de productos de seguridad de ESET y también es compatible con la generación anterior de productos.

Las páginas de ayuda de ESET PROTECT incluyen una guía completa de instalación y actualización:

- Arquitectura de ESET PROTECT
- El proceso de instalación
- Procedimientos de actualización
- Procedimientos de migración
- Procedimientos de desinstalación
- Administración de licencias
- Procesos de implementación e Implementación del agente con GPO o SCCM
- Primeros pasos después de la instalación de ESET PROTECT
- Guía de administración

Nuevas funciones de ESET PROTECT 9.1

Recorrido por el producto

Hemos añadido un nuevo recorrido por el producto para que explore rápidamente nuestra solución y acelere el proceso de integración. Más información

Cambios en los nombres de productos

ESET Enterprise Inspector se ha renombrado como ESET Inspect y ESET Dynamic Threat Defense se ha renombrado como ESET LiveGuard Advanced. Puede encontrar más información en este artículo.

Reinicios mejorados

Con la versión más reciente de ESET Endpoint Security para Windows (9.1), hemos rediseñado los reinicios e introducido nuevas opciones. Ahora puede configurar los reinicios de forma que los usuarios finales puedan posponerlos. Más información

Implementación más sencilla

Hemos rediseñado el asistente de creación del instalador para que sea más intuitivo. En la tarea Instalación de software, ahora puede usar el parámetro especial "latest" (más reciente), que garantiza que el instalador creado instale siempre la versión más reciente del producto cuando se haya iniciado. Más información

Compatibilidad nativa de ARM para macOS

Con la versión más reciente de ESET Management Agent y ESET Endpoint Antivirus para macOS (v7), ofrecemos compatibilidad nativa de ARM. Más información

Compatibilidad con aplicaciones de autenticación de dos factores de terceros

Hemos agregado compatibilidad con aplicaciones de autenticación de dos factores de terceros que admiten el protocolo TOTP necesario, como Google Authenticator, Microsoft Authenticator y Authy. Más información

Filtros avanzados

Hemos presentado un nuevo concepto de filtrado de datos que le ayudará a filtrar fácilmente los dispositivos pertinentes en entornos de mayor tamaño, pero no solo ahí. Siempre tendrá una visión estadística del número de dispositivos con atributos específicos que tiene en su red y sabrá cuántos resultados obtendrá antes de hacer clic en el filtro. Ya puede probar las nuevas opciones de filtrado en la sección Ordenadores. Más información

Comunicación mejorada de las actualizaciones automáticas

Hemos añadido una nueva sección azul a Estado de la versión del componente en el panel Información general del estado para que pueda identificar fácilmente los equipos con actualizaciones automáticas activadas que están pendientes de instalación, pero que también se pueden instalar de forma manual de antemano. Más información

Lista de componentes obsoletos

ESET PROTECT ahora detecta componentes obsoletos, muestra una lista de componentes obsoletos al administrador de la consola y ofrece instrucciones sobre cómo actualizarlos. Más información

Control de acceso web para MDM

Hemos optado por devolver la funcionalidad de control de acceso web de CloudMDM a la variante local. El administrador puede limitar el acceso de los empleados a varias categorías de contenido o vínculos de Internet específicos.

Otras mejoras y cambios para facilitar el uso

Puede ver más detalles en el registro de cambios.

Arquitectura

ESET PROTECT es un sistema de administración remota de nueva generación.

Para realizar una implementación completa de los productos de seguridad de ESET instale los siguientes componentes (plataformas Windows y Linux):

- ESET PROTECT Server
- ESET PROTECT Web Console
- ESET Management Agent

Los siguientes componentes complementarios son opcionales, pero se recomienda su instalación para garantizar el máximo rendimiento de la aplicación en la red:

- Proxy
- RD Sensor
- Proxy HTTP Apache
- Conector del dispositivo móvil

Los componentes de ESET PROTECT utilizan certificados para comunicarse con ESET PROTECT Server. Obtenga más información sobre los certificados en ESET PROTECT en nuestro artículo de la base de conocimiento.

Información general sobre los elementos de la infraestructura

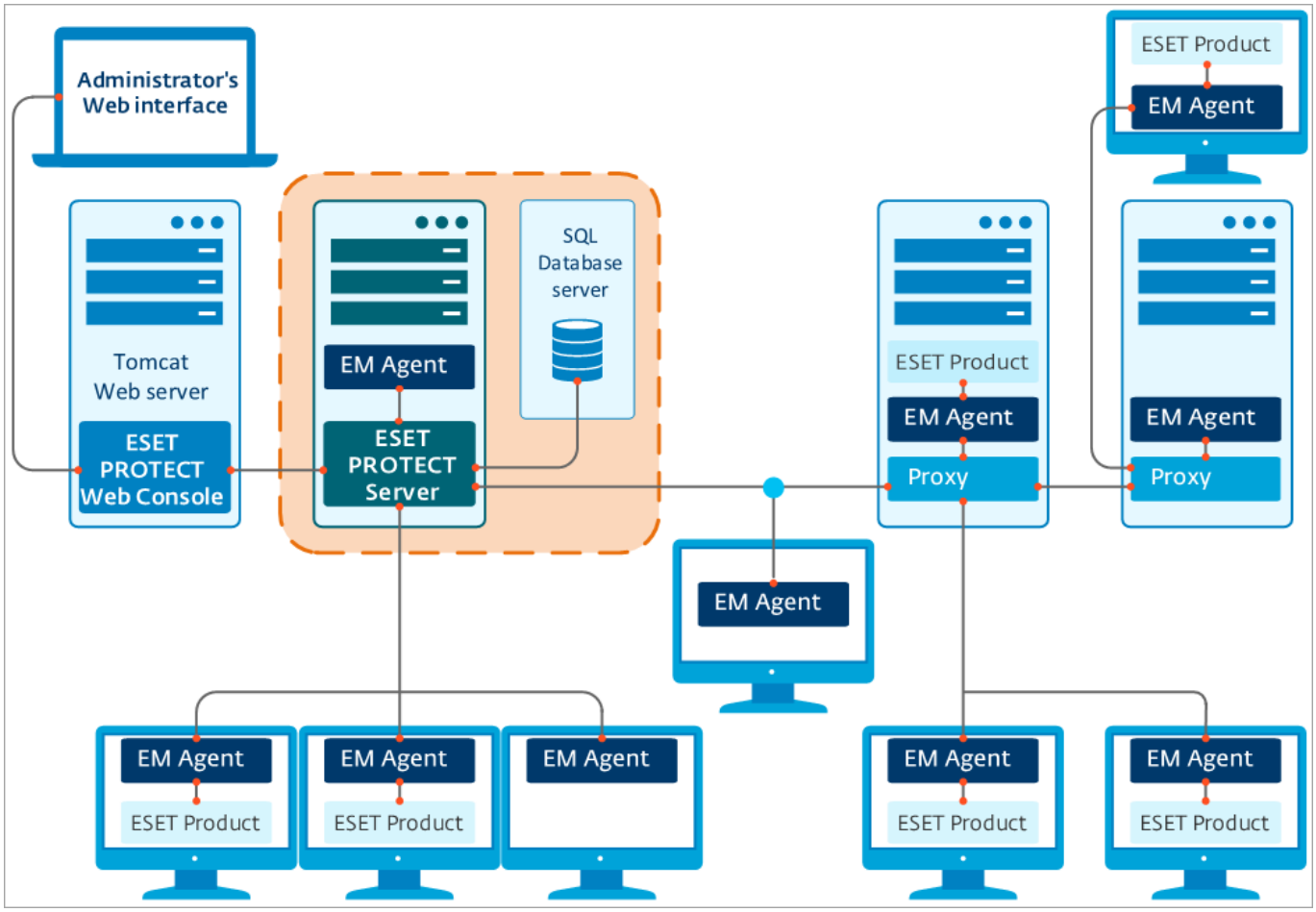
La siguiente tabla recoge información general sobre los elementos de la infraestructura de ESET PROTECT y sus funciones principales:

Funcionalidad	ESET PROTECT Server	ESET Management Agent	Producto de seguridad ESET	Proxy HTTP	Servidores de ESET	Conector del dispositivo móvil
Administración remota de productos de seguridad de ESET (creación de políticas, tareas, informes, etc.)	✔	X	X	X	X	X

Funcionalidad	ESET PROTECT Server	ESET Management Agent	Producto de seguridad ESET	Proxy HTTP	Servidores de ESET	Conector del dispositivo móvil
Comunicación con ESET PROTECT Server y administración del producto de seguridad de ESET en el dispositivo cliente	X	✔	X	X	X	✔
Suministro de actualizaciones, validación de licencias	X	X	X	X	✔	X
Almacenamiento en caché y reenvío de actualizaciones (motor de detección, instaladores, módulos)	X	X	✔	✔	X	X
Reenvío de tráfico de red entre ESET Management Agent y ESET PROTECT Server	X	X	X	✔	X	X
Protección del dispositivo cliente	X	X	✔	X	X	X
Administración remota de dispositivos móviles	X	X	X	X	X	✔

Servidor

ESET PROTECT Serveres la aplicación ejecutiva que procesa todos los datos recibidos de los clientes que se conectan al servidor (a través del ESET Management Agent o HTTP Proxy). Para procesar los datos correctamente, el servidor requiere una conexión estable a un servidor de base de datos donde se almacenan los datos. Le recomendamos que instale el servidor de base de datos en un ordenador diferente para lograr un mejor rendimiento.

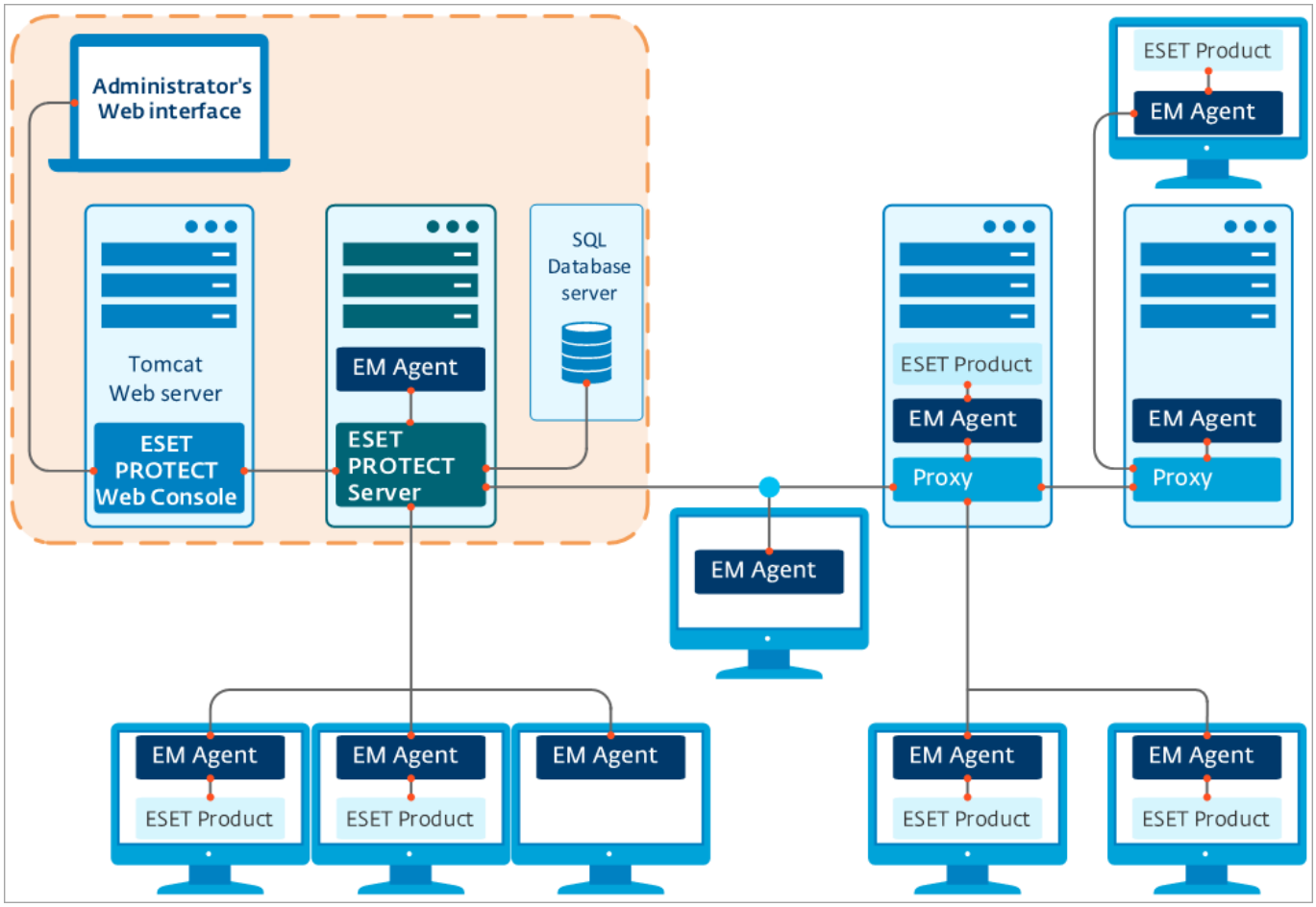


Web Console

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

Web Console utiliza Apache Tomcat como servidor web HTTP. Cuando se utiliza el Tomcat incluido en el dispositivo virtual o el instalador de ESET, solo permite conexiones TLS 1.2 y 1.3 con Web Console.

Puede seleccionar la instalación de ESET PROTECT Web Console en un ordenador distinto al ordenador donde se ha instalado ESET PROTECT Server.



Proxy HTTP

¿Qué es el proxy HTTP y qué utilidad ofrece?

El proxy HTTP reenvía la comunicación de los agentes a ESET PROTECT Server en entornos en los que las máquinas de los agentes no pueden establecer conexión con el servidor.

¿Cómo funciona el Proxy de ESET PROTECT?

ESET PROTECT9 utiliza una versión personalizada de Proxy HTTP Apache como componente proxy. Tras una configuración correcta, el proxy HTTP Apache se puede usar como proxy para los agentes de ESET Management. El proxy no almacena en caché ni abre la comunicación, solo la reenvía.

¿Puedo utilizar un proxy que no sea Proxy HTTP Apache?

Con ESET Management Agent se puede utilizar cualquier solución proxy que cumpla las siguientes condiciones:

- Puede reenviar comunicación SSL
- Es compatible con HTTP CONNECT
- No utiliza un nombre de usuario y una contraseña.

¿Qué diferencias presenta el nuevo protocolo de comunicación?

ESET PROTECT Server se comunica con las instancias de ESET Management Agent mediante el protocolo gRPC. La comunicación utiliza TLS y HTTP2, por lo que puede realizarse mediante servidores proxy. También hay nuevas funciones de recuperación automática y una conexión persistente que mejora el rendimiento global de las comunicaciones.

¿Qué efectos tiene esto en el rendimiento?

El uso del proxy HTTP no tiene consecuencias significativas en el rendimiento.

¿Cuándo debo utilizar el proxy?

Se recomienda utilizar un proxy si la infraestructura cumple una o más de las siguientes condiciones:

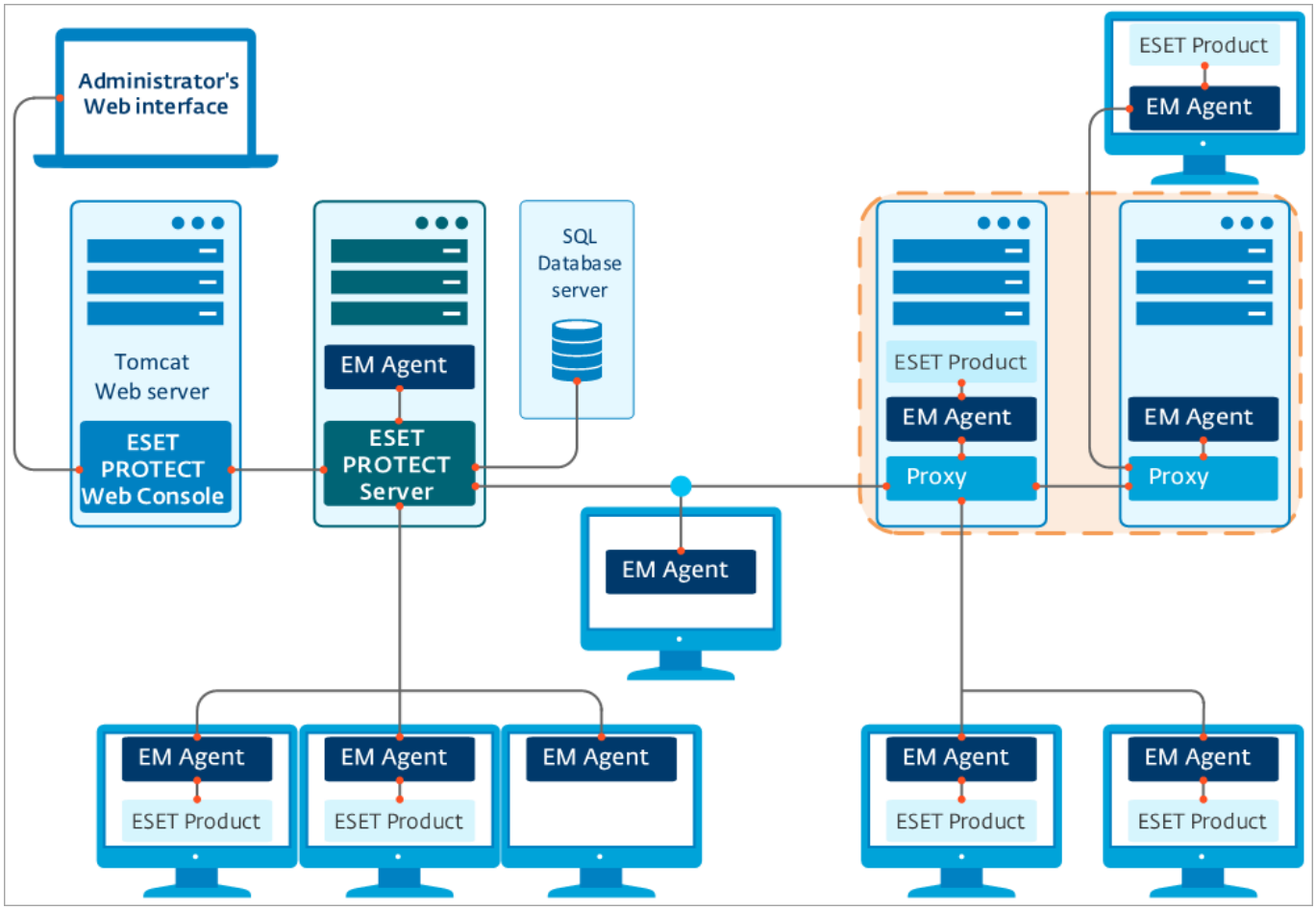
- Si las máquinas de los agentes no pueden conectarse directamente al ESET PROTECT Server.
- Si tiene una oficina remota o una sucursal y desea utilizar Proxy para gestionar la comunicación:
  - Entre ESET PROTECT Server y Proxy
  - Entre Proxy y los ordenadores cliente de una ubicación remota

Configuración del proxy HTTP

Para usar el proxy, el nombre de host del proxy HTTP debe estar configurado en la política del agente (**Configuración avanzada** > **Proxy HTTP**). Puede usar distintos proxies de almacenamiento en caché y reenvío; consulte a continuación la configuración de la política:

- **Proxy global**: utilizará una sola solución proxy para las descargas del almacenamiento en caché y para el reenvío de la comunicación del agente.
- **Un proxy distinto por servicio**: utilizará soluciones proxy independientes para el almacenamiento en caché y para el reenvío de la comunicación.

ℹ ¿Cuáles son las otras funciones del proxy HTTP Apache?



Proxy HTTP Apache

Apache HTTP Proxy es un servicio de proxy que puede usarse para distribuir las actualizaciones a los ordenadores cliente.

Para instalar Apache HTTP Proxy, lea las instrucciones de Windows, Linux o el dispositivo virtual.

Funciones del proxy HTTP Apache

Función	Solución proxy que proporciona esta función
Almacenamiento en caché de descargas y actualizaciones	Proxy HTTP Apache uotra solución proxy
Almacenamiento en caché de los resultados de ESET LiveGuard Advanced	Solo proxy HTTP Apache configurado
Replicación de la comunicación de las instancias de ESET Management Agent con ESET PROTECT Server	Proxy HTTP Apache uotra solución proxy

Función de almacenamiento en caché

Apache HTTP Proxydescarga y almacena en caché:

- Actualizaciones del módulo ESET
- Paquetes de instalación de los servidores de repositorio

- Actualizaciones del componente del producto

Los datos almacenados en caché se distribuyen a los clientes de punto de acceso de la red. El almacenamiento en caché puede reducir considerablemente el tráfico de Internet en la red.

A diferencia de la herramienta Mirror, que descarga todos los datos disponibles en los servidores de actualización de ESET, Apache HTTP Proxy reduce la carga de la red al descargar únicamente los datos que solicitan los componentes de ESET PROTECT o los productos de puntos de acceso de ESET. Si un cliente de punto de acceso solicita una actualización, Apache HTTP Proxy la descarga de los servidores de actualización de ESET, la almacena en su directorio de caché y la distribuye al cliente de punto de acceso en cuestión. Si otro cliente de punto de acceso solicita la misma actualización, Apache HTTP Proxy distribuye la descarga al cliente directamente de su caché, por lo que no se producen descargas adicionales desde los servidores de actualización de ESET.

Almacenamiento en caché para productos ESET Endpoint

La configuración de almacenamiento en caché de ESET Management Agent y Endpoint no es idéntica. ESET Management Agent puede gestionar ajustes de los productos de seguridad de ESET en los dispositivos cliente. Puede configurar el proxy para ESET Endpoint Security:

- A nivel local desde la GUI

- Desde ESET PROTECT Web Console, mediante una política (la forma recomendada de administrar la configuración de los dispositivos cliente).

Almacenamiento en caché de los resultados de ESET LiveGuard Advanced

El proxy HTTP Apache también puede almacenar en la caché los resultados proporcionados por ESET LiveGuard Advanced. El almacenamiento en caché requiere una configuración concreta que se incluye en el Apache HTTP Proxy distribuido por ESET. Siempre que sea posible, se recomienda utilizar el almacenamiento en caché con ESET LiveGuard Advanced. Para obtener más información, consulte la documentación del servicio.

Usar Apache como proxy HTTP para la comunicación entre el agente y el servidor

Cuando se configura correctamente, Apache HTTP Proxy se puede usar para recopilar y reenviar datos de los componentes de ESET PROTECT de una ubicación remota. Una solución proxy se puede usar para el almacenamiento en caché de las actualizaciones (se recomienda usar el proxy HTTP Apache) y otra para la comunicación entre agente y servidor. Se puede usar Apache HTTP Proxy para ambas funciones al mismo tiempo, aunque no se recomienda con redes con más de 10.000 máquinas cliente por proxy. En entornos empresariales (más de 1.000 ordenadores administrados), le recomendamos usar un servidor Apache HTTP Proxy dedicado

Obtenga más información sobre la función Proxy.

Configuración del proxy HTTP

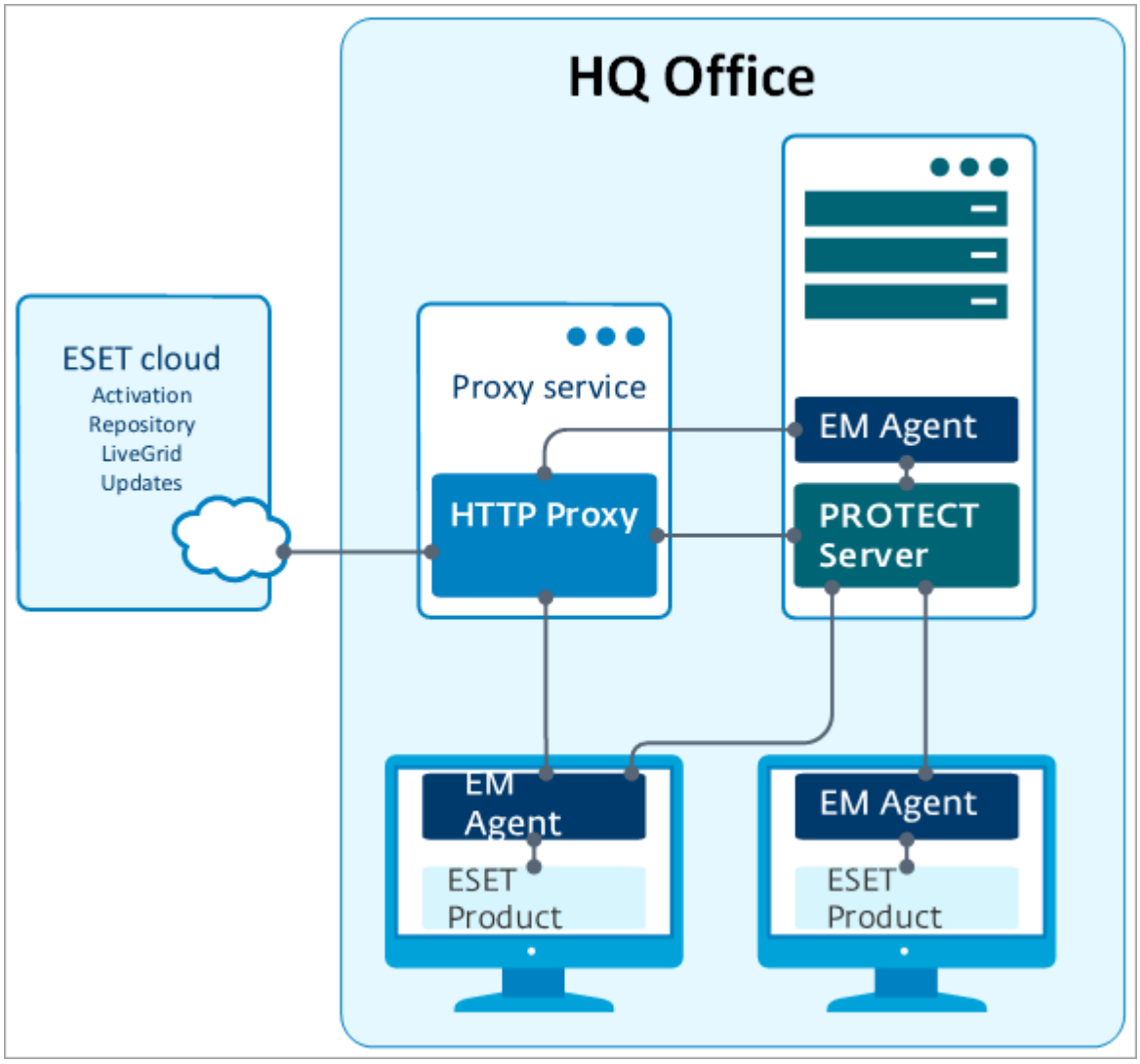
Para usar el proxy, el nombre de host del proxy HTTP debe estar configurado en la política del agente (**Configuración avanzada** > **Proxy HTTP**). Puede usar distintos proxies de almacenamiento en caché y reenvío; consulte a continuación la configuración de la política:

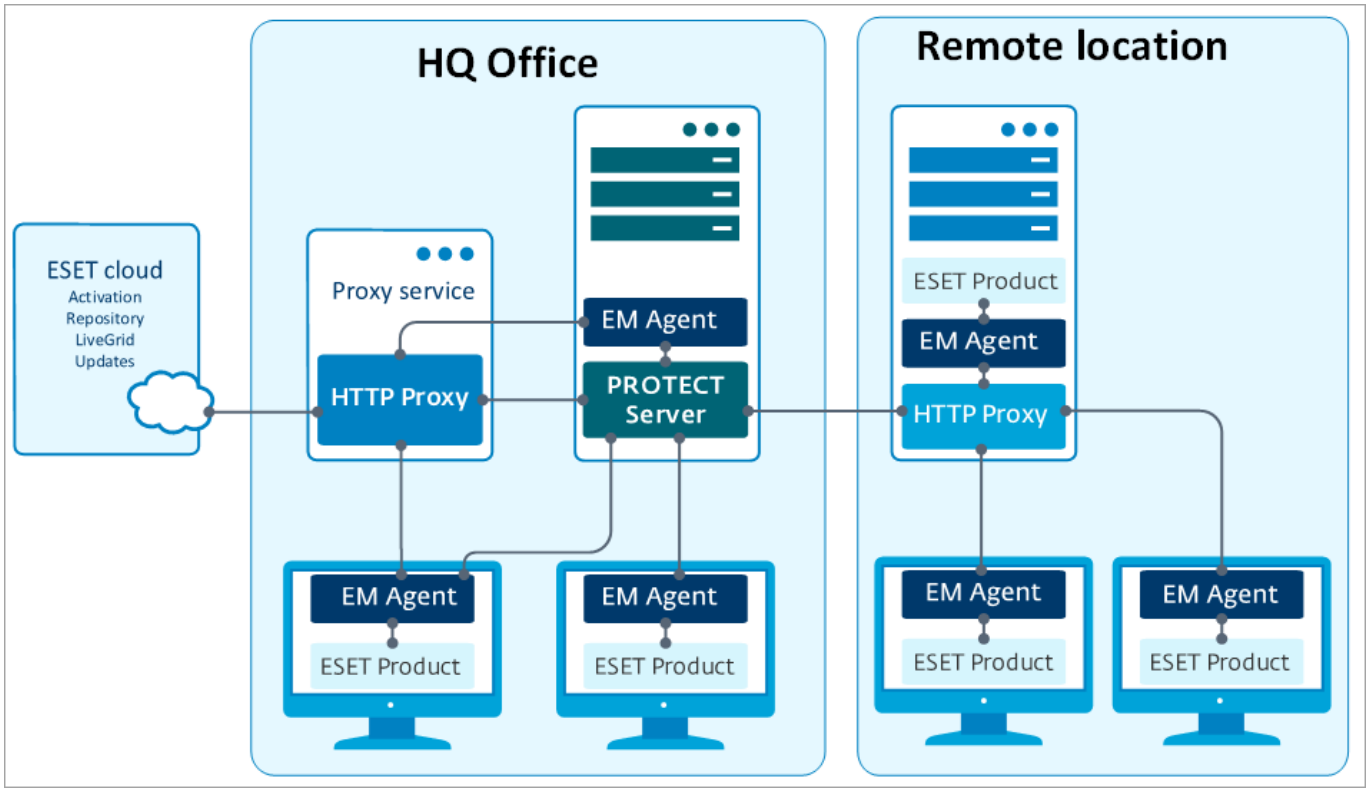
- **Proxy global**: utilizará una sola solución proxy para las descargas del almacenamiento en caché y para el reenvío de la comunicación del agente.

• **Un proxy distinto por servicio**: utilizará soluciones proxy independientes para el almacenamiento en caché y para el reenvío de la comunicación.

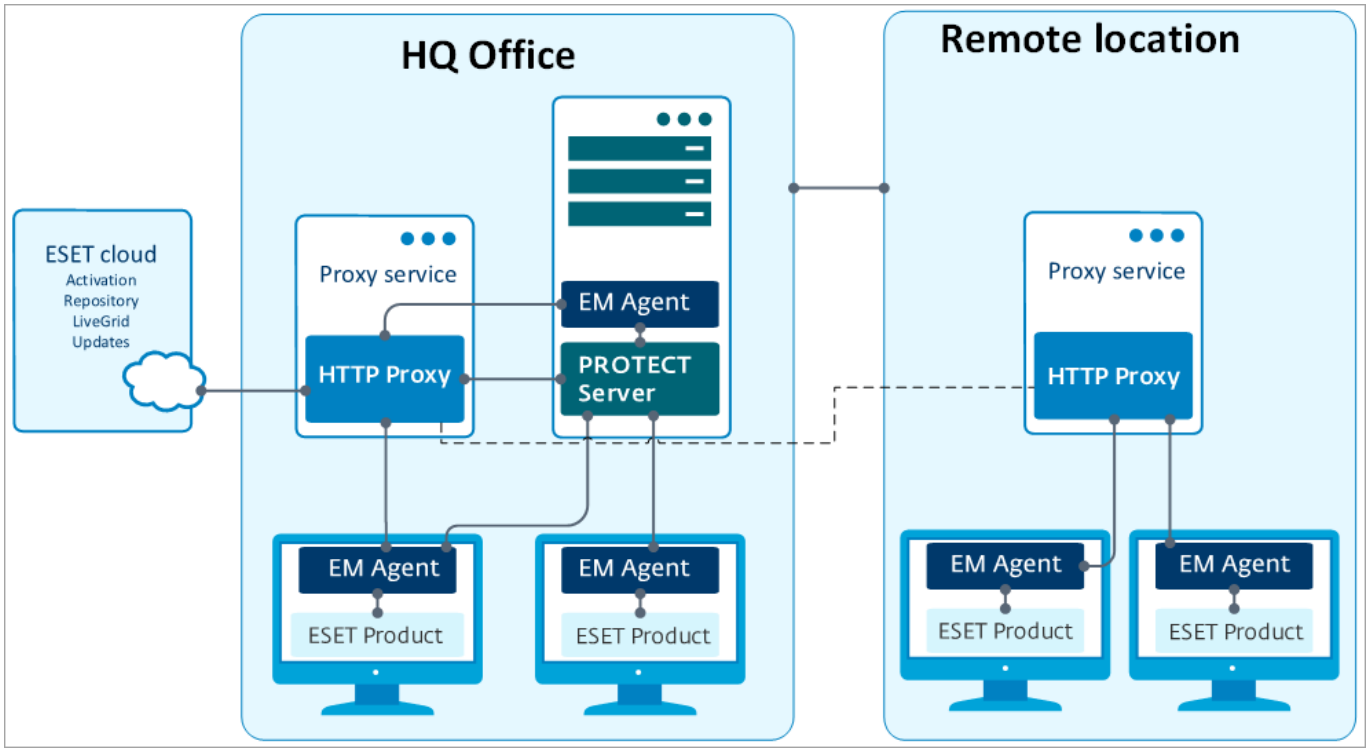
El proxy HTTP Apache en la infraestructura

En el siguiente diagrama se ilustra un servidor proxy (proxy HTTP Apache) que se usa para distribuir el tráfico en la nube de ESET a todos los componentes de ESET PROTECT y a los productos de punto de acceso de ESET.





Puede utilizar una cadena de proxy para agregar otro servicio de proxy a una ubicación remota. Tenga en cuenta que ESET PROTECT no admite el encadenado de proxy cuando los proxies requieren autenticación. Puede utilizar su propia solución de proxy web transparente, pero podría ser necesario configurar otros elementos además de los mencionados en el presente documento.



Para las actualizaciones del motor de detección sin conexión, utilice la herramienta Mirror (disponible para Windows y Linux) en lugar del proxy HTTP Apache.

Agente

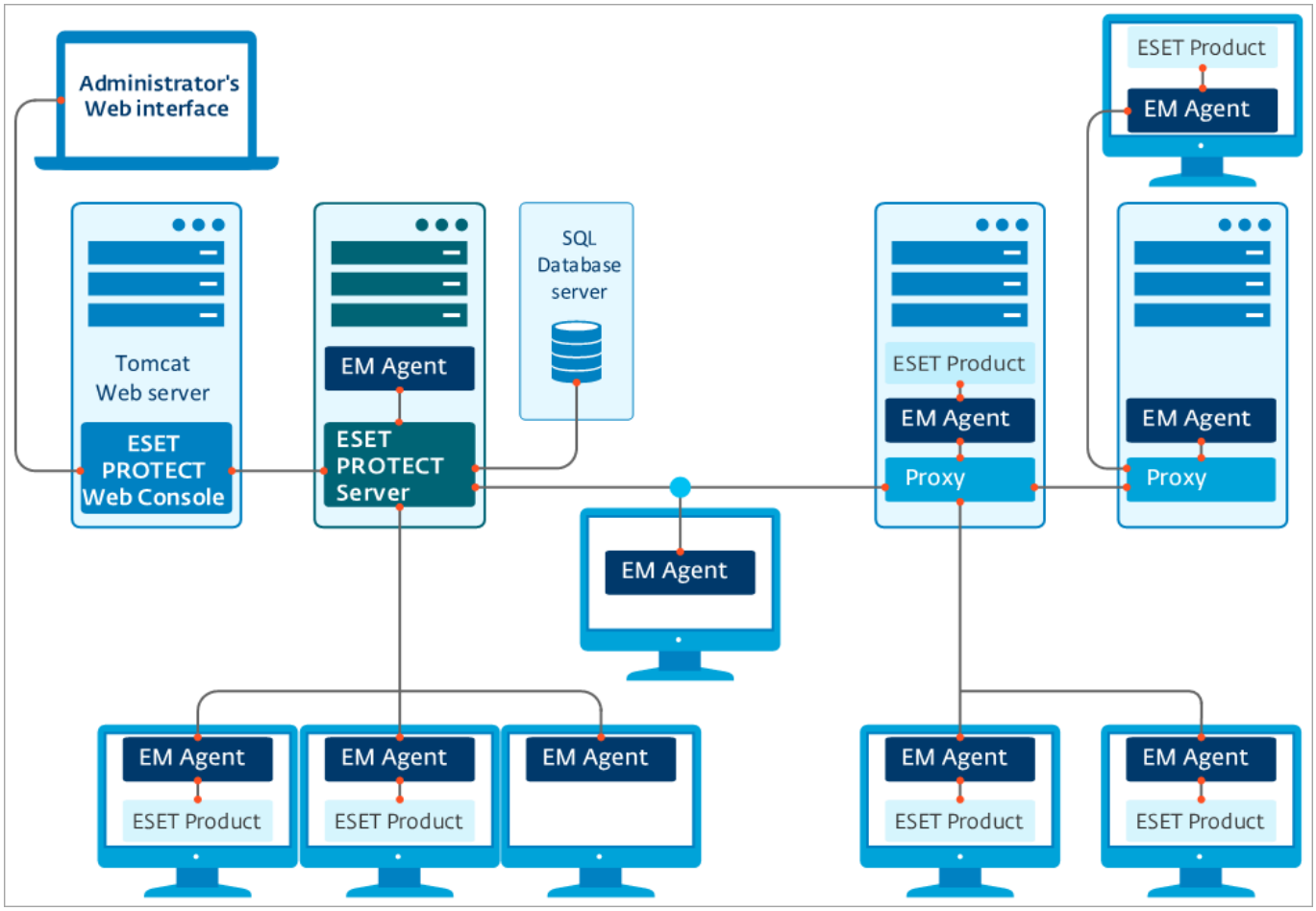
ESET Management Agent es una parte fundamental de ESET PROTECT. Los clientes no se comunican con ESET PROTECT Server directamente, sino que el agente facilita esta comunicación. El agente recopila información del cliente y la envía a ESET PROTECT Server. Si ESET PROTECT Server envía una tarea al cliente, se envía al agente que la envía, a su vez, al cliente. ESET Management Agent utiliza un nuevo protocolo de comunicaciones mejorado.

Para simplificar la aplicación de la protección de puntos de acceso, el ESET Management Agent autónomo está incluido en la suite de ESET PROTECT. Es un servicio sencillo, altamente modular y ligero que se encarga de toda la comunicación entre ESET PROTECT Server y cualquier producto de ESET o sistema operativo. En lugar de comunicarse con ESET PROTECT Server directamente, los productos de ESET se comunican a través del agente. Los ordenadores cliente que tienen instalado ESET Management Agent y se pueden comunicar con ESET PROTECT Server se conocen como "administrados". Puede instalar el agente en cualquier ordenador, independientemente de si se ha instalado o no otro software de ESET.

Las ventajas que ofrecen son:

- Fácil instalación: el agente se puede implementar como parte de la instalación estándar corporativa.
- Administración de seguridad in situ: como el agente puede configurarse para almacenar varias situaciones de seguridad, el tiempo de reacción a la detección se reduce significativamente.
- Administración de seguridad sin conexión: el agente puede responder a un suceso si no está conectado a ESET PROTECT Server.

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



Rogue Detection Sensor

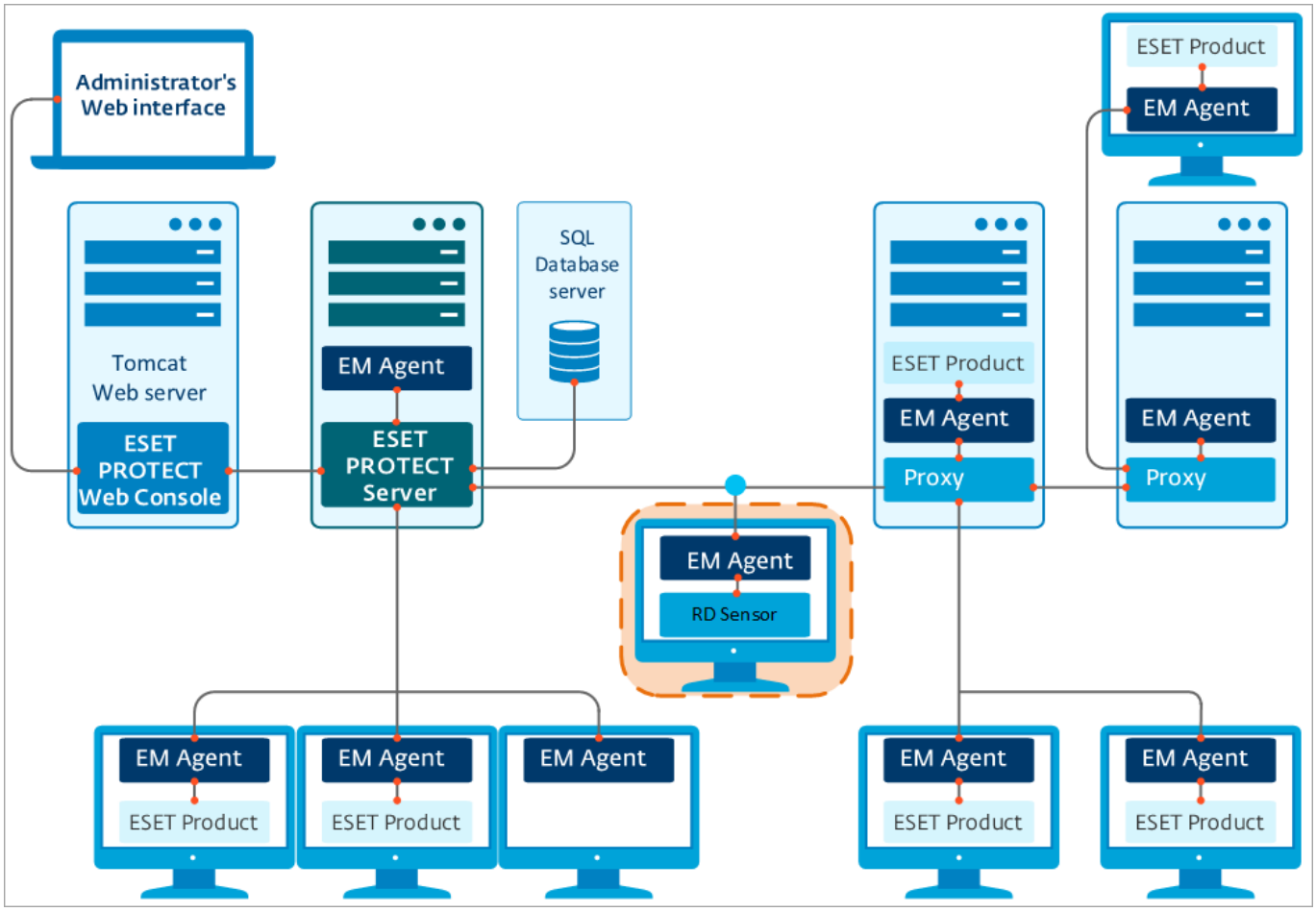
Rogue Detection Sensor (Sensor de RD) es una herramienta de detección que busca sistemas maliciosos en su red de ordenadores. El sensor es cómodo porque puede ubicar los nuevos ordenadores desde ESET PROTECT sin necesidad de buscarlos y agregarlos manualmente. Las máquinas detectadas se localizan inmediatamente y se incluyen en un informa predefinido, lo que le permite trasladarlas a grupos estáticos concretos y continuar con las tareas de administración.

RD Sensor detecta activamente las transmisiones ARP. Cuando RD Sensor detecta un nuevo componente de red activo, RD Sensor envía unidifusiones ARP, crea una huella digital del host (usando varios puertos y envía información sobre los ordenadores detectados a ESET PROTECT Server. A continuación, ESET PROTECT Server evalúa si los PC que se encuentran en la red son desconocidos o ya están administrados.

No puede desactivar la creación de huella digital del host, ya que es la funcionalidad principal de RD Sensor.

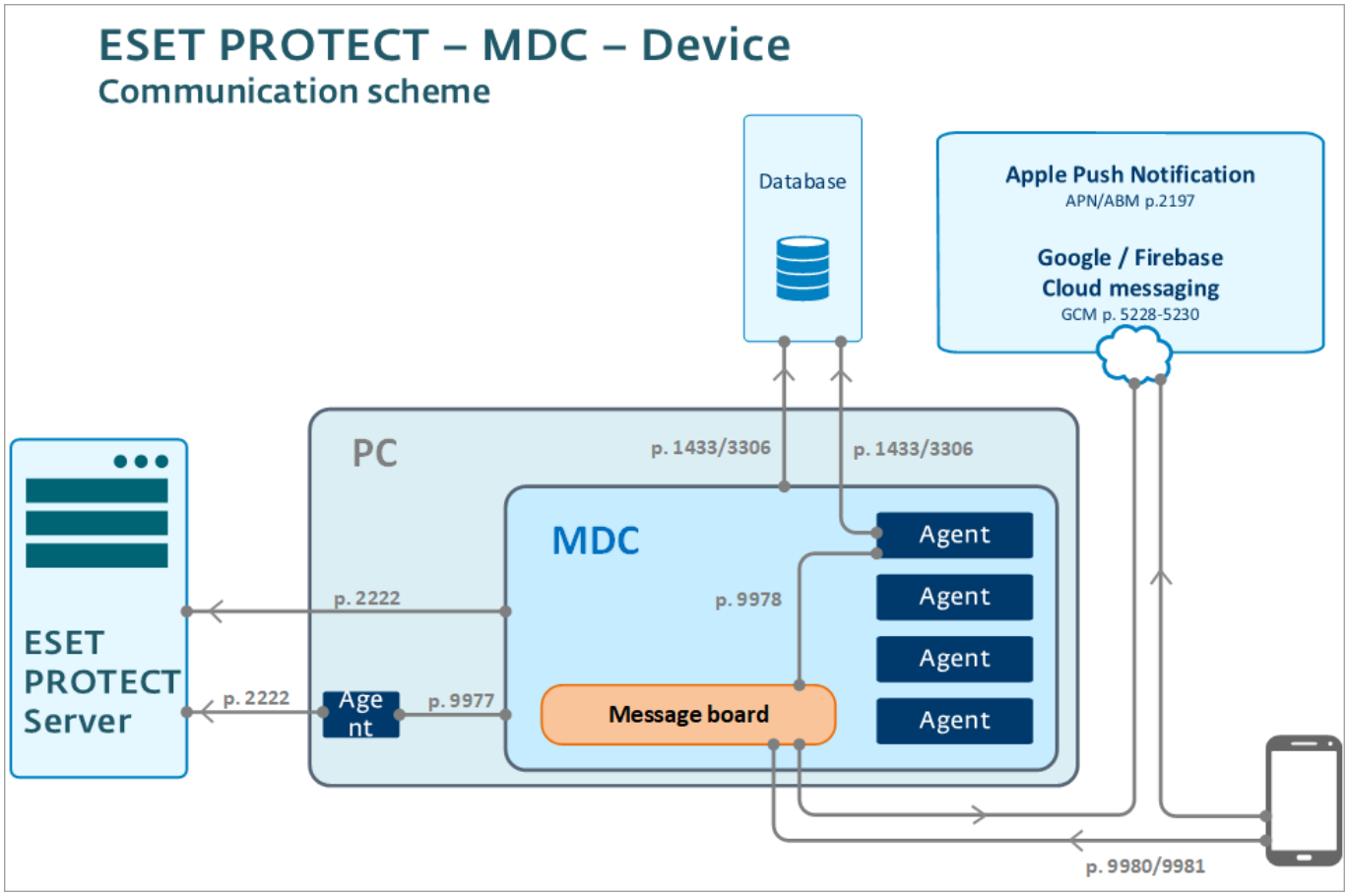
Si hay varios segmentos de red, Rogue Detection Sensor debe instalarse por separado en cada segmento de red para generar una lista completa de todos los dispositivos de toda la red.

Cada ordenador dentro de la estructura de red (dominio, LDAP, red de Windows) se añade a la lista de los ordenadores de ESET PROTECT Server automáticamente a través de una tarea de sincronización del servidor. Utilizar el Sensor de RD es una forma cómoda de encontrar ordenadores que no están en el dominio o en otra estructura de red y agregarlos a ESET PROTECT Server. Sensor de RD recuerda los ordenadores que ya se hayan detectado y no envía la misma información dos veces.



Conector del dispositivo móvil

El Conector del dispositivo móvil ESET PROTECT es un componente que permite utilizar la Administración de dispositivos móviles con ESET PROTECT, lo que posibilita la gestión de dispositivos móviles (Android e iOS) y la administración de ESET Endpoint Security para Android.



Ver la imagen más grande

Le recomendamos que implemente el componente de MDM en un dispositivo host distinto al que se aloja ESET PROTECT Server.

Las condiciones previas de hardware recomendadas para aproximadamente 80 dispositivos móviles son:

Hardware	Configuración recomendada
Procesador	4 núcleos, 2,5 GHz
RAM	4 GB (recomendado)
HDD	100 GB

Para más de 80 dispositivos móviles administrados, los requisitos de hardware no son mucho más estrictos. La latencia entre el envío de la tarea desde ESET PROTECT y la ejecución de la tarea en el dispositivo móvil aumentará proporcionalmente en función del número de dispositivos que haya en su entorno.

Siga las instrucciones de instalación de MDM para Windows (instalador todo en uno o instalación de componentes) o Linux.

Diferencias entre el proxy HTTP Apache, la herramienta Mirror y la conectividad directa

La comunicación con el producto de ESET conlleva la actualización de los módulos del programa y el motor de detección, así como el intercambio de datos de ESET LiveGrid® (consulte la tabla a continuación) y de información

de licencia.

ESET PROTECT descarga los productos más recientes para su distribución a los ordenadores cliente desde el repositorio. Una vez distribuido, el producto está listo para implementarlo en el equipo de destino.

Al instalar un producto de seguridad de ESET, se debe activar. Tras su activación, el motor de detección y los módulos del programa se actualizan de forma periódica.

El Sistema de alerta temprana ESET LiveGrid® ayuda a garantizar que ESET reciba información inmediata y continua de nuevas infiltraciones para proteger a nuestros clientes rápidamente. El sistema permite el envío de nuevas detecciones al laboratorio de investigación de ESET, donde se analizan y procesan.

La mayoría del tráfico de la red lo generan las actualizaciones del módulo del producto. De forma general, un producto de seguridad de ESET descarga aproximadamente 23,9 MB en actualizaciones de módulos al mes.

Los datos de ESET LiveGrid® (aproximadamente 22,3 MB) y el archivo de la versión de actualización (hasta 11 kB) son los únicos archivos distribuidos que no se pueden almacenar en caché.

Hay dos tipos de actualizaciones: actualizaciones de nivel y nano. Consulte nuestro artículo de la base de conocimiento para obtener más información sobre los tipos de actualización.

Hay dos formas de reducir la carga de red al distribuir las actualizaciones a una red de ordenadores, el proxy HTTP Apache y la herramienta Mirror (disponible para Windows y Linux).

> Lea este artículo de la Base de conocimiento para configurar el encadenado de la Herramienta Mirror (configurar la Herramienta Mirror para descargar las actualizaciones de otra Herramienta Mirror).

Tipos de comunicación de ESET

Tipo de comunicación	Frecuencia de comunicación	Repercusión en el tráfico de red	Comunicación reenviada al proxy	Opción 1 de almacenamiento en proxy	Opción 2 de replicación	Opción de entorno sin conexión
Implementación del agente (inserción/Live Installer desde repositorio)	Una vez	Aproximadamente 50 MB por cliente	SÍ	SÍ3	NO	SÍ (GPO/SCCM, Live Installer editados)4
Instalación en punto de acceso (instalación de software desde repositorio)	Una vez	Aproximadamente 100 MB por cliente	SÍ	SÍ3	NO	YES (GPO / SCCM, instalación mediante URL del paquete)4
Módulo del motor de detección/Actualización de módulo del programa	Más de seis veces al día	23,9 MB al mes5	SÍ	SÍ	SÍ	SÍ (Mirror Tool sin conexión y servidor HTTP personalizado)6
Archivo de versión de actualización update.ver	Aproximadamente ocho veces al día	2,6 MB al mes7	SÍ	NO	-	-
Comprobación de la activación o la licencia	Cuatro veces al día	Inapreciable	SÍ	NO	NO	SÍ (los archivos sin conexión se generan en ESET Business Account)8

Tipo de comunicación	Frecuencia de comunicación	Repercusión en el tráfico de red	Comunicación reenviada al proxy	Opción 1 de almacenamiento en proxy	Opción 2 de replicación	Opción de entorno sin conexión
Reputación basada en la nube de ESET LiveGrid®	Al vuelo	11 MB al mes	SÍ	NO	NO	NO

1.Para conocer las ventajas y las repercusiones del almacenamiento en caché del proxy, consulte ¿Cuándo empezar a utilizar el proxy HTTP Apache?

2.Para conocer las repercusiones del uso de la herramienta Mirror, consulte ¿Cuándo empezar a utilizar la herramienta Mirror?

3.Una vez por instalación o actualización, se recomienda implementar un agente (uno por versión concreta) o punto de acceso inicialmente, de forma que el instalador se almacene en caché.

4.Para implementar ESET Management Agent en una red grande, consulte Implementación del agente con GPO y SCCM.

5.La actualización del motor de detección inicial puede ser más grande de lo normal, en función de la antigüedad del paquete de instalación, ya que se descargarán todas las actualizaciones del motor de detección y las actualizaciones de módulos más recientes. Se recomienda instalar un cliente inicialmente y dejar que se actualice, para que las actualizaciones del motor de detección y de los módulos del programa necesarias se almacenen en caché.

6.Sin una conexión a Internet, Mirror Tool no puede descargar las actualizaciones del motor de detección. Puede utilizar Apache Tomcat como servidor HTTP para descargar las actualizaciones en un directorio disponible en la herramienta Mirror (disponible para Windows y Linux).

7.Al comprobar las actualizaciones del motor de detección, el archivo *update.ver* siempre se descarga y analiza. De forma predeterminada, el programador de ESET Endpoint consulta si hay actualizaciones nuevas cada hora. Suponemos que una estación de trabajo cliente está encendida 8 horas al día. El archivo *update.ver* contiene aproximadamente 11 kB.

8.Descargue los archivos de licencia sin conexión de ESET Business Administrator.

i no es posible almacenar en caché con el proxy HTTP Apache las actualizaciones de la versión 4 y 5 del producto. Para distribuir las actualizaciones de estos productos, utilice la Herramienta Mirror.

Cuándo se debe empezar a usar el proxy HTTP Apache

Según las pruebas prácticas que hemos realizados, se recomienda implementar el proxy HTTP Apache si tiene una red de 37 ordenadores o más.

Es esencial para que el almacenamiento en caché sea eficaz que la fecha y la hora del servidor proxy HTTP estén correctamente configuradas. Diferencias de varios minutos harían que el mecanismo de almacenamiento en caché no funcionara de forma eficaz y se descargarían más archivos de los necesarios.

El análisis del ancho de banda de red utilizado exclusivamente por las actualizaciones en una red de prueba de 1.000 ordenadores en la que se realizaron varias instalaciones y desinstalaciones arrojó los siguientes datos:

- Un solo ordenador descarga 23,9 MB de actualizaciones al mes de media si está conectado a Internet de forma directa (sin utilizar un proxy HTTP Apache).
- Utilizando el proxy HTTP Apache, las descargas de toda la red ascendieron a 900 MB mensuales.

Una sencilla comparación de los datos de actualización descargados al mes utilizando la conexión a Internet directa o el proxy HTTP Apache en una red de ordenadores:

N.º de PC en la red corporativa	25	36	50	100	500	1.000
Conexión directa con Internet (MB/mes)	375	900	1.250	2.500	12.500	25.000
Proxy HTTP apache (MB/mes)	30	50	60	150	600	900

¿Cuándo se debe empezar a utilizar la Mirror Tool?

Si tiene un entorno sin conexión, lo que significa que los ordenadores de la red no se conectan a Internet durante un periodo de tiempo prolongado (meses, un año), la herramienta Mirror (disponible para Windows y Linux) es la única forma de distribuir las actualizaciones de los módulos del producto, ya que descarga todas las actualizaciones de Nivel y Nano disponibles después de cada nueva solicitud de actualización, siempre que haya una nueva disponible.

> Lea este artículo de la Base de conocimiento para configurar el encadenado de la Herramienta Mirror (configurar la Herramienta Mirror para descargar las actualizaciones de otra Herramienta Mirror).

La principal diferencia entre el proxy HTTP Apache y la herramienta Mirror es que el proxy HTTP Apache descarga solo las actualizaciones que faltan (por ejemplo, la actualización Nano 3), mientras que Mirror Tool descarga todas las actualizaciones de Nivel y Nano disponibles, sea cual sea la actualización que le falta al módulo del producto en cuestión.

> Las actualizaciones secuenciadas no están disponibles con la herramienta Mirror. Se recomienda preferir la actualización mediante el proxy HTTP para actualizar desde un Mirror siempre que sea posible. Si un ordenador está sin conexión, pero tiene acceso a otro equipo que está conectado a Internet y puede ejecutar el proxy HTTP para almacenar en caché los archivos de actualización, seleccione esta opción.

En la misma red de 1.000 ordenadores probamos la herramienta Mirror en lugar del proxy HTTP Apache. El análisis demostró que se descargaban 5500 MB de actualizaciones al mes. El tamaño de las actualizaciones descargadas no aumentó al agregar más ordenadores a la red. Aún así se produjo una enorme disminución de la carga, en comparación con una configuración en la que los clientes se conectan directamente a Internet, pero la mejora de rendimiento no es tan importante como cuando se usa el proxy HTTP.

N.º de PC en la red corporativa	25	36	50	100	500	1.000
Conexión directa con Internet (MB/mes)	375	900	1.250	2.500	12.500	25.000
Herramienta Mirror (MB/mes)	5.500	5.500	5.500	5.500	5.500	5.500

> Hasta cuando había más de mil ordenadores en la red, el uso de ancho de banda para actualizaciones no aumenta significativamente, ya se utilice el proxy HTTP Apache o la herramienta Mirror.

Requisitos y dimensionamiento del sistema

Su sistema debe cumplir con un conjunto de requisitos previos de hardware, base de datos, red y software para instalar y ejecutar ESET PROTECT.

Sistemas operativos compatibles

En las siguientes secciones se describe la compatibilidad de los componentes de ESET PROTECT con Windows, Linux, macOS y versiones de sistemas operativos móviles.

Windows

En la siguiente tabla se muestran los sistemas operativos Windows compatibles con cada componente de ESET PROTECT:

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 de Windows más recientes (KB4474419 y KB4490628 como mínimo)		✔	✔	
Windows 7 x64 SP1 con las actualizaciones de Windows más recientes (KB4474419 y KB4490628 como mínimo)		✔	✔	
Windows 8 x86		✔	✔	
Windows 8 x64	*	✔	✔	*
Windows 8.1 x86		✔	✔	
Windows 8.1 x64	*	✔	✔	*
Windows 10 x86		✔	✔	
Windows 10 x64 (todas las versiones oficiales)	*	✔	✔	*
Windows 10 en ARM		✔		
Windows 11 x64	*	✔	✔	*

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

Sistemas MS Windows más antiguos:
• Instale siempre el Service Pack más reciente, sobre todo en sistemas más antiguos, como Server 2008 y Windows 7.
• ESET PROTECT no admite la administración de ordenadores que ejecutan Windows 7 (sin SP) Widows Vista y Windows XP.
• A partir del 24 de marzo de 2020, ESET dejará de ser compatible oficialmente o proporcionará soporte técnico para ESET PROTECT (Server y MDM) instalado en los siguientes sistemas operativos Microsoft Windows: Windows 7 Windows Server 2008 (todas las versiones).
No se admiten sistemas operativos ilegales o pirateados.

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

Puede ejecutar ESET PROTECT en un sistema operativo que no sea de servidor y sin necesidad de ESXi. Instalar VMware Player en un sistema operativo de escritorio e implementar el dispositivo virtual ESET PROTECT.

Linux

En la siguiente tabla se muestran los sistemas operativos Linux compatibles con cada componente de ESET PROTECT:

Sistema operativo	Servidor	Agente	RD Sensor	MDM
Ubuntu 16.04.1 LTS x86 Desktop		✔	✔	
Ubuntu 16.04.1 LTS x86 Server		✔	✔	
Ubuntu 16.04.1 LTS x64 Desktop	✔	✔	✔	✔
Ubuntu 16.04.1 LTS x64 Server	✔	✔	✔	✔
Ubuntu 18.04.1 LTS x64 Desktop	✔	✔	✔	✔
Ubuntu 18.04.1 LTS x64 Server	✔	✔	✔	✔
Ubuntu 20.04 LTS x64	✔	✔	✔	✔
RHEL Server 7 x86		✔	✔	
RHEL Server 7 x64	✔	✔	✔	✔
RHEL Server 8 x64	✔*	✔		✔
CentOS 7 x64	✔	✔	✔	✔
SLED 15 x64	✔	✔	✔	✔
SLES 12 x64	✔	✔	✔	✔
SLES 15 x64	✔	✔	✔	✔
OpenSUSE Leap 15.2 x64	✔	✔	✔	✔
Debian 9 x64	✔	✔	✔	✔
Debian 10 x64	✔	✔	✔	✔
Debian 11 x64		✔	✔	
Oracle Linux 8		✔	✔	
Amazon Linux 2		✔	✔	

* Red Hat Entreprise Linux Server 8.x does not support generating of *.pdf* reports - see more details in ESET PROTECT known issues.

macOS

Sistema operativo	Agente
macOS 10.12 Sierra	✔

Sistema operativo	Agente
macOS 10.13 High Sierra	✔
macOS 10.14 Mojave	✔
macOS 10.15 Catalina	✔
macOS 11.0 Big Sur	✔
macOS 12.0 Monterey	✔
macOS 13.0 Ventura	✔

macOS solo se admite como cliente. Los productos ESET Management Agent y ESET para macOS se pueden instalar en macOS. Sin embargo, ESET PROTECT Server no se puede instalar en macOS.

Móvil

Sistema operativo	EESA	Propietario del dispositivo EESA	MDM iOS	MDM iOS ABM
Android 5.x+	✔			
Android 6.x+	✔			
Android 7.x+	✔	✔		
Android 8.x+	✔	✔		
Android 9.0	✔	✔		
Android 10.0	✔	✔		
Android 11	✔	✔		
Android 12	✔			
iOS 9.x+			✔	*
iOS 10.x+			✔	*
iOS 11.x+			✔	*
iOS 12.0.x			✔	*
iOS 13.x+			✔	✔
iOS 14.x+			✔	✔
iOS 15			✔	✔
iOS 16			✔	✔
iPadOS 13.x+			✔	✔
iPadOS 14.x+			✔	✔
iPadOS 15			✔	✔

* iOS DEP solo está disponible en determinados países.

Le recomendamos que actualice el sistema operativo de su dispositivo móvil a la versión más reciente para seguir recibiendo importantes revisiones de seguridad.

Requisitos para iOS 10.3 y versiones posteriores:

Desde la publicación de iOS 10.3, una autoridad certificadora que se instala como parte del perfil de inscripción podría no ser de confianza automáticamente. Para resolver este problema, siga los pasos indicados a continuación.

a)Use un certificado emitido por un emisor de certificados en el que Apple confíe.

b)Instale la confianza en el certificado manualmente antes de realizar el proceso de inscripción. Esto significa que tendrá que instalar la autoridad certificadora raíz manualmente en el dispositivo móvil antes de la inscripción y activar la confianza completa para el certificado instalado.

Requisitos para iOS 12:

Revise los requisitos para iOS 10.3 y versiones posteriores.

- La conexión debe usar **TLS 1.2 o versiones posteriores**.

- La conexión debe usar cifrado simétrico **AES-128** o **AES-256**. El conjunto de cifrado de conexión TLS negociado debe ser compatible con **perfect forward secrecy (PFS)** mediante **intercambio de claves Elliptic Curved Diffie-Hellman Ephemeral (ECDHE)**, y debe ser uno de los siguientes:

```
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

- Estar firmado con una **clave RSA** con una longitud **mínima de 2048 bits**. El algoritmo hash del certificado debe ser **SHA-2 con una longitud de digest** (denominada a veces "huella digital") de 256 como mínimo (es decir, **SHA-256 o superior**). Puede generar un certificado con estos requisitos en ESET PROTECT con la Seguridad avanzada activada.

- Los certificados deben contener **toda la cadena del certificado, incluida la autoridad certificadora raíz**. La autoridad certificadora raíz incluida en el certificado se usa para establecer la confianza con los dispositivos y se instala como parte del perfil de inscripción MDM.

Requisitos para iOS 13:

- La administración de dispositivos móviles con iOS 13 exige cumplir los requisitos del nuevo certificado de comunicación de Apple (HTTPS de MDM). Los certificados emitidos antes del 1 de julio de 2019 también deben cumplir esos criterios.

- El certificado HTTPS firmado por la autoridad certificadora de ESMC no cumple estos requisitos.

Se recomienda encarecidamente no actualizar los dispositivos móviles a iOS 13 antes de cumplir los requisitos del certificado de comunicación de Apple. Esta acción provocará que los dispositivos dejen de conectarse a ESET PROTECT MDM.

- Si ya ha actualizado sin el certificado adecuado y su dispositivo ha dejado de conectarse a ESET PROTECT MDM, primero debe cambiar su certificado HTTPS actual usado para la comunicación con dispositivos iOS al certificado que cumpla los requisitos del certificado de comunicación de Apple (HTTPS de MDM) y, después, volver a inscribir los dispositivos iOS.

- Si no ha actualizado a iOS 13, asegúrese de que su certificado HTTPS de MDM actual usado para la comunicación con dispositivos iOS cumple los requisitos del certificado de comunicación de Apple (HTTPS de MDM). Si lo desea, puede seguir actualizando sus dispositivos iOS a iOS 13. Si no cumple los requisitos, cambie el certificado HTTPS de MDM actual al certificado HTTPS que cumpla los requisitos del certificado de comunicación de Apple (HTTPS de MDM) y, después continúe actualizando sus dispositivos iOS a iOS 13.

Entornos de aprovisionamiento de escritorios admitidos

El aprovisionamiento de escritorios facilita la administración de los dispositivos y permite proporcionar ordenadores de escritorio a los usuarios finales de una forma más rápida.

Los escritorios aprovisionados suelen ser físicos o virtuales. Para los entornos virtualizados que utilizan un SO transmitido (servicios de aprovisionamiento de Citrix), consulte a continuación la lista de hipervisores compatibles.

ESET PROTECT es compatible con:

- sistemas con discos no persistentes
- entornos VDI
- identificación de ordenadores clonados

Hipervisores y extensiones de hipervisor compatibles

Hipervisor	ESET PROTECT	ESET Full Disk Encryption
Citrix XenServer	✔	X
Microsoft Hyper-V	✔	✔ (no se admite el arranque seguro)
VMware vSphere	✔	✔ (7.0.3.00300)
VMware ESXi	✔	✔ (7.0)
VMware Workstation	✔	✔ (16.2.3)
VMware View	✔	X
Oracle VirtualBox	✔	X
VMware Fusion	X	✔ (12.2.3)
Paralelos	X	✔

Extensión del hipervisor	ESET PROTECT	ESET Full Disk Encryption
Citrix VDI-in-a-box	✔	X
Citrix XenDesktop	✔	X

Herramientas

(se aplica tanto a los equipos virtuales como físicos)

- Microsoft SCCM
- Windows Server 2012/2016/2019/2022 Server Manager
- Windows Admin Center

Dimensionamiento de hardware e infraestructura

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

Número de clientes	ESET PROTECT Server + Servidor de bases de datos SQL				
	Núcleos de la CPU	Velocidad de reloj de la CPU (GHz)	RAM (GB)	Unidad de disco[1]	ESPS[2] en disco
Hasta 1.000	4	2.1	4	Única	500
5.000	8	2.1	8		1.000
10,000 [3]	4	2.1	16	Independiente	2.000
20.000	4	2.1	16		4.000
50.000	8	2.1	32		10.000
100.000	16	2.1	64 o superior		20.000

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

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

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

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

3 Consulte el caso de ejemplo para un entorno de 10.000 clientes.

Recomendaciones de unidad de disco

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

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

- El rendimiento de un servidor SQL mejorará si coloca la los archivos de base de datos y de registro de transacciones en unidades independientes, a ser posible en unidades SSD físicas independientes.

- Si tiene una sola unidad de disco, le recomendamos utilizar una unidad SSD.

- Le recomendamos que utilice una arquitectura íntegramente con memoria flash. Los discos de estado sólido (SSD) son mucho más rápidos que la unidad de disco duro estándar.

- Si cuenta con una alta capacidad de RAM, una configuración SAS con R5 será suficiente. La configuración probada: Diez discos SAS de 1,2 TB en R5: dos grupos de paridad en 4+1 sin almacenamiento en caché adicional.

- El rendimiento no mejora cuando se utiliza un SSD empresarial con un alto número de IOPS.

- Una capacidad de 100 GB es suficiente para cualquier cantidad de clientes. Puede que necesite mayor capacidad si realiza copias de seguridad de la base de datos con frecuencia.

- No utilice una unidad de red, ya que su rendimiento ralentizará ESET PROTECT.

- Si trabaja con una infraestructura de almacenamiento de varios niveles que permite la migración al almacenamiento en línea, le recomendamos que empiece por niveles compartidos más lentos y supervise el rendimiento de ESET PROTECT. Si observa que la latencia de lectura/escritura supera los 20 ms, puede realizar un traslado sin interrupciones de la capa de almacenamiento a un nivel más rápido para utilizar el backend más rentable. Puede hacer lo mismo en un hipervisor (si utiliza ESET PROTECT como máquina virtual).

Recomendaciones de dimensionamiento para distintos recuentos de clientes

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

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

Núcleos de la CPU	Velocidad de reloj de la CPU (GHz)	RAM (GB)	Rendimiento		
			10.000 clientes	20.000 clientes	40.000 clientes
8	2.1	64	Alta	Alta	Normal
8	2.1	32	Normal	Normal	Normal
4	2.1	32	Normal	Normal	Baja
2	2.1	16	Baja	Baja	Insuficiente

Núcleos de la CPU	Velocidad de reloj de la CPU (GHz)	RAM (GB)	Rendimiento		
			10.000 clientes	20.000 clientes	40.000 clientes
2	2.1	8	Muy bajo (no recomendado)	Muy bajo (no recomendado)	Insuficiente

Recomendaciones de implementación

Prácticas recomendadas para la implementación de ESET PROTECT

Número de clientes	Hasta 1.000	1.000 - 5.000	5.000 - 10.000	10.000 - 50.000	50.000 - 100.000	Más de 100 000
ESET PROTECT Server y servidor de bases de datos en el mismo equipo	✔	✔	✔	X	X	X
Uso de MS SQL Express	✔	?*	X	X	X	X
Uso de MS SQL	✔	✔	✔	✔	✔	✔
Uso de MySQL	✔	✔	✔	X	X	X
Uso de dispositivo virtual de ESET PROTECT	✔	✔	No recomendado	X	X	X
Uso de servidor de máquinas virtuales	✔	✔	✔	Opcional	X	X
Intervalo de conexión recomendado (durante la fase de implementación)	60 segundos	5 minutos	10 minutos	15 minutos	20 minutos	25 minutos
Intervalo de conexión recomendado (tras la implementación, durante la fase estándar)	10 minutos	10 minutos	20 minutos	30 minutos	40 minutos	60 minutos

* Para evitar llenar la base de datos de ESET PROTECT, no recomendamos proceder de esta forma si también utiliza ESET Inspect.

Intervalo de conexión

ESET PROTECT Server está conectado a ESET Management Agents mediante conexiones permanentes. Pese a la conexión permanente, la transmisión de datos solo se produce una vez durante el intervalo de conexión. Por ejemplo, si el intervalo de replicación en 5.000 clientes está configurado en ocho minutos, hay 5.000 transmisiones en 480 segundos, 10,4 por segundo. Asegúrese de establecer el intervalo de conexión del cliente adecuado. Asegúrese de mantener el número total de conexiones entre el agente y el servidor por debajo de 1.000 por segundo para las configuraciones de hardware de gran rendimiento.

Si un servidor está sobrecargado o se produce un estallido de código malicioso (por ejemplo, cuando se conectan 20.000 clientes a un servidor que solo tiene capacidad para atender a 10.000 clientes cada 10 minutos), omite algunos de los clientes conectados. Los clientes que no se conecten intentarán conectarse a ESET PROTECT Server más tarde.

Un solo servidor (pequeñas empresas)

Para administrar redes pequeñas (1.000 clientes o menos) utilice una sola máquina con ESET PROTECT Server y todos los componentes de ESET PROTECT instalados. En los entornos de redes de pequeño tamaño/pequeñas y medianas empresas, le recomendamos que realice una instalación de ESET PROTECT para Linux o utilice un dispositivo virtual cuando corresponda.

Sucursales remotas con proxies

Si las máquinas cliente no ven directamente el ESET PROTECT Server, utilice un proxy para reenviar la comunicación con productos de ESET. El proxy HTTP no está agregando la comunicación ni reduciendo el tráfico de replicación.

Alta disponibilidad (empresas)

Para entornos empresariales (más de 10 000 clientes), tenga en cuenta lo siguiente:

- El Sensor de RD ayuda a buscar en la red y encontrar ordenadores nuevos.
- Puede instalar ESET PROTECT Server en un clúster de conmutación por error.
- Configure su proxy HTTP para un número elevado de clientes.

Configuración de Web Console para soluciones empresariales o sistemas de bajo rendimiento

De forma predeterminada, ESET PROTECT Web Console instalado con el instalador todo en uno para Windows reserva un límite de memoria de 1.024 MB para Apache Tomcat.

Puede cambiar la configuración predeterminada de Web Console en función de su infraestructura:

- En un entorno empresarial, la configuración predeterminada de Web Console puede ser inestable si se trabaja con un gran número de objetos. Cambie la configuración de Tomcat para evitar que la memoria se llene. Asegúrese de que el sistema tenga suficiente RAM (16 GB o más) antes de realizar estos cambios.
- Si tiene un sistema de bajo rendimiento con recursos de hardware limitados, puede disminuir el uso de memoria de Tomcat.

> Los valores de memoria indicados a continuación son recomendaciones. Puede ajustar la configuración de la memoria de Tomcat en función de los recursos de hardware.

Windows

1. Abra *tomcat9w.exe* o ejecute la aplicación `Configure Tomcat`.
2. Cambie a la ficha **Java**.
3. Cambie el uso de la memoria:

a.Aumentar (empresa): Cambie los valores de **Bloque de memoria inicial** a 2.048 MB y de **Bloque de memoria máxima** a 16.384 MB.

b.Reducir (sistemas de bajo rendimiento): Cambie los valores de **Bloque de memoria inicial** a 256 MB y de **Bloque de memoria máxima** a 2.048 MB.

4.Reinicie el servicio Tomcat.

LINUX y el dispositivo virtual de ESET PROTECT

1.Abra el terminal como usuario raíz o utilice `sudo`.

2.Abra el archivo:

a.Dispositivo virtual de ESET PROTECT / CentOS: `/etc/sysconfig/tomcat`

b.Debian: `/etc/default/tomcat9`

3.Añada la siguiente línea al archivo:

a.Aumentar el uso de memoria (empresa): `JAVA_OPTS="-Xms2048m -Xmx16384m"`

b.Disminuir el uso de memoria (sistemas de bajo rendimiento): `JAVA_OPTS="-Xms256m -Xmx2048m"`

4.Guarde el archivo y reinicie el servicio Tomcat.

```
service tomcat restart
```

Implementación para 10.000 clientes

A continuación puede ver los resultados de rendimiento de un entorno virtual con 10.000 clientes en ejecución durante un año.

Configuración del servidor Hypervisor

Componente	Valor
VMware	ESXi 6.7 Update 2 y versiones posteriores (versión 15 de la máquina virtual)
Hipervisor	VMware ESXi, 6.7.0
Procesadores lógicos	112
Tipo de procesador	Intel(R) Xeon(R) Platinum 8176 CPU @ 2.10GHz

La prueba se ejecutó en equipos dedicados
La base de datos de y ESET PROTECT se están ejecutando en máquinas virtuales independientes con configuraciones de hardware idénticas.

Software que se utiliza en las máquinas virtuales

ESET PROTECT:

- SO: Microsoft Windows Server 2016 Standard (64-bit)

Base de datos:

- Database server: Microsoft SQL Server 2017 (RTM) Standard Edition (64-bit)
- SO: Microsoft Windows Server 2016 Standard (64-bit)

Descripción del entorno de ESET PROTECT

- 10.000 clientes conectándose
- Aproximadamente 2.000 grupos dinámicos y 2.000 plantillas para grupos dinámicos
- Aproximadamente 255 grupos estáticos
- 20 usuarios
- Intervalo de conexión de 15 minutos para las instancias de ESET Management Agent
- Cuando el entorno lleva un año en funcionamiento, el tamaño de la base de datos es de 15 GB

Número de CPU	RAM (GB)	Rendimiento
8	64	Alta
4	32	Normal
2	16	Baja
2	8	Muy bajo (no recomendado)

Base de datos

Especifique el servidor de base de datos y el conector que desee utilizar cuando instale ESET PROTECT Server. Puede utilizar un servidor de bases de datos que se ejecute en su entorno; sin embargo, debe cumplir los requisitos que se indican a continuación.

El instalador todo en uno de ESET PROTECT 9.1 instala Microsoft SQL Server Express 2019 de forma predeterminada.

- Si utiliza una versión anterior de Windows (Server 2012 o SBS 2011), Microsoft SQL Server Express 2014 se instalará de forma predeterminada.
- El instalador genera automáticamente una contraseña aleatoria para la autenticación de la base de datos (almacenada en *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

> ⚠ Microsoft SQL Server Express tiene un límite de tamaño de 10 GB en cada base de datos relacional. No recomendamos el uso de Microsoft SQL Server Express:
> - En entornos empresariales o redes de gran tamaño.
> - Si desea usar ESET PROTECT con ESET Inspect.

Servidores de bases de datos y conectores de bases de datos compatibles

ESET PROTECT es compatible con dos tipos de servidores de bases de datos: Microsoft SQL Server y MySQL.

ESET PROTECT no es compatible con MariaDB. MariaDB es una base de datos predeterminada en la mayoría de los entornos Linux actuales y se instala cuando selecciona instalar MySQL.

Servidor de bases de datos compatibles	Versiones de bases de datos compatibles	Conectores de bases de datos compatibles
Microsoft SQL Server	• Ediciones Express y no Express • 2014, 2016, 2017, 2019	• SQL Server • Cliente nativo de SQL Server versión 10.0 • Controlador ODBC para SQL Server 11, 13, 17, 18
MySQL	• 5.6* • 5.7 • 8.0	Versiones del controlador MySQL ODBC: • 5.1, 5.2 • 5.3.0-5.3.10 • 8.0.16, 8.0.17 • 8.0.27 Solo Windows

* MySQL 5.6 llegó al fin de su vida útil en febrero de 2021. Le recomendamos que actualice el servidor de base de datos MySQL a la versión 5.7 y posteriores.

Las siguientes versiones del controlador MySQL ODBC no son compatibles:
- 5.3.11 y 5.3.x posteriores
- 8.0.0-8.0.15
- 8.0.18 y posteriores

Requisitos de hardware del servidor de base de datos

Consulte las instrucciones de hardware y dimensionamiento.

Recomendaciones de rendimiento

Se recomienda usar la versión de Microsoft SQL Server compatible más reciente como base de datos de ESET PROTECT para conseguir el máximo rendimiento. Aunque ESET PROTECT es compatible con MySQL, utilizar MySQL puede afectar negativamente al rendimiento del sistema cuando se trabaja con grandes cantidades de datos, incluidos paneles, detecciones y clientes. El mismo hardware con Microsoft SQL Server puede gestionar un número considerablemente mayor de clientes que con MySQL.

Puede decidir si desea instalar un servidor de bases de datos SQL en:

- El mismo equipo que ESET PROTECT Server.
- El mismo equipo pero en un disco independiente
- Un servidor dedicado para la instalación de un servidor de bases de datos SQL.

Se recomienda utilizar uno o varios ordenadores dedicados con recursos reservados si desea gestionar más de

10 000 clientes.

Base de datos	Cliente de pyme	Cliente de gran empresa	Límite de clientes	Windows	Linux
MS SQL Express	✔	(opcional)	5.000	✔	
MS SQL Server	✔	✔	Ninguno	✔	
MySQL	✔	✔	10.000	✔	✔

Información adicional

ESET PROTECT Server no usa una copia de seguridad integrada. Le recomendamos encarecidamente que realice una copia de seguridad de su servidor de base de datos para evitar la pérdida de datos.

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

- Si tiene previsto utilizar la cuenta de usuario de base de datos dedicada que tendrá acceso solo a la base de datos de ESET PROTECT, deberá crear una cuenta de usuario con privilegios específicos antes de la instalación. Para obtener más información, consulte Cuenta de usuario de base de datos dedicada. Además, deberá crear una base de datos vacía para que la utilice ESET PROTECT.

- Consulte las instrucciones sobre cómo instalar y configurar MySQL para Windows y MySQL para Linux para que funcionen correctamente con ESET PROTECT.

- No se admite MS SQL Server en Linux. Sin embargo, puede conectar ESET PROTECT Server en Linux a MS SQL Server en Windows.

- Si instala ESET PROTECT Server y MS SQL Server en ordenadores independientes, puede activar la conexión cifrada con la base de datos.

- La configuración en clúster de la base de datos en entornos Windows solo es compatible con MS SQL Server, no con MySQL.

Versiones compatibles de Apache Tomcat y Java

Apache Tomcat

Apache Tomcat es un componente obligatorio necesario para ejecutar ESET PROTECT Web Console.

ESET PROTECT solo es compatible con Apache Tomcat 9.x (64 bits). Se recomienda usar la versión más reciente de Apache Tomcat 9.x.

ESET PROTECT no es compatible con versiones alfa/beta/RC de Apache Tomcat.

Java

Apache Tomcat requiere Java/OpenJDK de 64 bits.

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

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

Navegadores web, productos de seguridad de ESET e idiomas compatibles

Los siguientes sistemas operativos son compatibles con ESET PROTECT:

- Windows, Linux y macOS

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

Navegador web
Mozilla Firefox
Microsoft Edge
Google Chrome
Safari
Opera

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

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

Versiones más recientes de productos de ESET que se pueden administrar con ESET PROTECT 9.1

Producto	Versión del producto
ESET Endpoint Security para Windows	7.x, 8.x, 9.x
ESET Endpoint Antivirus para Windows	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
ESET Server Security para Microsoft Windows Server	8.x, 9.x
ESET File Security para Microsoft Windows Server	7.x
ESET File Security para Microsoft Azure	7.x
ESET Mail Security para Microsoft Exchange Server	7.x, 8.x, 9.x

Producto	Versión del producto
ESET Security para Microsoft SharePoint Server	7.x, 8.x, 9x
ESET Mail Security para IBM Domino Server	7.x, 8.x, 9.x
ESET File Security en Linux	7.x, 8.x
ESET Server Security en Linux	8.1+
ESET Endpoint Antivirus en Linux	7.x, 8.x, 9.x
ESET LiveGuard Advanced	
ESET Inspect Connector	1.6+
ESET Full Disk Encryption para Windows	
ESET Full Disk Encryption para macOS	

Versiones más recientes de productos de ESET que se pueden administrar con ESET PROTECT 9.1

Producto	Versión del producto
ESET Endpoint Security para Windows	6.5+
ESET Endpoint Antivirus para Windows	6.5+
ESET File Security para Microsoft Windows Server	6.5
ESET File Security para Microsoft Azure	6.5
ESET Mail Security para Microsoft Exchange Server	6.5
ESET Mail Security para IBM Lotus Domino	6.5
ESET Security para Microsoft SharePoint Server	6.5
ESET Mail Security para Linux/FreeBSD*	4.5.x
ESET File Security para Linux/FreeBSD*	4.5.x
ESET Gateway Security para Linux/FreeBSD*	4.5.x

* No puede administrar este producto con ESET Management Agent 9. Para administrar el producto, utilice ESET Management Agent 8.1 o una versión anterior.

Las versiones de productos de seguridad de ESET anteriores a las mostradas en la tabla anterior no pueden gestionarse aún con ESET PROTECT 9.
Si desea obtener más información sobre la compatibilidad, visite la política sobre el fin de la vida útil de los productos de ESET para empresas.

Productos compatibles con la activación a través de la licencia de suscripción

Producto de ESET	Disponible desde la versión
ESET Endpoint Antivirus/Security para Windows	7.0
ESET Endpoint Antivirus/Security para macOS	6.8.x
ESET Endpoint Security para Android	2.0.158
Administración de dispositivos móviles de ESET para Apple iOS	7.0

Producto de ESET	Disponible desde la versión
ESET File Security para Microsoft Windows Server	7.0
ESET Mail Security para Microsoft Exchange	7.0
ESET File Security para Windows Server	7.0
ESET Mail Security para IBM Domino	7.0
ESET Security para Microsoft SharePoint Server	7.0
ESET File Security en Linux	7.0
ESET Endpoint Antivirus en Linux	7.0
ESET Server Security para Windows	8.0
ESET Server Security para Linux	8.1
ESET LiveGuard Advanced	
ESET Inspect (con ESET Endpoint para Windows 7.3 y versiones posteriores)	1.5

Idiomas compatibles

Idioma	Código
Inglés (Estados Unidos)	en-US
Árabe (Egipto)	ar-EG
Chino simplificado	zh-CN
Chino tradicional	zh-TW
Croata (Croacia)	hr-HR
Checo (República Checa)	cs-CZ
Francés (Francia)	fr-FR
Francés (Canadá)	fr-CA
Alemán (Alemania)	de-DE
Griego (Grecia)	el-GR
Húngaro (Hungría)*	hu-HU
Indonesio (Indonesia)*	id-ID
Italiano (Italia)	it-IT
Japonés (Japón)	ja-JP
Coreano (Corea)	ko-KR
Polaco (Polonia)	pl-PL
Portugués (Brasil)	pt-BR
Ruso (Rusia)	ru-RU
Español (Chile)	es-CL
Español (España)	es-ES
Eslovaco (Eslovaquia)	sk-SK
Turco (Turquía)	tr-TR
Ucraniano (Ucrania)	uk-UA

* Solo está disponible el producto en este idioma; la ayuda en línea no está disponible.

Red

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

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

ESET PROTECT para Windows/Linux es compatible con los protocolos de Internet IPv4 e IPv6. El dispositivo virtual de ESET PROTECT solo es compatible con IPv4.

Puertos utilizados

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

Repercusión de la comunicación de ESET PROTECTServer y ESET Management Agent sobre el tráfico de red

Las aplicaciones de los equipos cliente no se comunican directamente con ESET PROTECT Server, ESET Management Agent facilita esta comunicación. Esta solución resulta más sencilla de administrar y transfiere menos datos mediante la red. El tráfico de red depende del intervalo de conexión de los clientes y los tipos de tareas que estos realizan. Aunque no haya ninguna tarea programada o en ejecución en un cliente, ESET Management Agent se comunica con ESET PROTECT Server una vez en cada intervalo de conexión. Cada conexión genera tráfico. En la siguiente tabla puede ver ejemplos de tráfico:

Tipo de acción	Tráfico en un intervalo de conexión
Tareas del cliente: Analizar sin desinfectar	4 kB
Tareas del cliente: Actualización de módulos	4 kB
Tareas del cliente: Solicitud de registro de SysInspector	300 kB
Política Antivirus: máxima seguridad	26 kB

ESET ManagementIntervalo de replicación de Agent	Tráfico diario generado por una instancia de ESET Management Agent en inactividad
1 minuto	16 MB
15 minutos	1 MB
30 minutos	0,5 MB
1 hora	144 kB
1 día	12 kB

Utilice la siguiente fórmula para calcular el tráfico global generado por las instancias de ESET Management Agent:

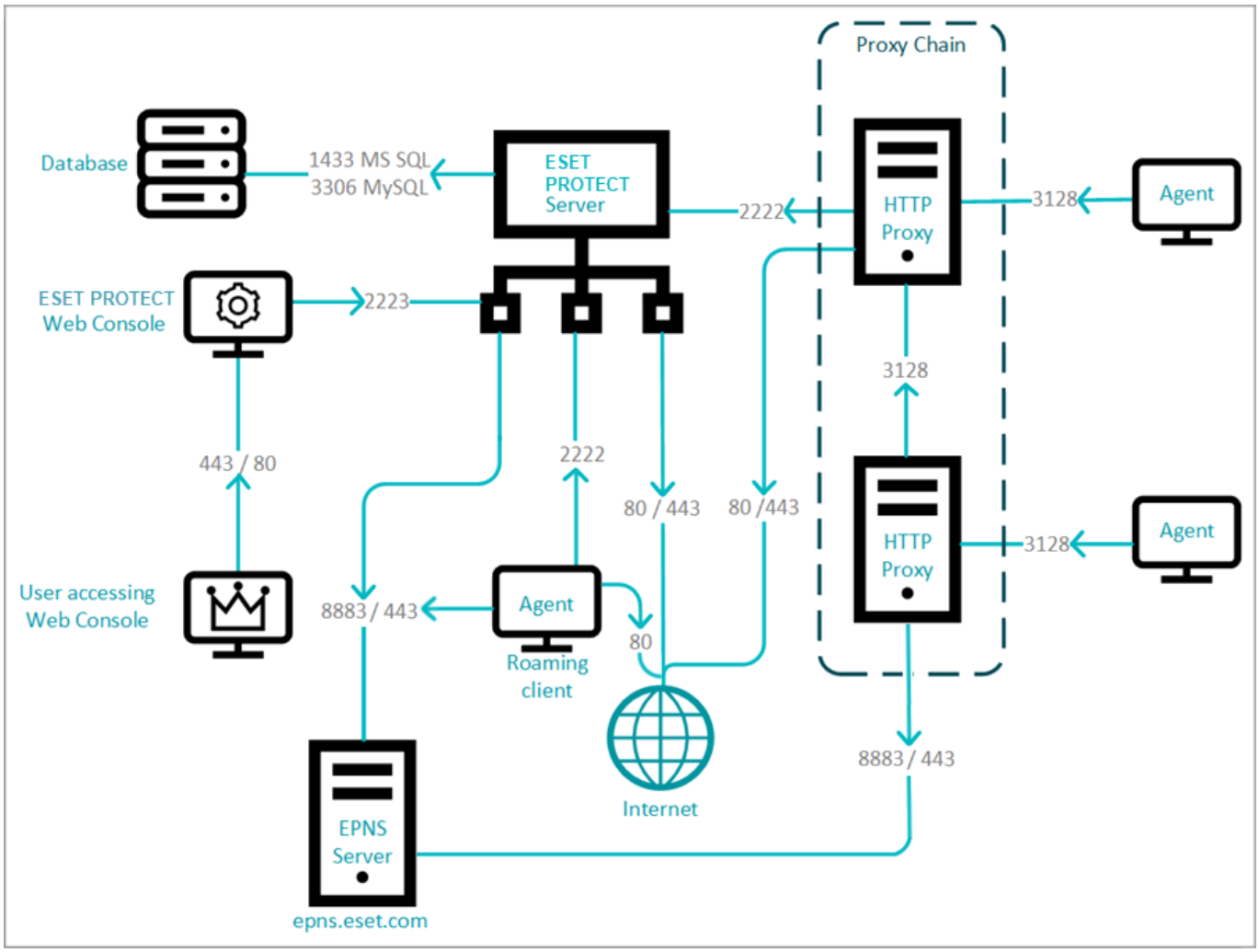
*Número de clientes * (tráfico diario de agente inactivo + (tráfico de una tarea determinada * repeticiones diarias*

de la tarea))

Si utiliza ESET Inspect, ESET Inspect Connector genera un tráfico diario de 2 a 5 MB (varía en función del número de sucesos).

Puertos utilizados

ESET PROTECT Server se puede instalar en el mismo ordenador que la base de datos, la Consola web de ESET PROTECT y el proxy HTTP Apache. En el siguiente diagrama se muestra la instalación separada y los puertos utilizados (las flechas indican el tráfico de red):



En las tablas que aparecen a continuación se exponen los posibles puertos de comunicación de red que se utilizan cuando se instala ESET PROTECT y sus componentes en su infraestructura. Se produce otra comunicación por medio de procesos nativos del sistema operativo (por ejemplo NetBIOS sobre TCP/IP).

Para el correcto funcionamiento de ESET PROTECT, el resto de aplicaciones no deben utilizar ninguno de los puertos que se indican a continuación.
Asegúrese de configurar los cortafuegos de su red de forma para permitir la comunicación a través de los puertos indicados a continuación.

Máquina cliente (ESET Management Agent) o proxy HTTP Apache

Protocolo	Puerto	Descripciones
TCP	2222	Comunicación entre las instancias de ESET Management Agent y ESET PROTECT Server
TCP	80	Conexión con el repositorio de ESET
MQTT	8883, 443	ESET Push Notification Service: llamadas de activación entre ESET PROTECT Server y ESET Management Agent, el puerto de conmutación por error es el 443.
TCP	3128	Comunicación con el proxy HTTP Apache
TCP	443	Comunicación con ESET LiveGuard Advanced (solo proxy)

ESET Management Agent: puertos usados para la implementación remota en un ordenador de destino con el sistema operativo Windows

Protocolo	Puerto	Descripciones
TCP	139	Uso del recurso compartido ADMIN$
TCP	445	Acceso directo a recursos compartidos utilizando TCP/IP durante la instalación remota (una alternativa a TCP 139)
UDP	137	Resolución del nombre durante la instalación
UDP	138	Explorar durante la instalación remota

Máquina Consola web de ESET PROTECT (si no es la misma que la máquina ESET PROTECT Server)

Protocolo	Puerto	Descripciones
TCP	2223	Comunicación entre ESET PROTECT Web Console y ESET PROTECT Server, empleada para la instalación asistida por el servidor.
TCP	443/80	Tomcat que difunde la Consola web
TCP	443	Fuente RSS noticias de soporte: • https://era.welivesecurity.com:443 • https://support.eset.com:443/rss/news.xml

Máquina de ESET PROTECT Server

Protocolo	Puerto	Descripciones
TCP	2222	Comunicación entre ESET Management Agent y ESET PROTECT Server
TCP	80	Conexión con el repositorio de ESET
MQTT	8883	ESET Push Notification Service: llamadas de activación entre ESET PROTECT Server y ESET Management Agent
TCP	2223	Resolución de DNS y conmutación por error MQTT
TCP	3128	Comunicación con el proxy HTTP Apache
TCP	1433 (MS SQL) 3306 (MySQL)	Conexión con una base de datos externa (solo si la base de datos está en otra máquina)
TCP	389	Sincronización LDAP; abra este puerto también en su controlador de AD
UDP	88	Tickets de Kerberos (solo se aplica al dispositivo virtual de ESET PROTECT)

Sensor de detección de acceso no autorizado (RD Sensor)

Protocolo	Puerto	Descripciones
TCP	22, 139	Detección de sistemas operativos mediante los protocolos SMB (TCP 139) y SSH (TCP 22).
UDP	137	Resolución del nombre de host del ordenador mediante NetBIOS.

Máquina de ESET PROTECT MDC

Protocolo	Puerto	Descripciones
TCP	9977 9978	Comunicación **interna** entre Conector del dispositivo móvil y ESET Management Agent
TCP	9980	Inscripción de dispositivo móvil
TCP	9981	Comunicación del dispositivo móvil
TCP	2195	Envío de notificaciones al servicio de notificaciones push de Apple (*gateway.push.apple.com*) hasta la versión de ESMC 7.2.11.1
TCP	2196	Servicio de comentarios de Apple (*feedback.push.apple.com*) hasta la versión de ESMC 7.2.11.1
HTTPS	2197	• Comentarios y notificaciones push de Apple (*api.push.apple.com*) ESMC 7.2.11.3 y posteriores
TCP	2222	Comunicación (replicación) entre ESET Management Agent, MDC and ESET PROTECT Server
TCP	1433 (MS SQL) 3306 (MySQL)	Conexión con una base de datos externa (solo si la base de datos está en otra máquina)

Dispositivo administrado mediante MDM

Protocolo	Puerto	Descripciones
TCP	9980	Inscripción de dispositivo móvil
TCP	9981	Comunicación del dispositivo móvil
TCP	5223	Comunicación externa con el servicio de notificaciones push de Apple (iOS)
TCP	443	• Restauración de Wi-Fi únicamente cuando los dispositivos no llegan a APN en el puerto 5223 (iOS) • Conexión de dispositivo Android al servidor GCM. • Conexión al portal de licencias de ESET • ESET LiveGrid® (Android) (entrante: *https://i1.c.eset.com*; saliente: *https://i3.c.eset.com*) • Información estadística anónima para el laboratorio de investigación de ESET (Android) (*https://ts.eset.com*) • Clasificación de aplicaciones instaladas en el dispositivo; Se usa para el Control de aplicaciones cuando se ha definido el bloqueo de algunas categorías de aplicaciones. (Android) (*https://play.eset.com*) • Envío de solicitud de soporte con la función Enviar una solicitud de soporte (Android) (*https://suppreq.eset.eu*)

Protocolo	Puerto	Descripciones
TCP	5228 5229 5230	Envío de notificaciones a Google Cloud Messaging (Android)* Envío de notificaciones a Firebase Cloud Messaging (Android)*
TCP	80	• Actualización de módulos (Android) (*http://update.eset.com*) • Solo se usa en la versión web;. Información sobre la actualización a la versión más reciente de la aplicación y descarga de una nueva versión (Android) (*http://go.eset.eu*)

* El servicio GCM (Google Cloud Messaging) está obsoleto y se eliminó el 11 de abril de 2019. Se ha sustituido por FCM (Firebase Cloud Messaging). MDM v7 sustituyó el servicio GCM por el servicio FCM en esta fecha; solo tiene que permitir la comunicación para el servicio FCM.

Los puertos predefinidos 2222 y 2223 se pueden cambiar si es necesario.

Proceso de instalación

La guía de instalación abarca varios métodos para instalar ESET PROTECT y está destinada principalmente a los clientes empresariales. Consulte la guía para pequeñas y medianas empresas si desea instalar ESET PROTECT en una plataforma Windows para administrar hasta 250 productos ESET Endpoint para Windows. Para obtener instrucciones para actualizar su instalación de ESET PROTECT existente, consulte Procedimientos de actualización.

Los instaladores de ESET PROTECT están disponibles en la sección Descargar ESET PROTECT del sitio web de ESET. Los ofrecemos en varios formatos para permitir distintos métodos de instalación. De forma predeterminada se selecciona la ficha **Instalador todo en uno**. Para descargar un VA o un instalador independiente, haga clic en la ficha correspondiente. Están disponibles las descargas siguientes:

- El paquete del instalador todo en uno de ESET PROTECT para Windows en formato comprimido.
- Una imagen ISO que contiene todos los instaladores de ESET PROTECT (excepto los dispositivos virtuales de ESET PROTECT).
- Dispositivos virtuales (archivos OVA). Se recomienda la implementación del dispositivo virtual de ESET PROTECT a los usuarios que deseen ejecutar ESET PROTECT en un entorno virtualizado o que prefieran una instalación más sencilla. Consulte la Guía de implementación del dispositivo virtual de ESET PROTECT completa para acceder a instrucciones paso a paso.
- Instaladores individuales para cada componente: para las plataformas Windows y Linux.

Métodos de instalación adicionales:

- Instalación en Microsoft Azure
- Instrucciones de instalación para Linux paso a paso

No cambie el nombre del ordenador del equipo ESET PROTECT Server después de la instalación. Consulte Cambiar la dirección IP o el nombre de host en ESET PROTECT Server para obtener más información.

Si quiere decidir qué tipo de instalación de ESET PROTECT es apta para su entorno, consulte la siguiente tabla de decisión, le ayudará a tomar la mejor decisión posible: Por ejemplo:

- No utilice una conexión a Internet lenta para ESET PROTECT en la nube.
- Si es una pyme, seleccione el instalador todo en uno.

Consulte también Dimensionamiento de hardware e infraestructura.

Método de instalación	Tipo de cliente		Migración		Entorno para la instalación de ESET PROTECT					Conexión a Internet		
	Pyme	Gran empresa	Sí	No	Sin servidor	Servidor dedicado	Servidor compartido	Plataforma de virtualización	Servidor en la nube	Ninguno	Bueno	Malo
Todo en uno en Windows Server	✓	✓	✓			✓	✓		✓	✓	✓	✓
Todo en uno en Windows Desktop	✓		✓		✓					✓	✓	✓
Dispositivo virtual	✓		✓					✓		✓	✓	✓
Máquina virtual de Microsoft Azure	✓			✓					✓		✓	
Componente Linux		✓	✓			✓	✓		✓	✓	✓	✓
Componente Windows		✓	✓			✓	✓		✓	✓	✓	✓

Instalación todo en uno en Windows

Puede instalar ESET PROTECT de varias maneras. Seleccione el tipo de instalación que se adapte mejor a sus necesidades y entorno. El método más sencillo es utilizar el instalador todo en uno de ESET PROTECT. Este método permite instalar ESET PROTECT y sus componentes en una única máquina.

La instalación de componentes le permite personalizar la instalación e instalar cada componente de ESET PROTECT en un ordenador independiente, siempre que cumpla los requisitos del sistema.

Puede instalar ESET PROTECT utilizando:

- La instalación del paquete todo en uno de ESET PROTECT Server, Proxy HTTP Apache o Conector del dispositivo móvil
- Instaladores independientes para componentes de ESET PROTECT (instalación de componentes)

Entre las situaciones de instalación personalizada se incluyen:

- Instalación con certificados personalizados
- Instalación en un clúster de conmutación por error

En numerosas situaciones de instalación, es necesario instalar los diferentes componentes de ESET PROTECT en diferentes máquinas para dar cabida a arquitecturas de red, cumplir con los requisitos de rendimiento, o por otras razones. Los siguientes paquetes de instalación están disponibles para componentes de ESET PROTECT individuales:

Instalación de componentes principales

- ESET PROTECT Server
- ESET PROTECT Web Console – Puede seleccionar la instalación de ESET PROTECT Web Console en un ordenador distinto al ordenador donde se ha instalado ESET PROTECT Server.
- ESET Management Agent (debe estar instalado en los ordenadores cliente, opcional en ESET PROTECT Server)

Instalación de componentes opcionales

- RD Sensor
- Conector del dispositivo móvil
- Proxy HTTP Apache
- Herramienta Mirror

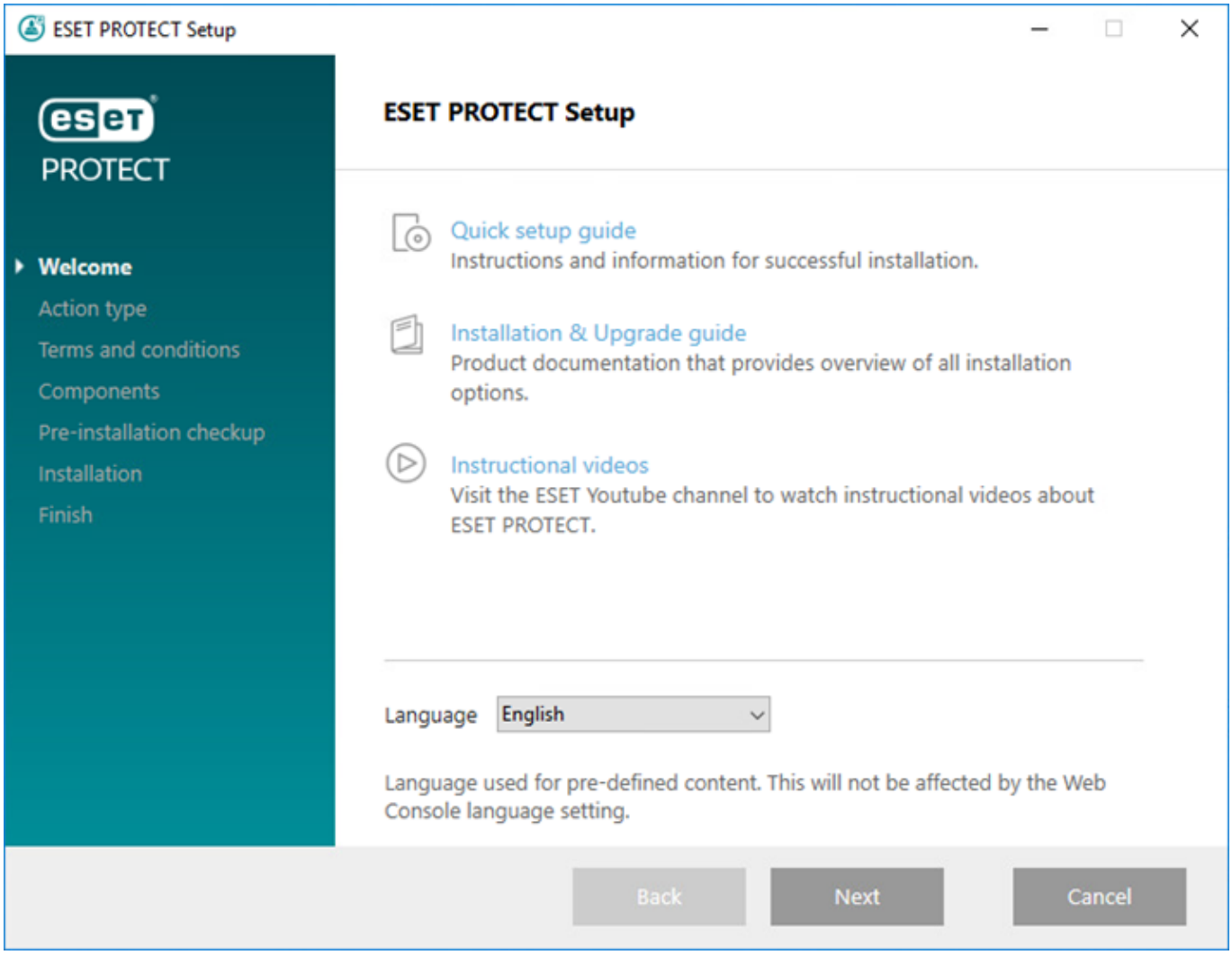
Consulte también Instalación todo en uno de ESET PROTECT.

Si desea obtener instrucciones sobre cómo actualizar ESMC a la versión ESET PROTECT 9.1 más reciente, consulte nuestros procedimientos de actualización.

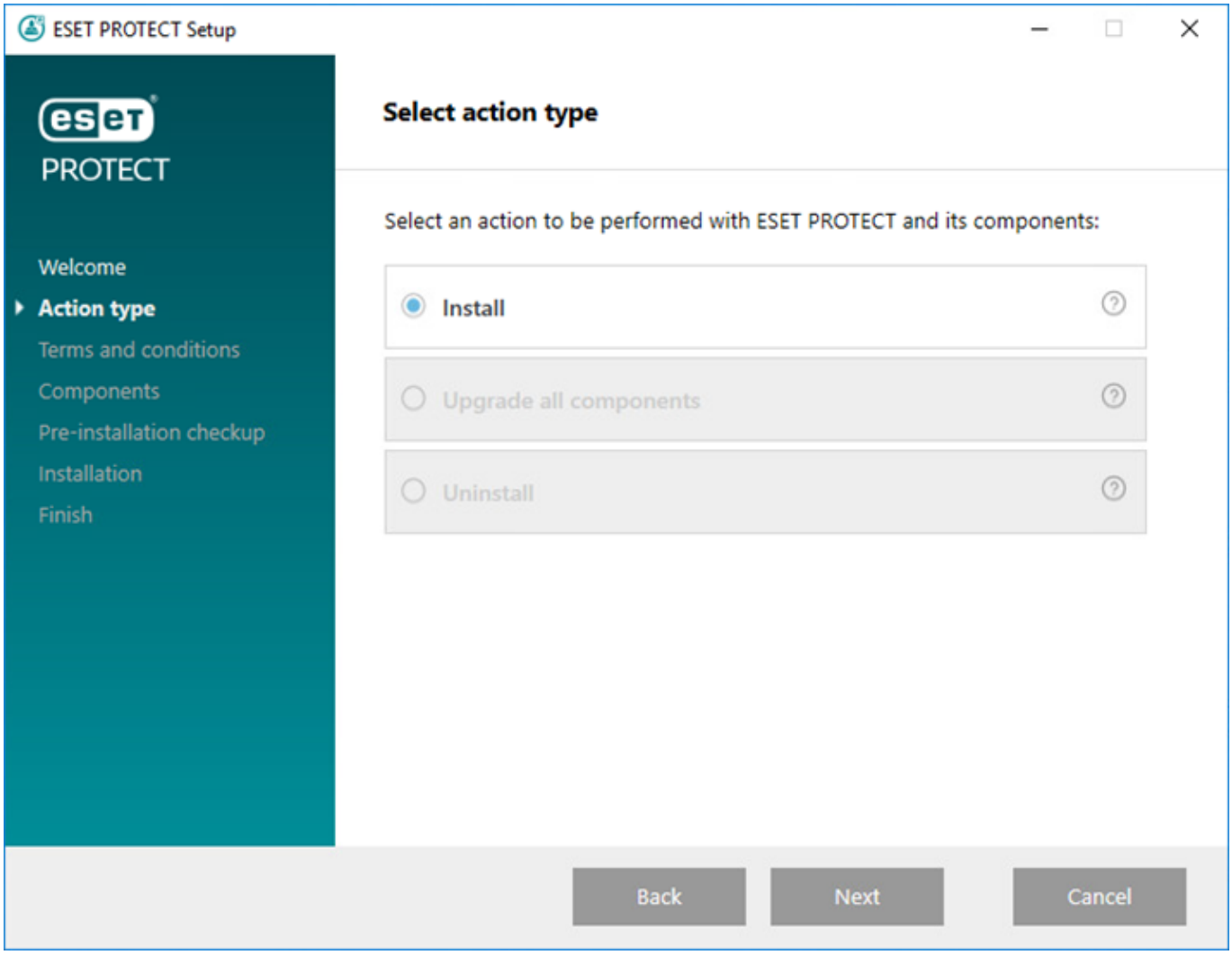
Instalar ESET PROTECT Server

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

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



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



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

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

Microsoft SQL Server Express

- El instalador todo en uno de ESET PROTECT 9.1 instala Microsoft SQL Server Express 2019 de forma predeterminada.
  - Si utiliza una versión anterior de Windows (Server 2012 o SBS 2011), Microsoft SQL Server Express 2014 se instalará de forma predeterminada.
  - El instalador genera automáticamente una contraseña aleatoria para la autenticación de la base de datos (almacenada en *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

Microsoft SQL Server Express tiene un límite de tamaño de 10 GB en cada base de datos relacional. No recomendamos el uso de Microsoft SQL Server Express:
- En entornos empresariales o redes de gran tamaño.
- Si desea usar ESET PROTECT con ESET Inspect.

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

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

Agregar certificado HTTPS personalizado para la consola web

- Seleccione esta opción si desea usar un certificado HTTPS personalizado para ESET PROTECT Web Console.

- Si no selecciona esta opción, el instalador genera automáticamente un nuevo almacén de claves para Tomcat nuevo (un certificado HTTPS autofirmado).

Proxy HTTP Apache

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

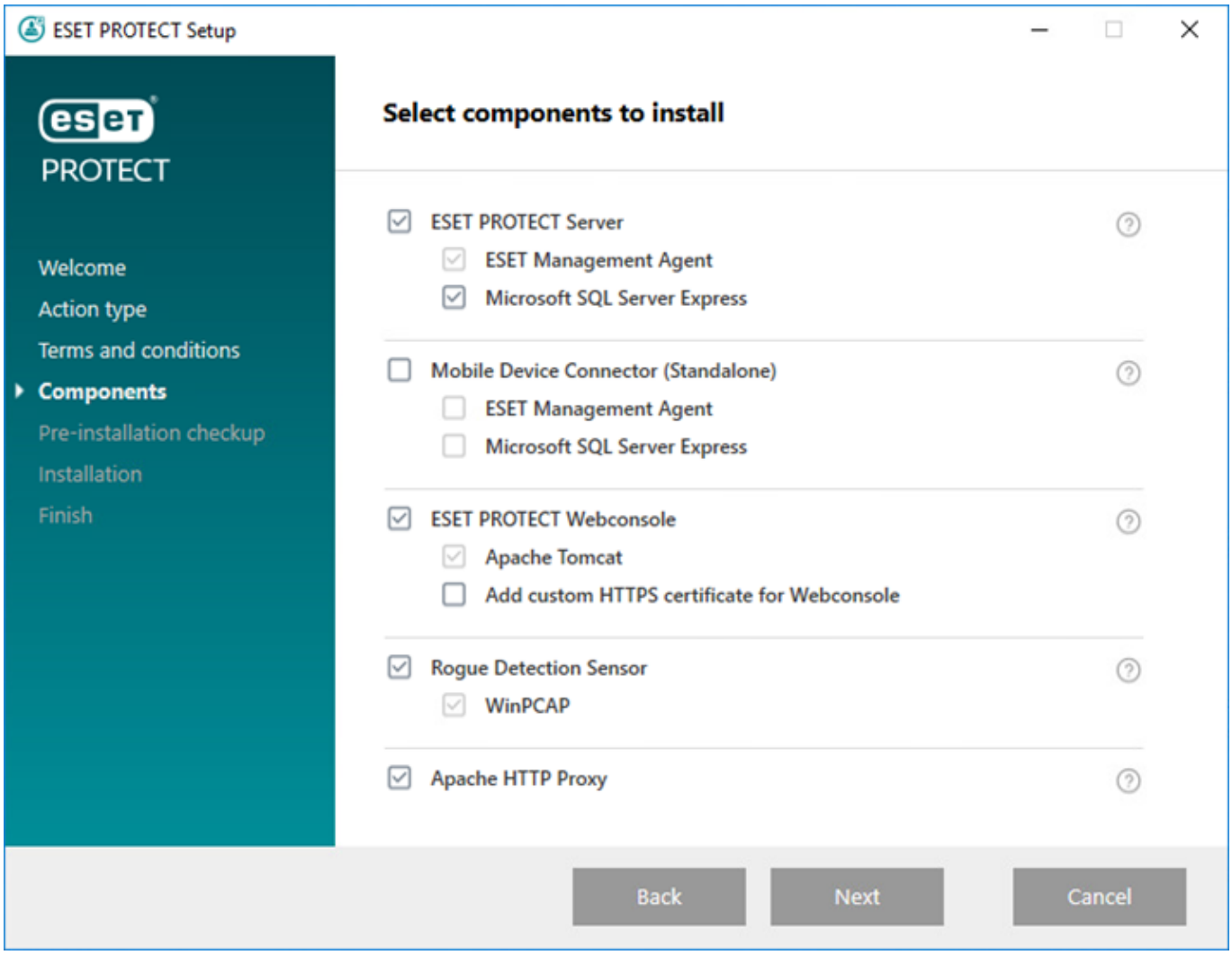
- El uso del proxy HTTP puede ahorrar gran cantidad de ancho de banda en los datos descargados de Internet y mejorar las velocidades de descarga de las actualizaciones de los productos. Le recomendamos que marque la casilla de verificación situada junto a **Proxy HTTP Apache** si va a administrar más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

- Para obtener más información, consulte ¿Qué es el proxy HTTP Apache? y Diferencias entre el proxy HTTP Apache, la herramienta Mirror y la conectividad directa.

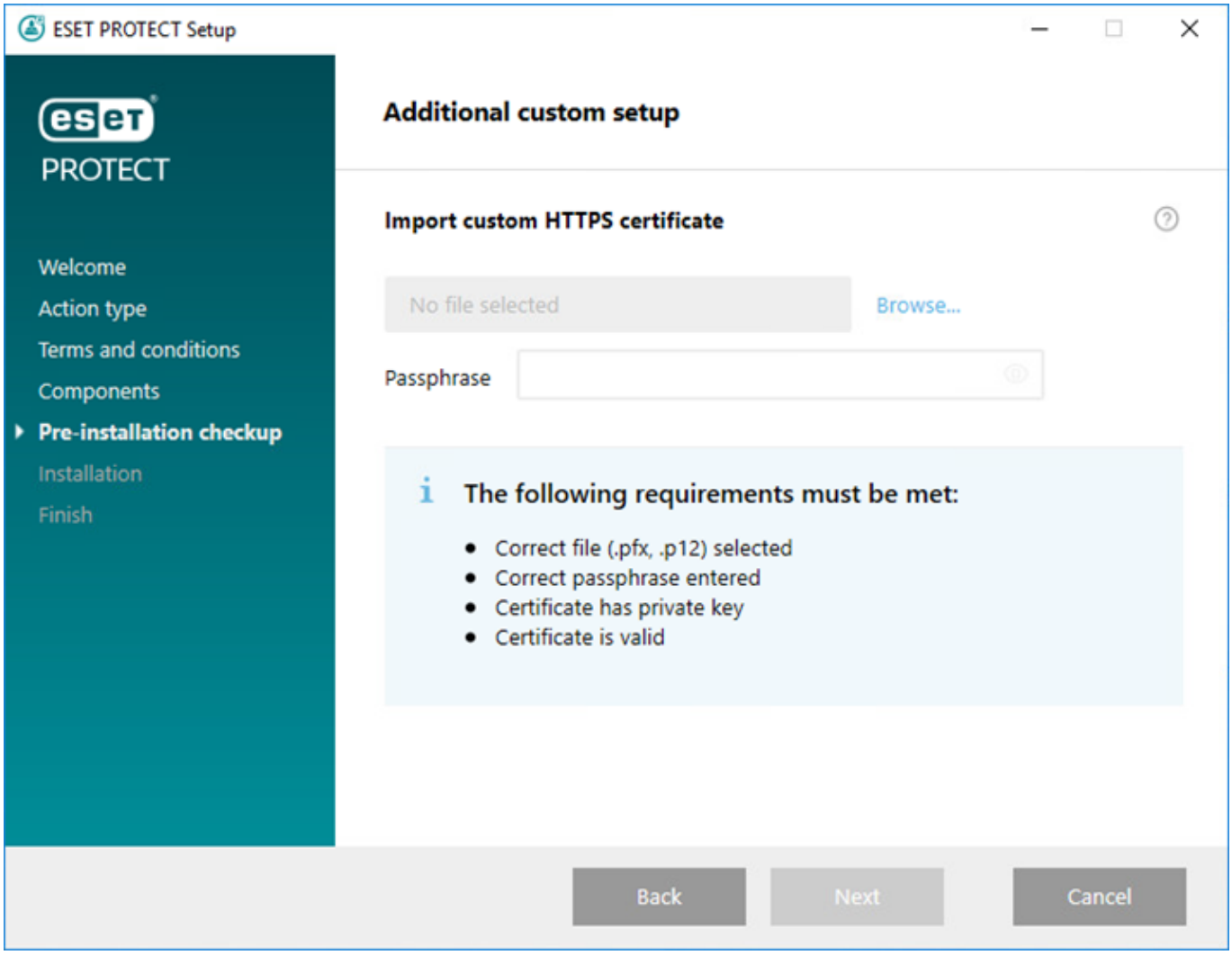
- Seleccione **Proxy HTTP Apache** para instalar el proxy HTTP Apache y crear y aplicar políticas (por ejemplo, **Uso de proxy HTTP**, aplicada al grupo **Todos**) para los siguientes productos:

  - ESET Endpoint para Windows
  - ESET Endpoint para macOS (OS X) y Linux
  - ESET Management Agent
  - ESET File Security para Windows Server (6+)
  - ESET Server Security para Windows (8 o posterior)
  - Caché local compartida de ESET

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



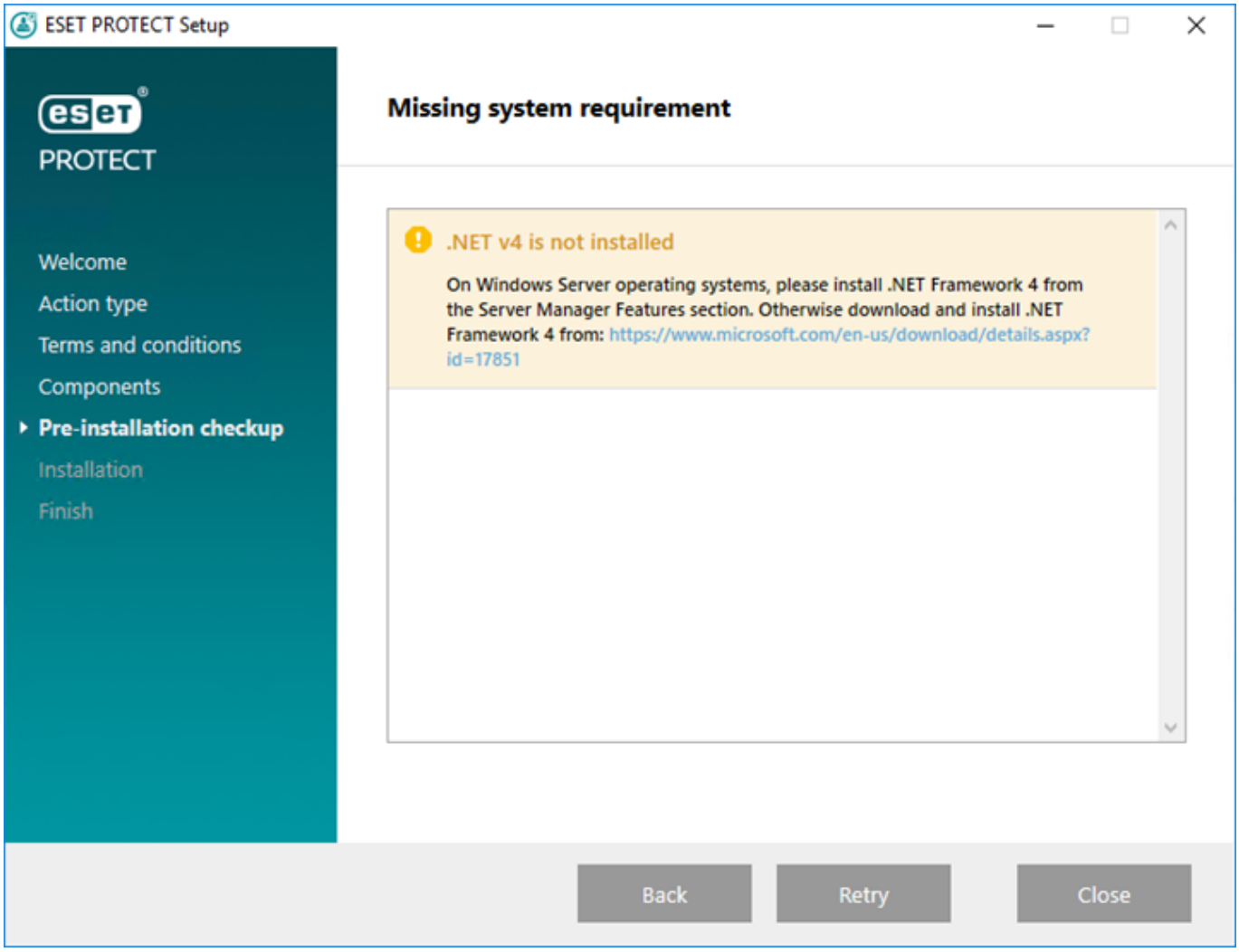
5. Si ha seleccionado **Agregar certificado HTTPS personalizado para la consola web**, haga clic en **Examinar**, seleccione un certificado válido (archivo *.pfx* o .p12) y escriba la **contraseña** (o deje el campo vacío si no hay contraseña). El instalador instalará el certificado para el acceso a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



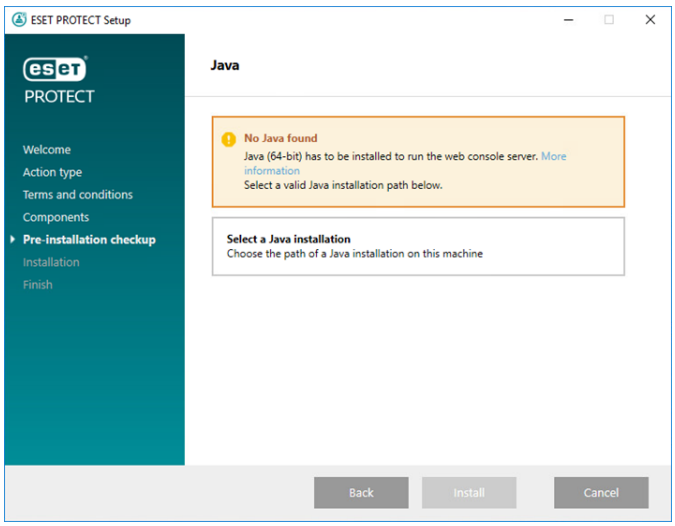
6. Si se encuentran errores durante los requisitos previos, abórdelos como corresponde. Asegúrese de que su sistema cumple con todos los requisitos previos.

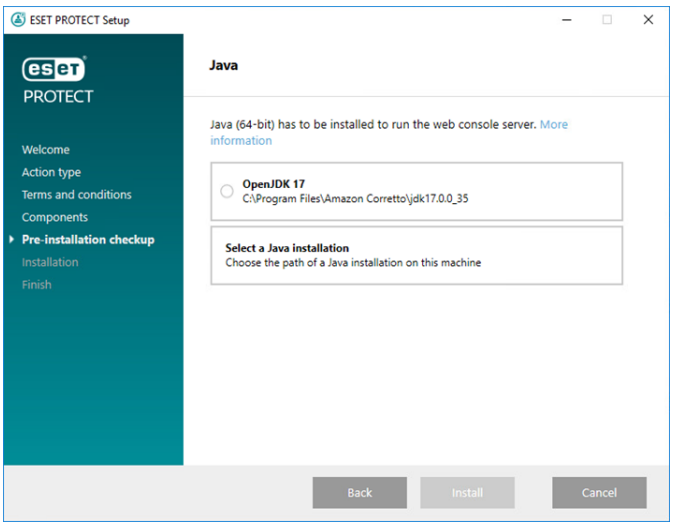
.NET v4 no está instalado

Instalar .NET Framework



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





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

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

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

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

El disco del sistema solo tiene 32 MB libres

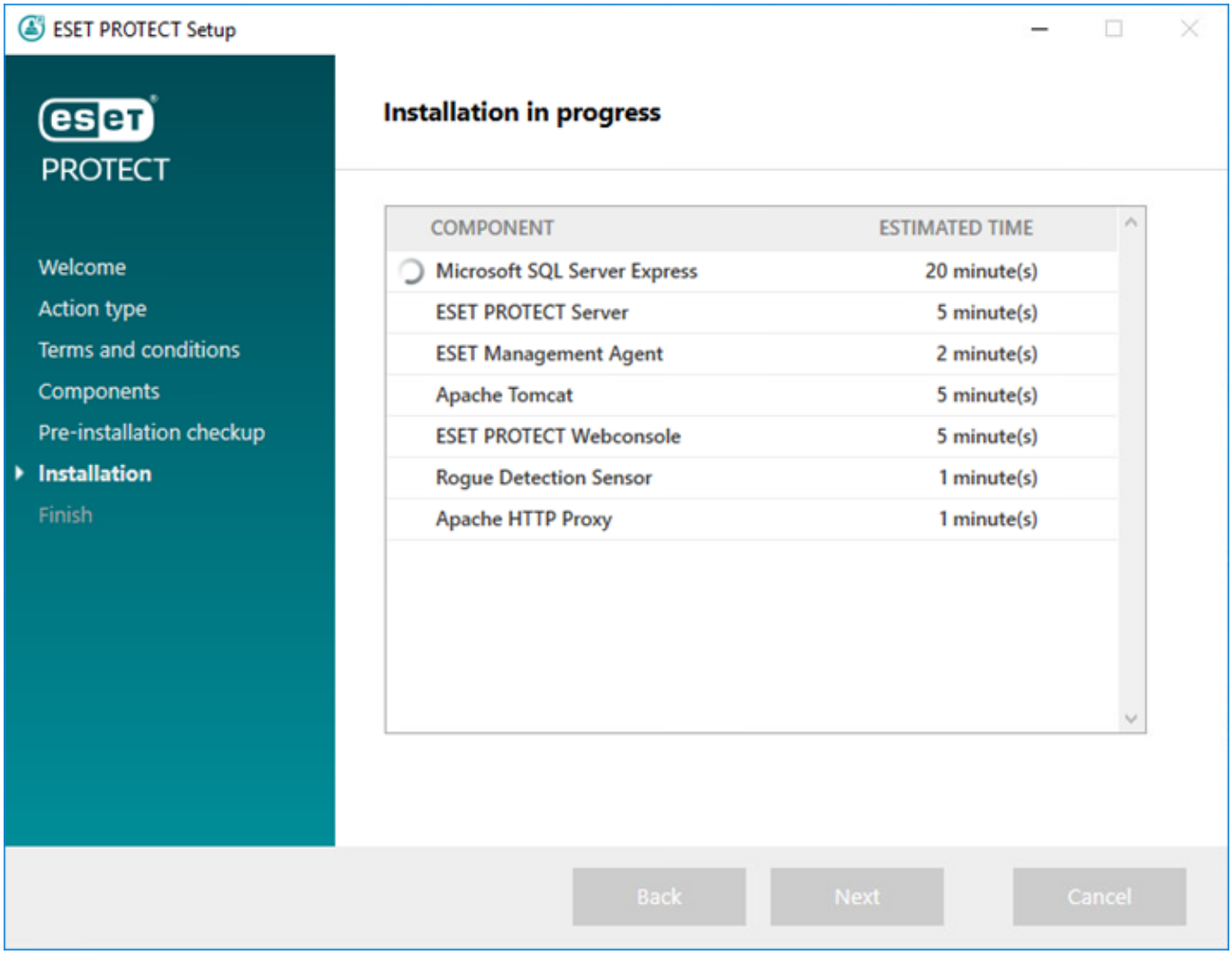
- El instalador puede mostrar esta notificación si su sistema no tiene espacio en disco suficiente para la instalación de ESET PROTECT.
- Para instalar ESET PROTECT y todos sus componentes, debe tener al menos 4.400 MB de espacio libre en el disco.

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

La actualización directa no es compatible; consulte Migración desde ERA 5.x o Actualización desde ERA 6.x.

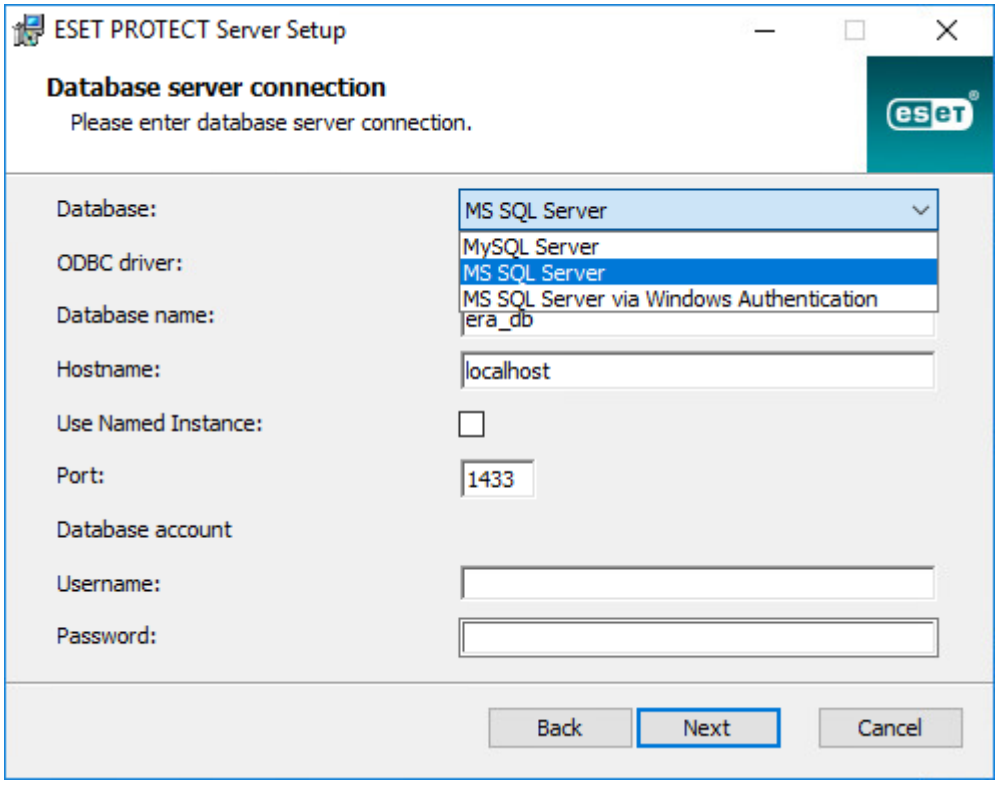
7. Cuando finalice la comprobación de los requisitos previos y su entorno cumpla todos los requisitos, se iniciará la instalación. Tenga en cuenta que la instalación puede durar más de una hora, en función del sistema y la configuración de red.

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



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

Configurar la conexión con SQL/MySQL Server

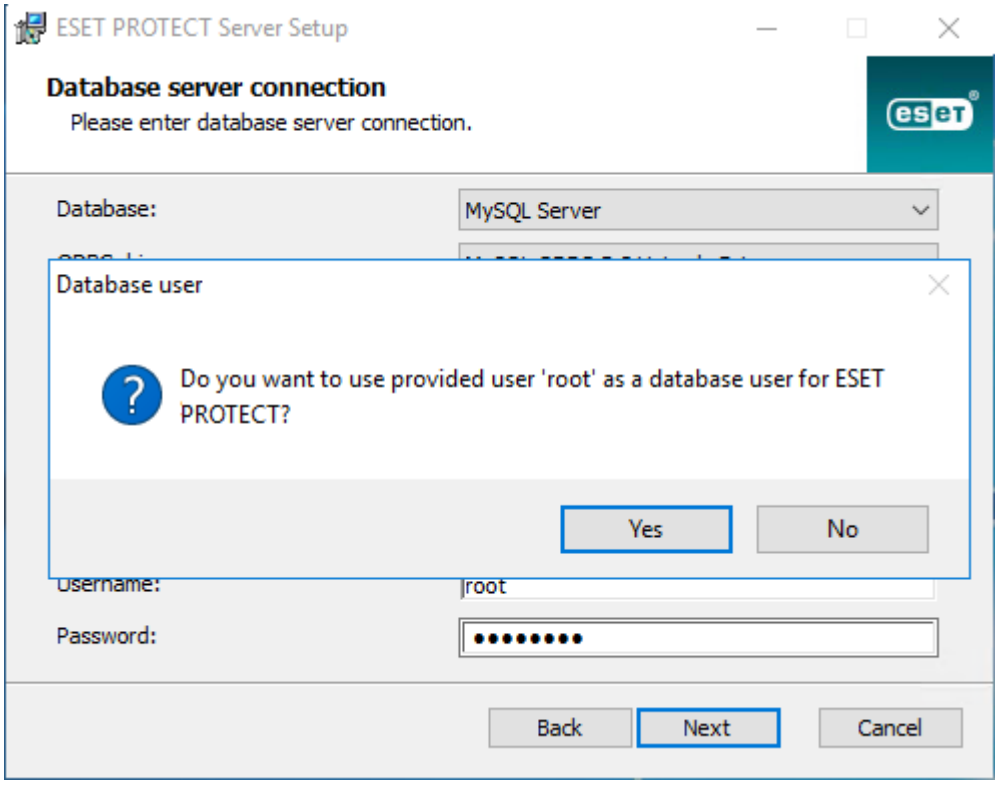


Introduzca el **Nombre de la base de datos**, **Nombre de host**, número de **Puerto** (puede encontrar esta información en el administrador de configuración de Microsoft SQL Server) y los detalles de la **cuenta de la base de datos** (**nombre de usuario** y **contraseña**) en los campos correspondientes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

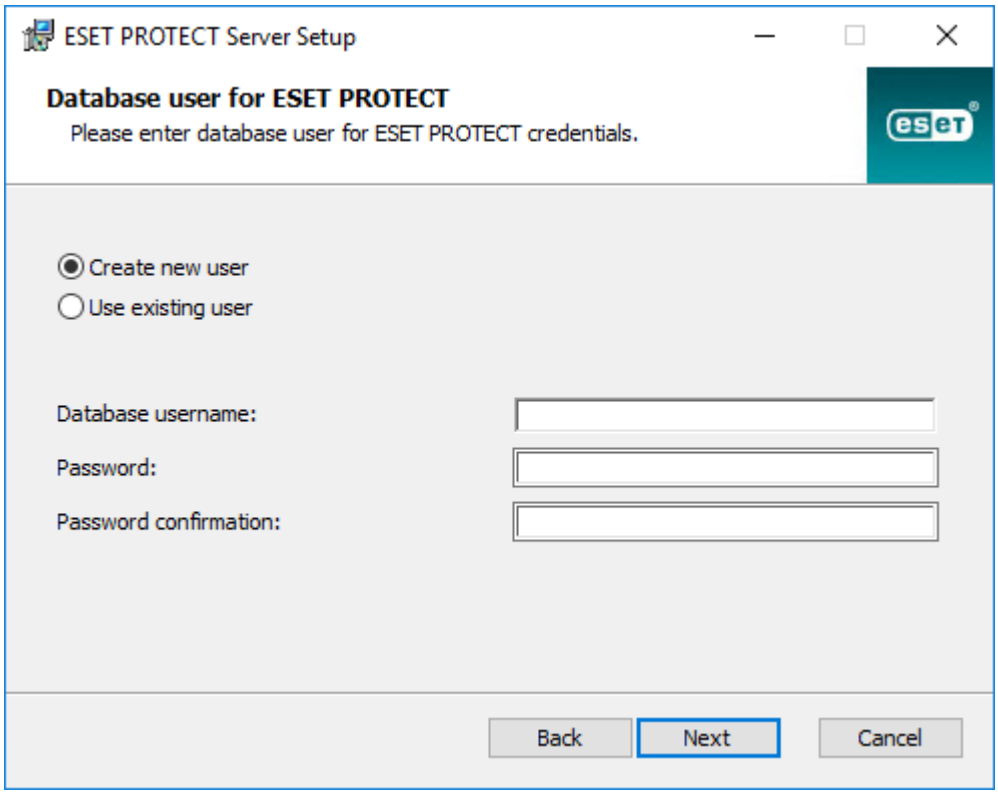
Usar instancia con nombre: si está utilizando una base de datos de MS SQL, también puede marcar la casilla de verificación **Usar instancia con nombre** para usar una instancia de la base de datos personalizada. Puede configurarlo en el campo **Nombre del host** con el formato *NOMBRE_HOST\INSTANCIA_BD* (por ejemplo, *192.168.0.10\ESMC7SQL*). Para las bases de datos en clústeres utilice únicamente el nombre de clúster. Si se selecciona esta opción, no podrá cambiar el puerto de conexión de la base de datos; el sistema utilizará los puertos predeterminados que Microsoft ha definido. Para conectar ESET PROTECT Server a la base de datos de MS SQL instalada en un clúster de conmutación por error, escriba el nombre del clúster en el campo **Nombre del host**.

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

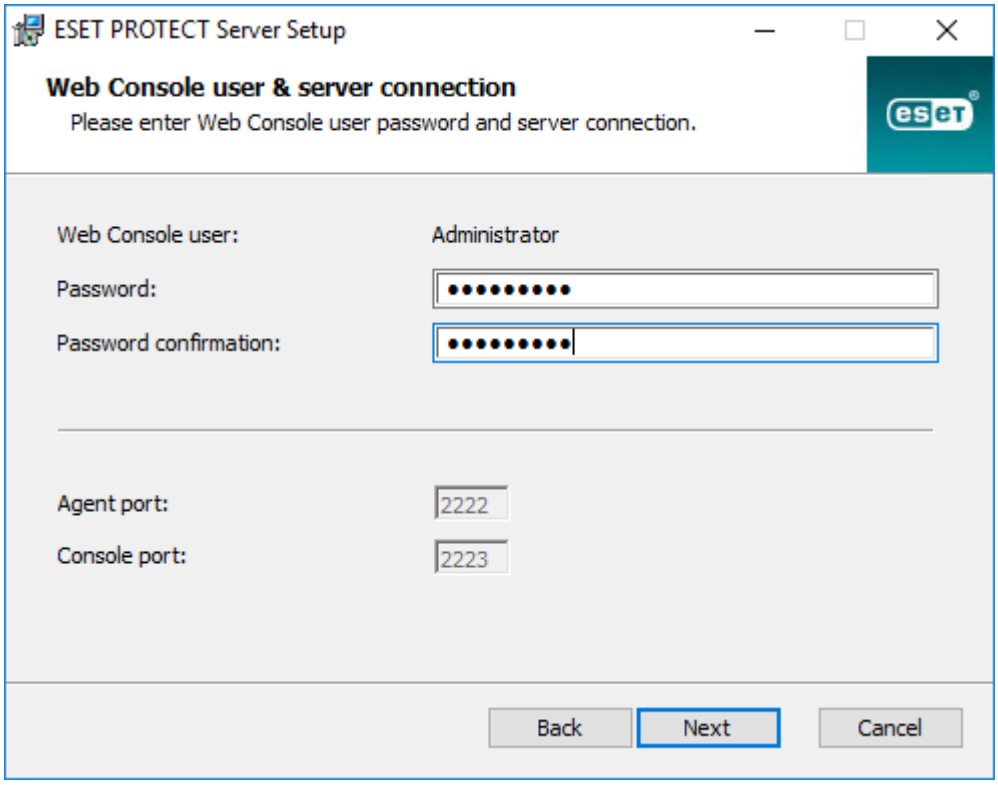
Si introdujo una **cuenta de SA** o una **cuenta raíz** en la ventana anterior, haga clic en **Sí** para continuar utilizando la cuenta SA/raíz como usuario de la base de datos de ESET PROTECT.



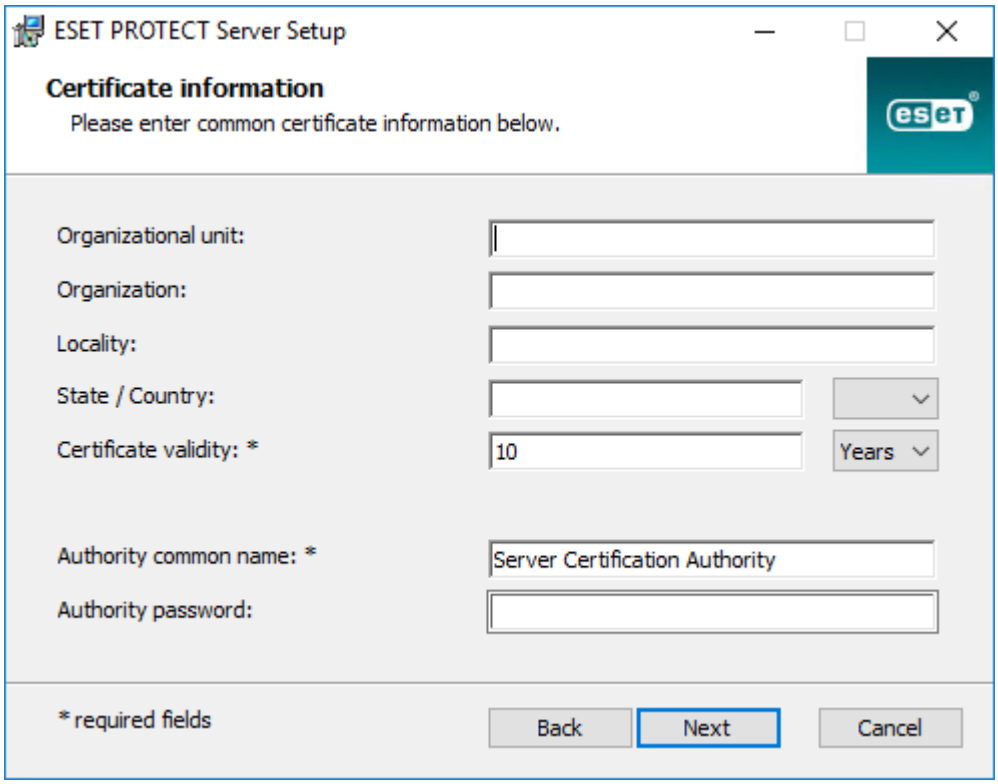
Si hace clic en **No**, deberá seleccionar **Crear usuario nuevo** (si aún no lo ha creado) o **Utilizar usuario existente** (si tiene una cuenta de usuario de base de datos dedicada).



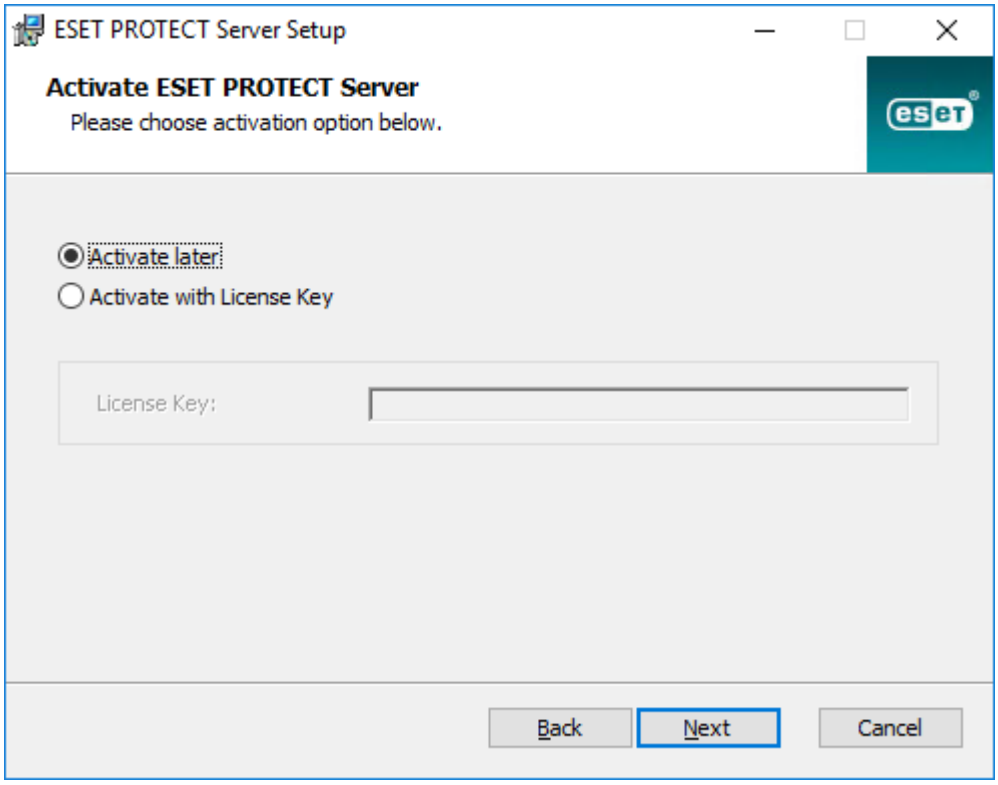
9. El instalador le pedirá que introduzca una contraseña para la cuenta de administrador de Web Console. Esta contraseña es importante, ya que la utilizará para iniciar sesión en ESET PROTECT Web Console. Haga clic en **Siguiente**.



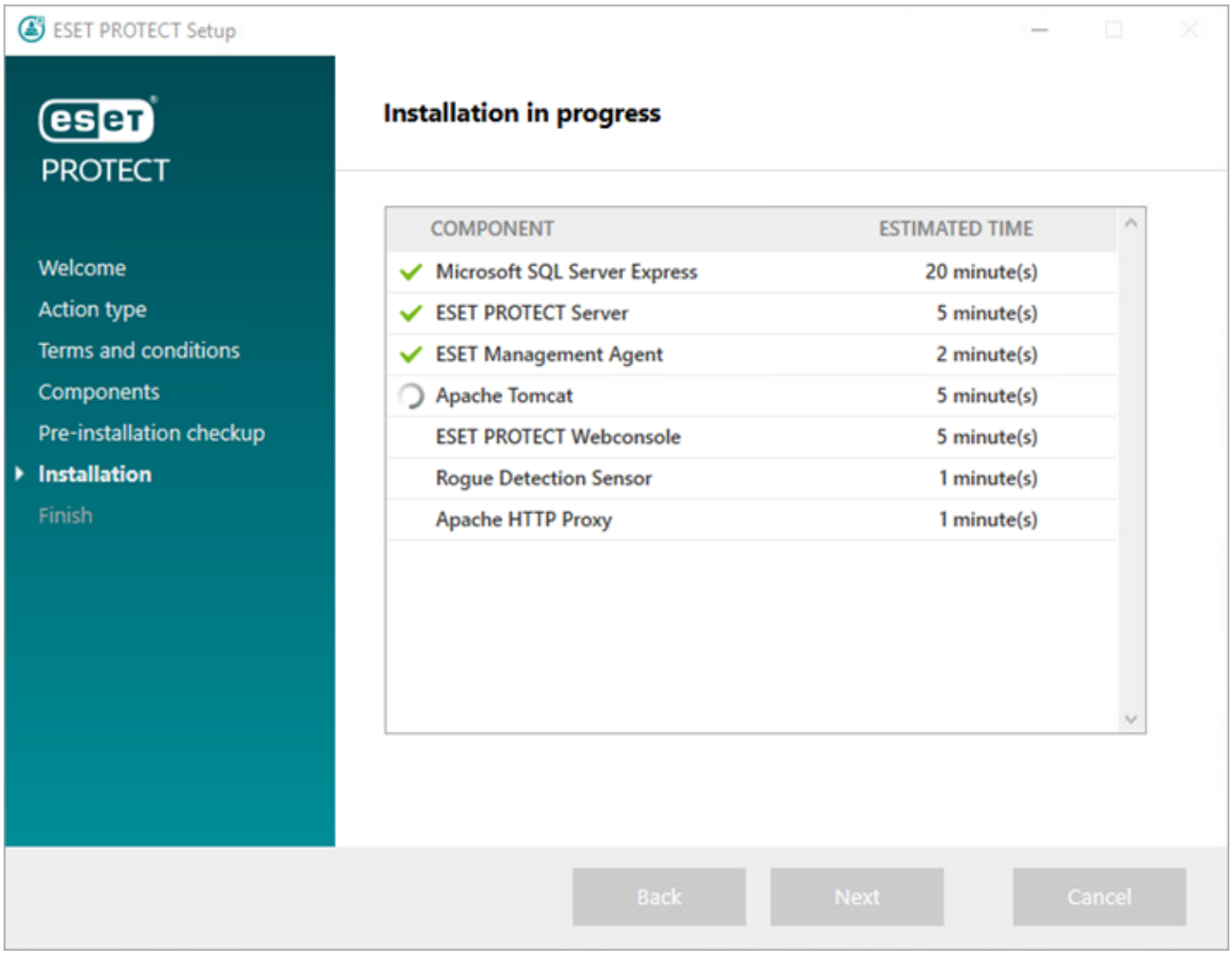
10. Deje los campos como están o escriba su información corporativa para que aparezca en los detalles de los certificados de ESET Management Agent y ESET PROTECT Server. Si decide introducir una contraseña en el campo **Contraseña de la autoridad**, asegúrese de recordarla. Haga clic en **Siguiente**.



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



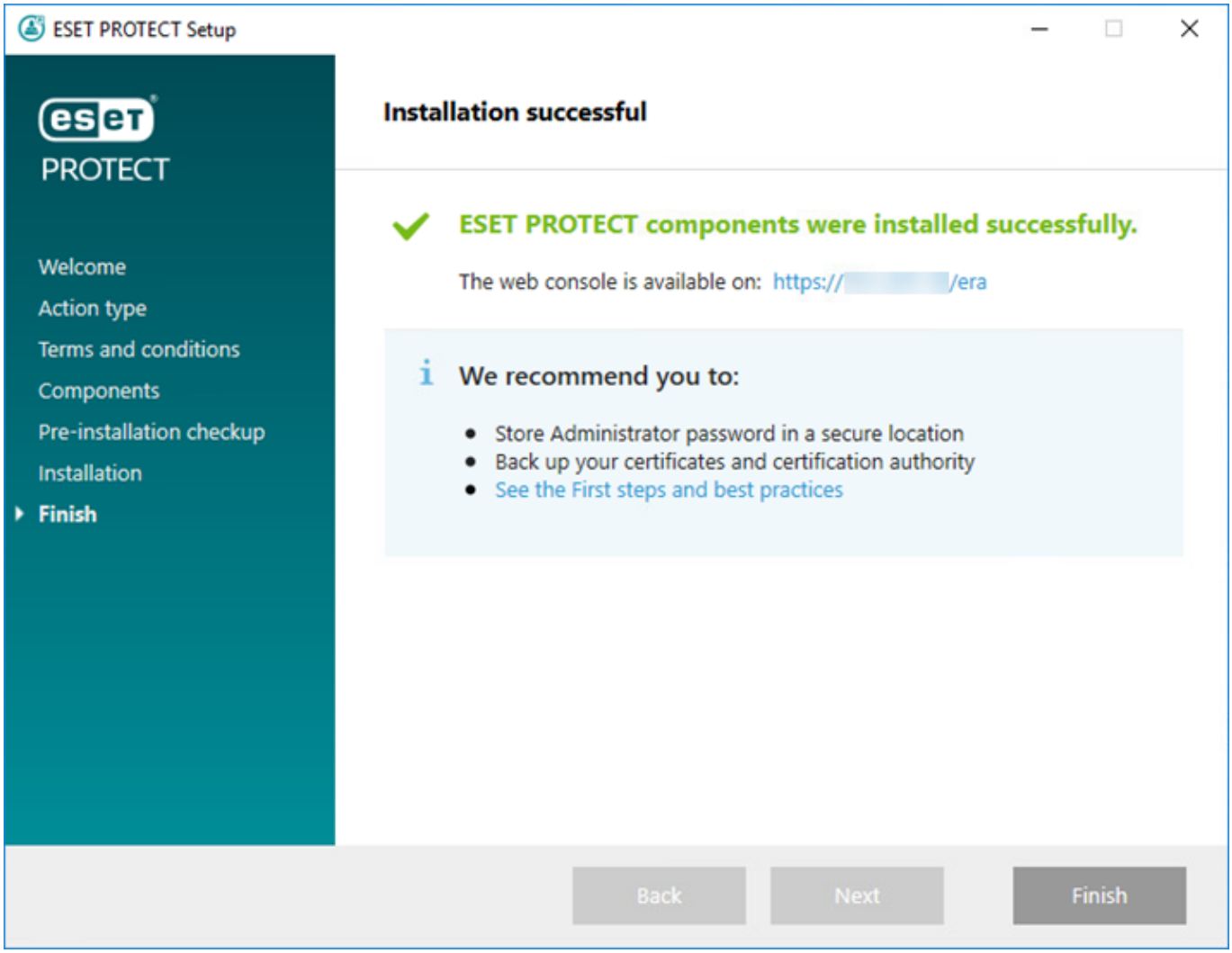
12. Verá el progreso de la instalación.



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

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

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



Si la instalación no finaliza correctamente:

- Revise los archivos de registro de la instalación en el paquete de instalación todo en uno. El directorio de registros es el mismo que el directorio del instalador todo en uno, por ejemplo: `C:\Users\Administrator\Downloads\x64\logs\`

- Consulte Resolución de problemas para conocer los pasos adicionales para resolver su problema.

Instalación del Conector del dispositivo móvil ESET PROTECT (independiente)

Para instalar el Conector del dispositivo móvil como herramienta independiente en un ordenador diferente al de ESET PROTECT Server, siga los pasos que se indican a continuación.

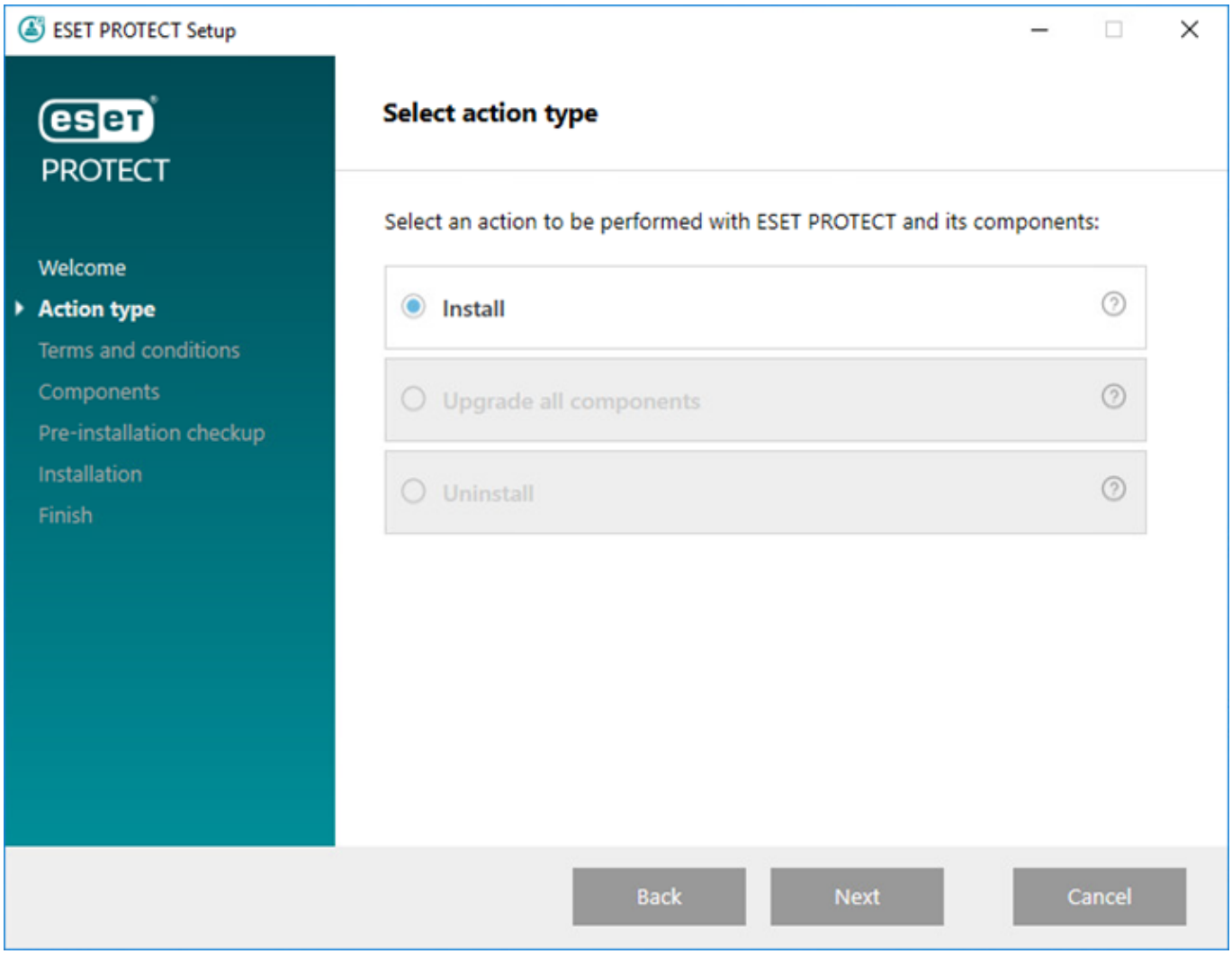
el Conector del dispositivo móvil debe estar disponible a través de Internet para que los dispositivos móviles pueden administrarse en todo momento independientemente de su ubicación.

Tenga en cuenta que un dispositivo móvil se comunica con el Conector del dispositivo móvil, lo que inevitablemente afecta al uso de datos móviles. Esto se aplica especialmente a la itinerancia.

Para instalar el Conector del dispositivo móvil en Windows, siga los pasos indicados a continuación:

1. Lea los requisitos previos en primer lugar y asegúrese de que se cumplan todos.

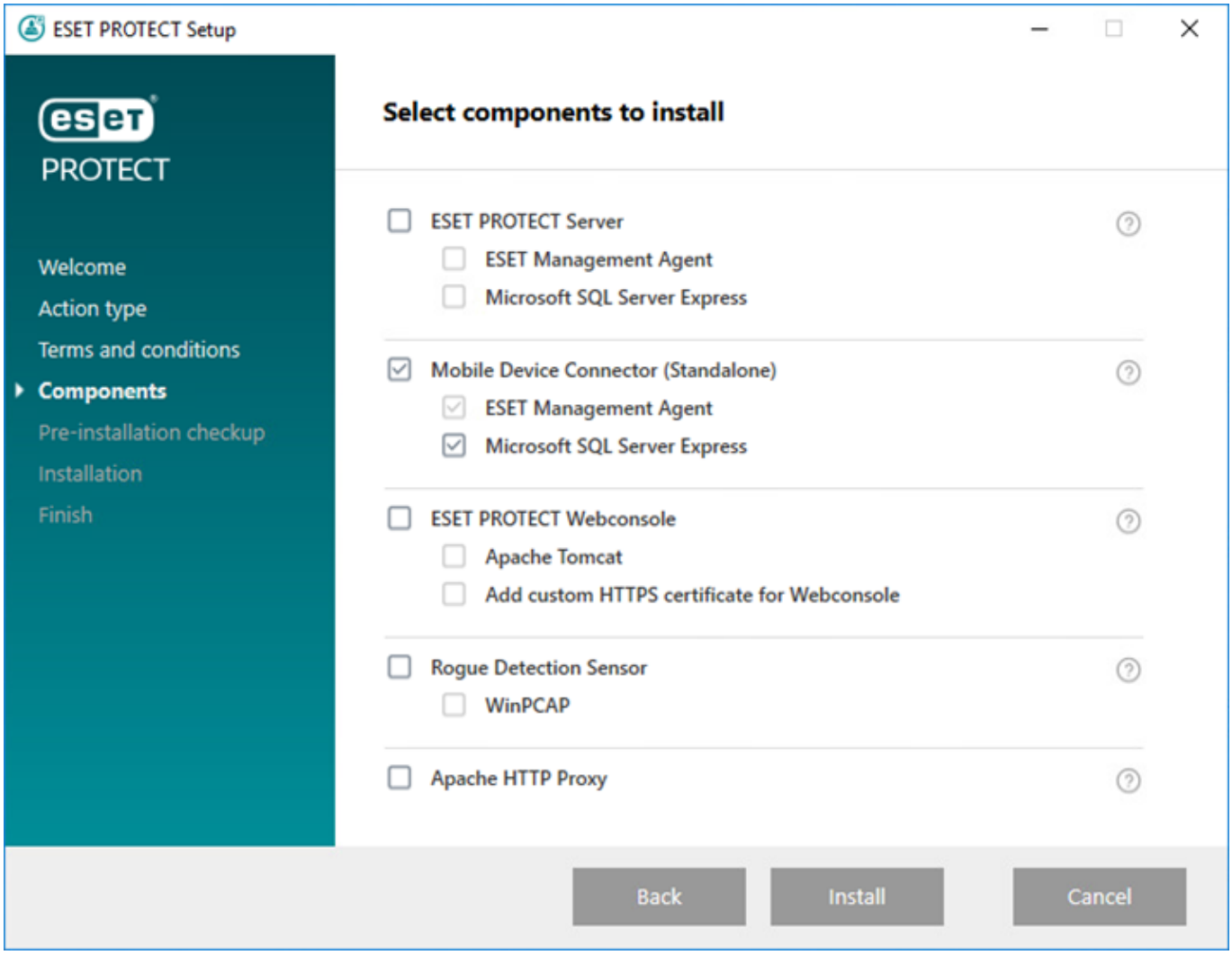
2. Haga doble clic en el paquete de instalación para abrirlo, seleccione **Instalar** y haga clic en **Siguiente**.



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

4. Tras aceptar el EULA, haga clic en **Siguiente**.

5. Seleccione únicamente la casilla de verificación situada junto a **Mobile Device Connector (Independiente)**. El Conector del dispositivo móvil ESET PROTECT necesita una **base de datos** para que funcione. Seleccione **Microsoft SQL Server Express** si desea instalar la base de datos o deje la casilla de verificación vacía. Si le gustaría conectarse a una base de datos existente, tendrá la opción de hacerlo durante la instalación. Haga clic en **Instalar** para continuar con el proceso de instalación.



6. Si ha instalado la base de datos como parte de esta instalación en el paso 5, la base de datos se instalará automáticamente y podrá omitir el paso 8. Si ha decidido no instalar una base de datos en el paso 5, se le solicitará que conecte el componente MDM a su base de datos existente.

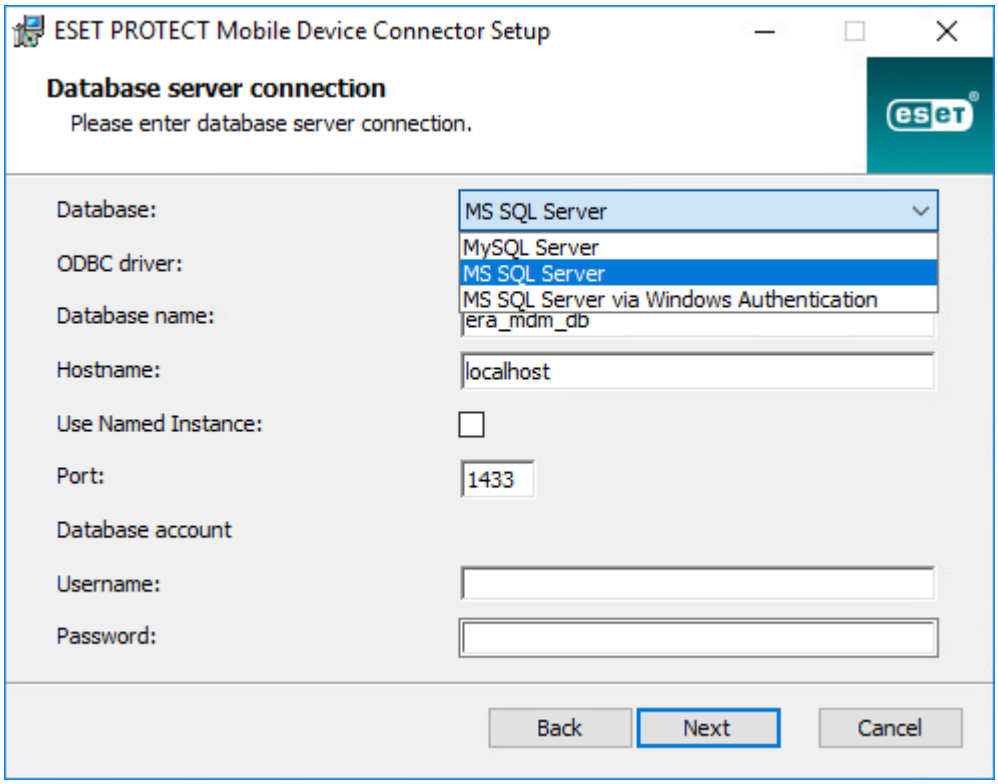
> Puede utilizar el mismo servidor de bases de datos que está utilizando para la base de datos de ESET PROTECT, pero le recomendamos utilizar un servidor de bases de datos distinto, si tiene previsto inscribir más de 80 dispositivos móviles.

7. El instalador debe conectarse a una base de datos existente que utilizará el Conector del dispositivo móvil. Especifique los siguientes datos de conexión:

- **Base de datos**: MySQL Server/MS SQL Server/MS SQL Server mediante autenticación de Windows
- **Controlador de ODBC**: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/MySQL ODBC 8.0 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 para SQL Server/ODBC Driver 13 para SQL Server/ODBC Driver 17 para SQL Server/ODBC Driver 18 para SQL Server
- **Nombre de la base de datos**: Se recomienda utilizar el nombre predefinido o cambiarlo si es necesario.
- **Nombre de host**: nombre del host o dirección IP del servidor de base de datos
- **Puerto**: se utiliza para conectar al servidor de base de datos

- **Nombre de usuario/Contraseña** de la cuenta admin de la base de datos

- **Usar instancia con nombre**: si está utilizando una base de datos de MS SQL, también puede marcar la casilla de verificación **Usar instancia con nombre** para usar una instancia de la base de datos personalizada. Puede configurarlo en el campo **Nombre del host** con el formato *NOMBRE_HOST**INSTANCIA_BD* (por ejemplo, *192.168.0.10**ESMC7SQL*). Para las bases de datos en clústeres utilice únicamente el nombre de clúster. Si se selecciona esta opción, no podrá cambiar el puerto de conexión de la base de datos; el sistema utilizará los puertos predeterminados que Microsoft ha definido. Para conectar ESET PROTECT Server a la base de datos de MS SQL instalada en un clúster de conmutación por error, escriba el nombre del clúster en el campo **Nombre del host**.

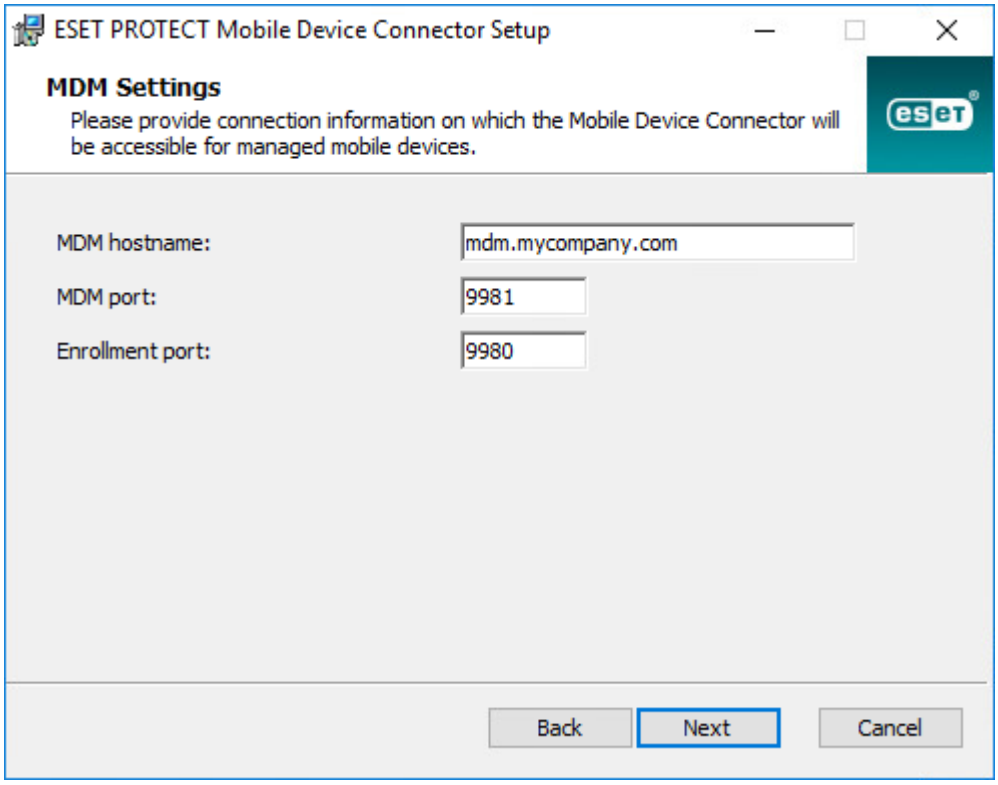


8. Si la conexión se realizó correctamente, se le solicitará que verifique que desea utilizar el usuario suministrado como usuario de la base de datos para ESET PROTECT MDM.

9. Después de que la nueva base de datos se haya instalado correctamente, o el instalador se haya conectado correctamente a la base de datos existente, puede continuar con la instalación de MDM. Especifique el **Nombre de host MDM**: este es el dominio público o la dirección IP pública de su servidor MDM, accesible para los dispositivos móviles desde Internet.

El nombre de host de MDM debe introducirse como aparece en su **certificado del servidor HTTPS**; de lo contrario, el dispositivo móvil iOS rechazará la instalación del perfil MDM. Por ejemplo, si se ha especificado una dirección IP en el certificado HTTPS, escriba esta dirección IP en el campo **Nombre de host MDM**. Si se especifica un FQDN (por ejemplo, `mdm.mycompany.com`) en el certificado HTTPS, especifique este FQDN en el campo **Nombre de host MDM**. Además, si se emplea un comodín * (por ejemplo, `*.miempresa.com`) en el certificado HTTPS, puede utilizar `mdm.miempresa.com` en el campo **Nombre de host MDM**.

Tenga mucho cuidado de lo que escribe en el campo **Nombre de host MDM** en este paso de la instalación. Si la información es incorrecta, o está en un formato incorrecto, el Conector MDM no funcionará correctamente y la única forma de solucionarlo será la reinstalación del componente.



10. En el paso siguiente, haga clic en **Siguiente** para verificar la conexión a la base de datos.

11. Conecte el Conector MDM a ESET PROTECT Server. Complete los campos **Host del servidor** y **Puerto del servidor** necesarios para la conexión a ESET PROTECT Server y seleccione **Instalación ayudada por el servidor** o **Instalación sin conexión** para continuar:

- **Instalación ayudada por el servidor**: facilite las credenciales de administrador de ESET PROTECT Web Console y el instalador descargará los certificados necesarios automáticamente. Compruebe también los permisos necesarios para la instalación ayudada por el servidor.

    1.Introduzca el nombre del **Host del servidor** o la dirección IP de ESET PROTECT Server y el **Puerto de Web Console** (si no utiliza un puerto personalizado, conserve el puerto predeterminado 2223). Facilite también las credenciales de la cuenta de administrador de Web Console (**Nombre de usuario/Contraseña**).

    2.Cuando aparezca el mensaje Aceptar certificado, haga clic en **Sí**. Continúe con el paso 11.

- **Instalación sin conexión**: facilite un Certificado del proxy y Autoridad certificadora que pueda exportarse desde ESET PROTECT. También puede usar su certificado personalizado y la Autoridad certificadora adecuada.

    1.Haga clic en **Examinar** junto al Certificado de igual y desplácese hasta la ubicación del **Certificado de igual** (el certificado del proxy que exportó desde ESET PROTECT). Mantenga el campo de texto **Contraseña del certificado** en blanco, ya que este certificado no necesita contraseña.

    2.Repita el procedimiento para la Autoridad certificadora y continúe con el paso 11.

> Si está utilizando certificados personalizados con ESET PROTECT (en lugar de los predeterminados que se generaron automáticamente durante la instalación de ESET PROTECT), se deben utilizar cuando se le pida que suministre un certificado de proxy.

12. Especifique la carpeta de destino del Conector del dispositivo móvil (se recomienda utilizar la ubicación

predeterminada), haga clic en **Siguiente** > **Instalar**.

Una vez finalizada la instalación de MDM, se le solicitará la instalación de un agente. Haga clic en **Siguiente** para iniciar la instalación y aceptar el EULA si está de acuerdo con él y siga estos pasos:

1. Introduzca el **Host del servidor** (nombre de host o dirección IP de su ESET PROTECT Server) y el **Puerto del servidor** (el puerto predeterminado es el 2222, si utiliza un puerto distinto, cambie el puerto predeterminado por su número de puerto personalizado).

Asegúrese de que el **host del servidor** coincide con al menos uno de los valores (idealmente sería FQDN) que se definen en el campo **Host** de **Certificado del servidor**. De lo contrario, se mostrará el error "El certificado de servidor recibido no es válido". La única excepción es si existe un comodín (*) en el campo Host del certificado del servidor, lo que implica que funcionará con cualquier **host del servidor**.

2. Si está utilizando proxy, marque la casilla de verificación **Usar proxy**. Cuando lo seleccione, el instalador continuará con la **instalación sin conexión**.

Este ajuste de proxy se utiliza para la (replicación) entre ESET Management Agent y ESET PROTECT Server, no para el almacenamiento en caché de actualizaciones.
- **Nombre de host del servidor**: nombre de host o dirección IP de la máquina de proxy HTTP.
- **Puerto de proxy**: el valor predeterminado es 3128.
- **Nombre de usuario**, **Contraseña**: introduzca las credenciales utilizadas por el proxy si utiliza la autenticación.

Puede cambiar la configuración de proxy más adelante en la política. El proxy debe instalarse antes de poder configurar una conexión entre el agente y el servidor a través del proxy.

3. Seleccione una de las siguientes opciones de instalación y los pasos de la siguiente sección que se ajuste a su contexto:

Instalación ayudada por el servidor: tendrá que facilitar las credenciales de administrador de ESET PROTECT Web Console (el programa de instalación descargará los certificados necesarios automáticamente).

Instalación sin conexión: tendrá que facilitar un Certificado del agente y una autoridad certificadora que pueden exportarse desde ESET PROTECT. También puede usar su certificado personalizado.

- Para continuar con la instalación **del agente ayudada por el servidor**, siga estos pasos:

1. Introduzca el nombre de host o la dirección IP de su ESET PROTECT Web Console (igual que en ESET PROTECT Server) en el campo **Host del servidor.** Deje el **Puerto de Web Console** establecido en el puerto predeterminado 2223 si no utiliza el puerto personalizado. Asimismo, introduzca sus credenciales de la cuenta de Web Console en los campos **Nombre de usuario y Contraseña**. Para iniciar sesión como un usuario de dominio, marque la casilla de verificación situada junto a **Iniciar sesión en el dominio**.

- Asegúrese de que el **host del servidor** coincide con al menos uno de los valores (idealmente sería FQDN) que se definen en el campo **Host** de **Certificado del servidor**. De lo contrario, se mostrará el error "El certificado de servidor recibido no es válido". La única excepción es si existe un comodín (*) en el campo Host del certificado del servidor, lo que implica que funcionará con cualquier **host del servidor**.
- No puede utilizar un usuario con autenticación de doble factor en instalaciones ayudadas por el servidor.

2. Cuando se le pregunte si desea aceptar el certificado, haga clic en **Sí**.

3. Seleccione **No cree un ordenador (el ordenador se creará automáticamente durante la primera conexión)** o **Elija grupo estático personalizado**. Si hace clic en **Elija grupo estático personalizado**, podrá seleccionar entre una lista de grupos estáticos existentes de ESET PROTECT. El ordenador se agregará al grupo que haya seleccionado.

4. Especifique la carpeta de destino de ESET Management Agent (se recomienda utilizar la ubicación predeterminada), haga clic en **Siguiente** y, a continuación, haga clic en **Instalar**.

- Para continuar con la **instalación del agente sin conexión**, siga estos pasos:

1. Si seleccionó **Usar proxy** en el paso anterior, proporcione el **Nombre de host del proxy**, el **Puerto del proxy** (el puerto predeterminado es el 3128), el **Nombre de usuario** y la **Contraseña**, y haga clic en **Siguiente**.

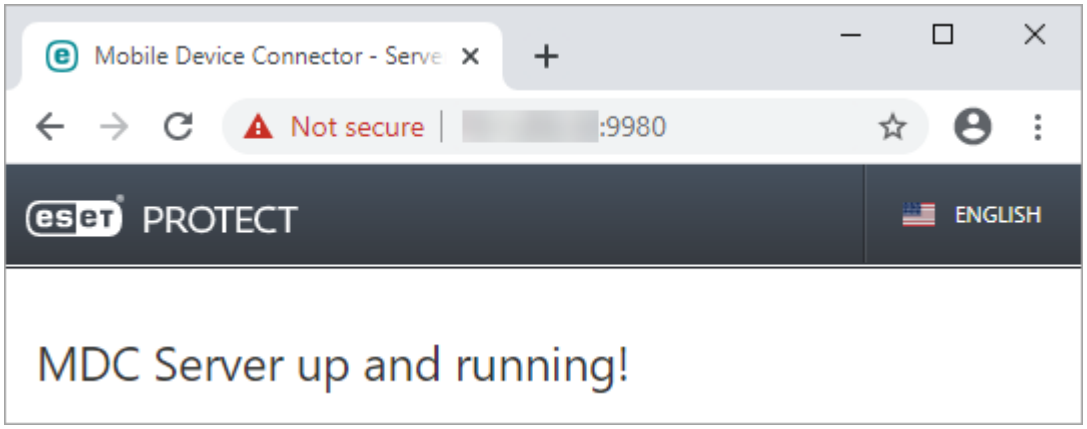
2. Haga clic en **Examinar** y desplácese hasta la ubicación en la que tiene almacenado su certificado de igual (el certificado de agente que exportó desde ESET PROTECT). Mantenga el campo de texto **Contraseña del certificado** en blanco, ya que este certificado no necesita contraseña. No es necesario que examine para indicar la ubicación de la **Autoridad certificadora** - mantenga este campo en blanco.

> Si está utilizando un certificado personalizado con ESET PROTECT (en lugar de los predeterminados que se generaron automáticamente durante la instalación de ESET PROTECT), utilice sus certificados personalizados según proceda.

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

3. Haga clic en **Siguiente** para instalarlo en la carpeta predeterminada o haga clic en **Cambiar** para elegir otra carpeta (se recomienda utilizar la ubicación predeterminada).

Una vez completada la instalación, compruebe si el Conector del dispositivo móvil funciona correctamente; para ello abra *https://your-mdm-hostname:enrollment-port* (por ejemplo, *https://mdm.company.com:9980*) en el navegador web o desde un dispositivo móvil. Si la instalación se completó correctamente, se mostrará el siguiente mensaje:



Ya puede activar MDM desde ESET PROTECT.

Instalación en Microsoft Azure

Para aquellos usuarios que prefieren utilizar una solución administrada, en lugar de mantener ESET PROTECT en sus instalaciones, ESET ofrece ESET PROTECT en la plataforma de nube Microsoft Azure.

Consulte el contenido de nuestra base de conocimiento para obtener más información:

- Primeros pasos con ESET PROTECT - Azure
- Máquina virtual de ESET PROTECT para Microsoft Azure: preguntas más frecuentes
- Puede instalar ESET PROTECT 9.1 en Azure siguiendo los pasos de este artículo de la Base de conocimiento y usando el instalador todo en uno de ESET PROTECT 9.1. También puede instalar ESMC 7.2 en Azure y, a continuación, actualizarlo a ESET PROTECT.

Instalación de componentes en Windows

En numerosas situaciones de instalación, es necesario instalar los diferentes componentes de ESET PROTECT en diferentes máquinas para dar cabida a arquitecturas de red, cumplir con los requisitos de rendimiento, o por otras razones. Los siguientes paquetes de instalación están disponibles para componentes de ESET PROTECT individuales:

Instalación de componentes principales

- ESET PROTECT Server
- ESET PROTECT Web Console – Puede seleccionar la instalación de ESET PROTECT Web Console en un ordenador distinto al ordenador donde se ha instalado ESET PROTECT Server.
- ESET Management Agent (debe estar instalado en los ordenadores cliente, opcional en ESET PROTECT Server)

Instalación de componentes opcionales

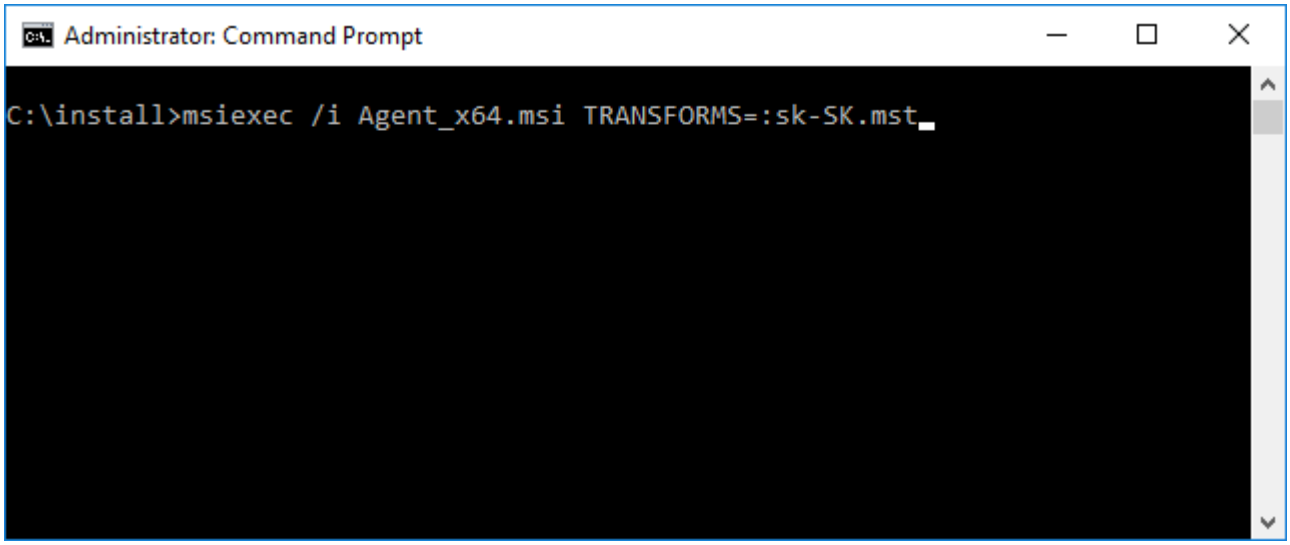
- RD Sensor
- Conector del dispositivo móvil
- Proxy HTTP Apache
- Herramienta Mirror

Consulte también Instalación todo en uno de ESET PROTECT.

Si desea obtener instrucciones sobre cómo actualizar ESMC a la versión ESET PROTECT 9.1 más reciente, consulte nuestros procedimientos de actualización.

Si desea ejecutar la instalación en su propio idioma, tendrá que iniciar el archivo instalador MSI del componente ESET PROTECT en concreto desde la línea de comandos.

A continuación se muestra un ejemplo de cómo ejecutar la instalación en eslovaco:



Si desea seleccionar el idioma de ejecución del instalador, especifique el parámetro `TRANSFORMS` correspondiente según lo expuesto en esta tabla:

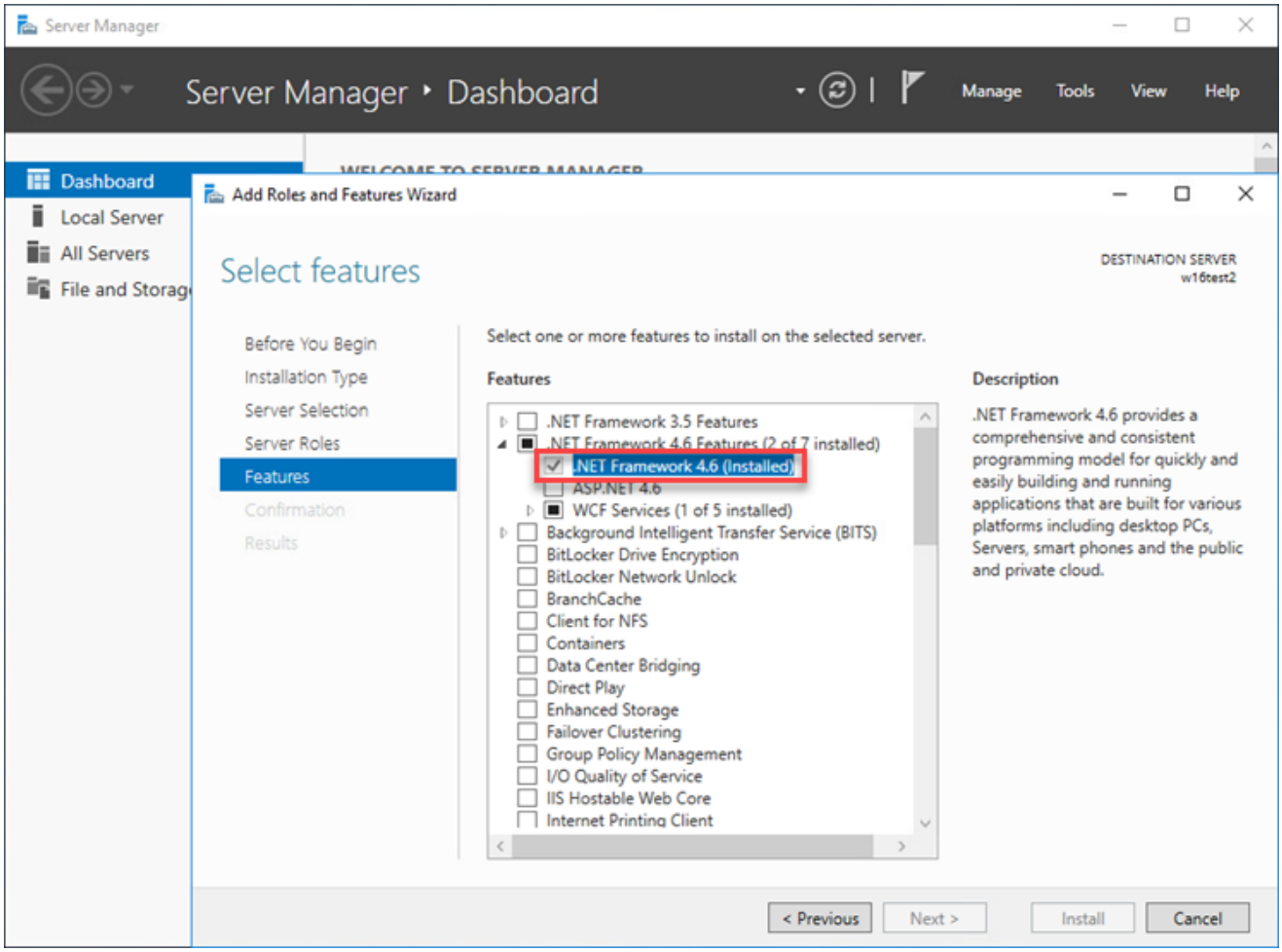
Idioma	Código
Inglés (Estados Unidos)	en-US
Árabe (Egipto)	ar-EG
Chino simplificado	zh-CN
Chino tradicional	zh-TW
Croata (Croacia)	hr-HR
Checo (República Checa)	cs-CZ
Francés (Francia)	fr-FR
Francés (Canadá)	fr-CA
Alemán (Alemania)	de-DE
Griego (Grecia)	el-GR
Húngaro (Hungría)*	hu-HU
Indonesio (Indonesia)*	id-ID
Italiano (Italia)	it-IT
Japonés (Japón)	ja-JP
Coreano (Corea)	ko-KR
Polaco (Polonia)	pl-PL
Portugués (Brasil)	pt-BR
Ruso (Rusia)	ru-RU
Español (Chile)	es-CL
Español (España)	es-ES
Eslovaco (Eslovaquia)	sk-SK
Turco (Turquía)	tr-TR
Ucraniano (Ucrania)	uk-UA

* Solo está disponible el producto en este idioma; la ayuda en línea no está disponible.

Instalación del servidor - Windows

Requisitos previos

- Debe disponer de una clave de licencia válida.
- Debe tener un sistema operativo Windows compatible.
- Los puertos necesarios deben estar abiertos y disponibles; consulte la lista completa de puertos aquí.
- El servidor de base de datos y el conector compatibles (Microsoft SQL Server o MySQL) están instalados y se están ejecutando. Le recomendamos revisar los detalles de configuración del servidor de la base de datos (Microsoft SQL Server o MySQL) para que la base de datos esté correctamente configurada de cara a su uso con ESET PROTECT. Lea el artículo de la Base de conocimiento para configurar la base de datos y el usuario de la base de datos de MS SQL o MySQL.
- ESET PROTECT Web Console instalado para administrar ESET PROTECT Server.
- La instalación de MS SQL Server Express requiere Microsoft .NET Framework 4. Puede instalarlo con el **Asistente para agregar roles y características**:



Instalación

Para instalar el componente ESET PROTECT Server en Windows, siga los pasos indicados a continuación:

Asegúrese de cumplir todos los requisitos previos de la instalación indicados anteriormente.

1. Visite la sección de descargas de ESET PROTECT para descargar un instalador independiente de este componente de ESET PROTECT (*server_x64.msi*).

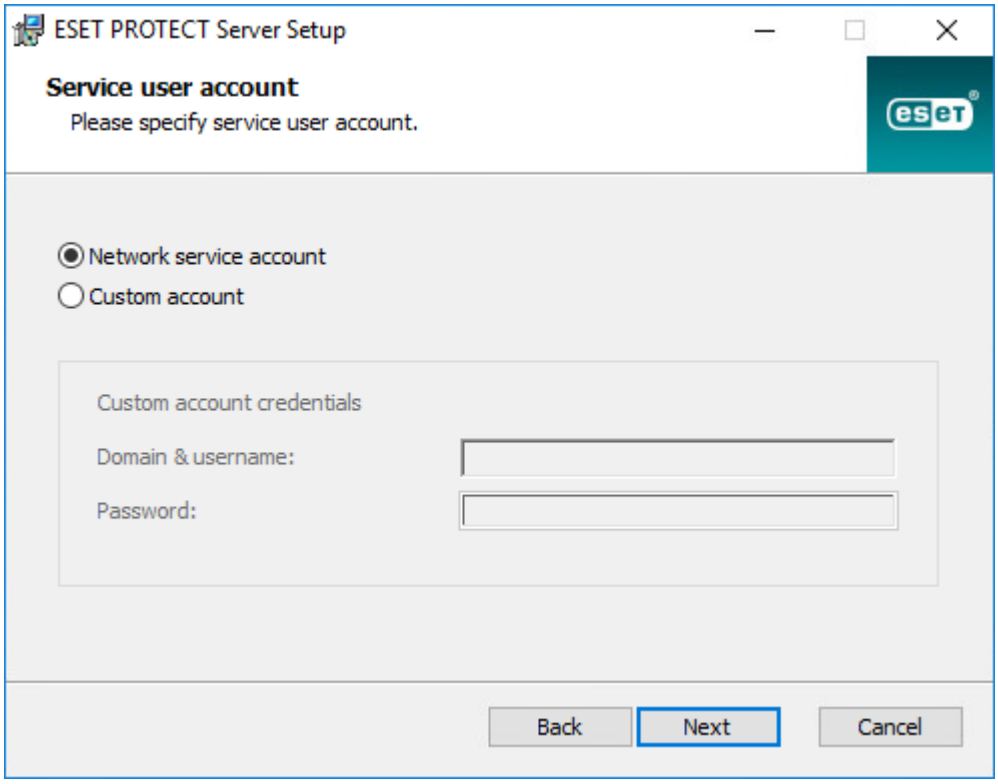
2. Ejecute el programa de instalación de ESET PROTECT Server y acepte el EULA si está de acuerdo con él.

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

4. Deje la casilla de verificación situada junto a **Esta es una instalación de clúster** vacía y haga clic en **Siguiente**. ¿Es una instalación de clúster?

5. Seleccione una **cuenta del usuario de servicio**. Esta cuenta se utiliza para ejecutar el servicio de servidor de ESET PROTECT. Están disponibles las opciones siguientes:

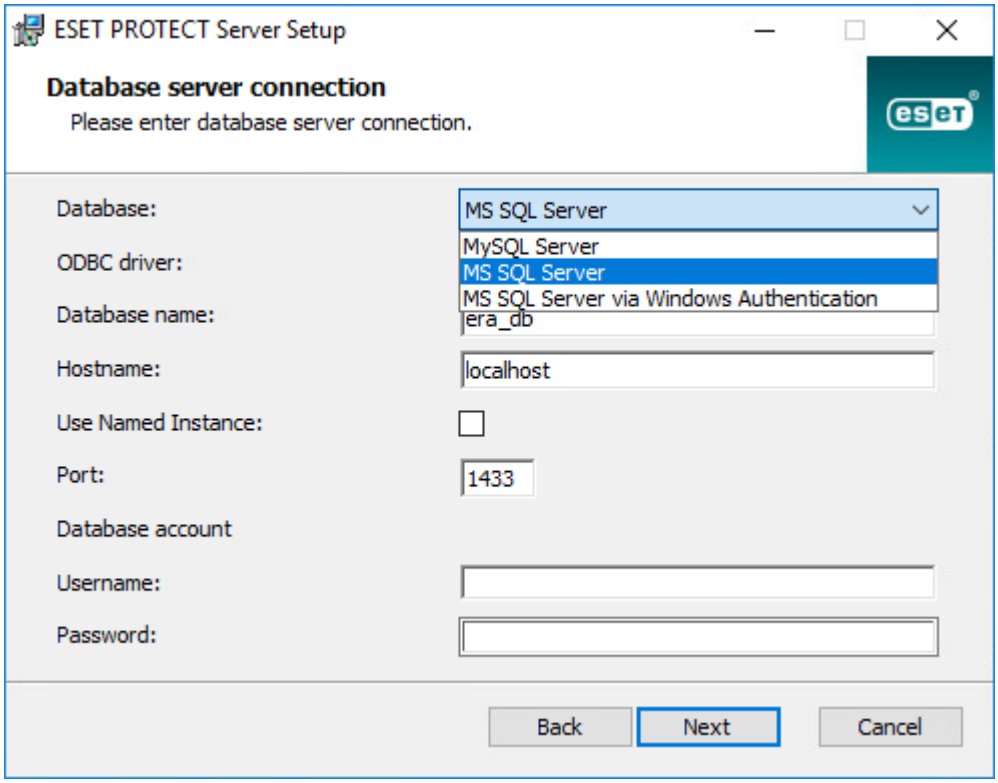
- **Cuenta de servicio de red**: seleccione esta opción si no utiliza un dominio.
- **Cuenta personalizada**: proporcione las credenciales de usuario del dominio: `DOMINIO\NOMBRE DE USUARIO` y contraseña.



6. Conéctese a una base de datos. Todos los datos se guardan aquí (contraseña de ESET PROTECT Web

Console, registros del ordenador cliente, etc.):

- **Base de datos**: MySQL Server/MS SQL Server/MS SQL Server mediante autenticación de Windows
- **Controlador de ODBC**: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/MySQL ODBC 8.0 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 para SQL Server/ODBC Driver 13 para SQL Server/ODBC Driver 17 para SQL Server/ODBC Driver 18 para SQL Server
- **Nombre de la base de datos**: Se recomienda utilizar el nombre predefinido o cambiarlo si es necesario.
- **Nombre de host**: nombre del host o dirección IP del servidor de base de datos
- **Puerto**: se utiliza para conectar al servidor de base de datos
- **Nombre de usuario/Contraseña** de la cuenta admin de la base de datos
- **Usar instancia con nombre**: si está utilizando una base de datos de MS SQL, también puede marcar la casilla de verificación **Usar instancia con nombre** para usar una instancia de la base de datos personalizada. Puede configurarlo en el campo **Nombre del host** con el formato *NOMBRE_HOST\INSTANCIA_BD* (por ejemplo, *192.168.0.10\ESMC7SQL*). Para las bases de datos en clústeres utilice únicamente el nombre de clúster. Si se selecciona esta opción, no podrá cambiar el puerto de conexión de la base de datos; el sistema utilizará los puertos predeterminados que Microsoft ha definido. Para conectar ESET PROTECT Server a la base de datos de MS SQL instalada en un clúster de conmutación por error, escriba el nombre del clúster en el campo **Nombre del host**.

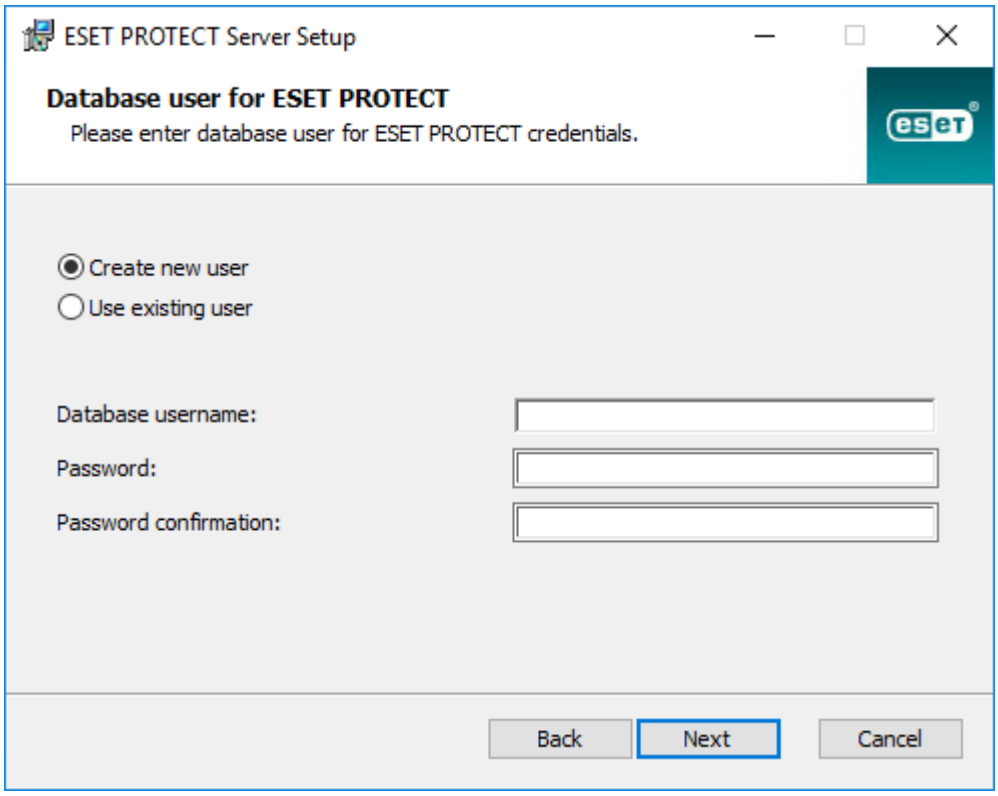


ESET PROTECT Server almacena grandes blobs de datos en la base de datos. Por tanto, para que ESET PROTECT se ejecute correctamente, es necesario configurar MySQL de forma que acepte paquetes de gran tamaño.

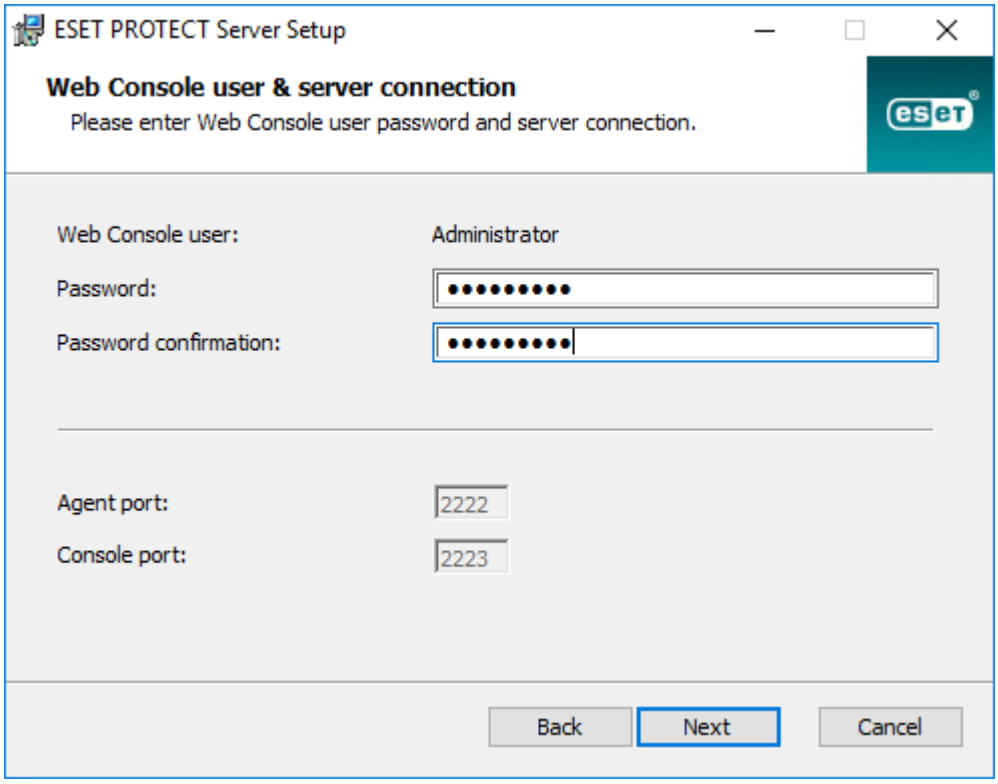
Este paso comprobará la conexión a la base de datos. Si la conexión es correcta, puede continuar con el siguiente

paso.

7. Seleccione un usuario de ESET PROTECT que tenga acceso a la base de datos. Puede utilizar un usuario existente o la instalación puede crear uno para usted.



8. Introduzca una contraseña de acceso a **Web Console**.

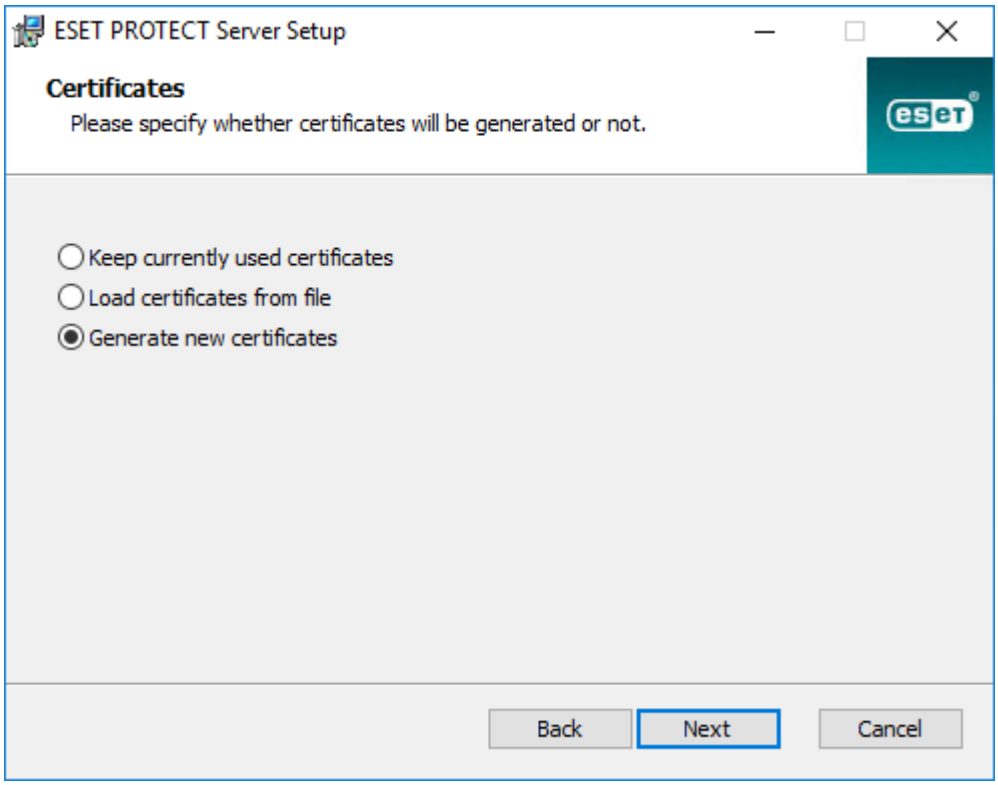


9. ESET PROTECT utiliza certificados para la comunicación entre cliente-servidor. Seleccione una de las siguientes opciones:

• **Conservar los certificados actualmente en uso**: esta opción solo está disponible si la base de datos ya se ha utilizado con otro ESET PROTECT Server antes.

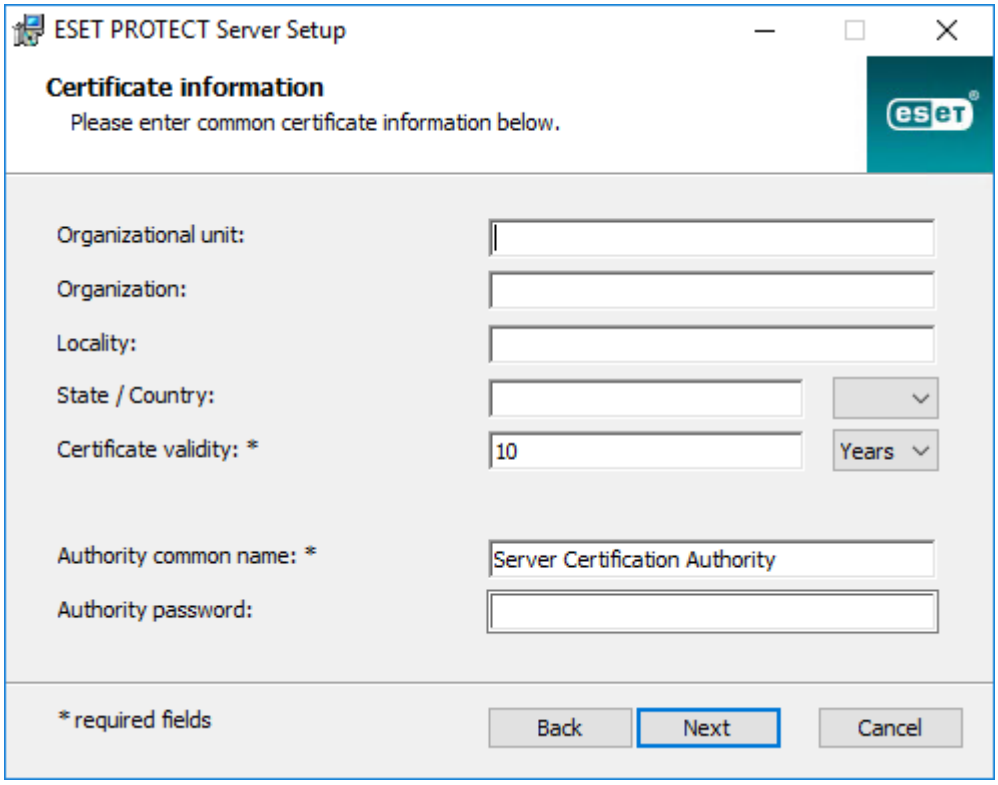
• **Cargar certificados desde archivo**: seleccione el certificado de Server y la autoridad certificadora existentes.

• **Generar certificados nuevos**: el instalador genera nuevos certificados.



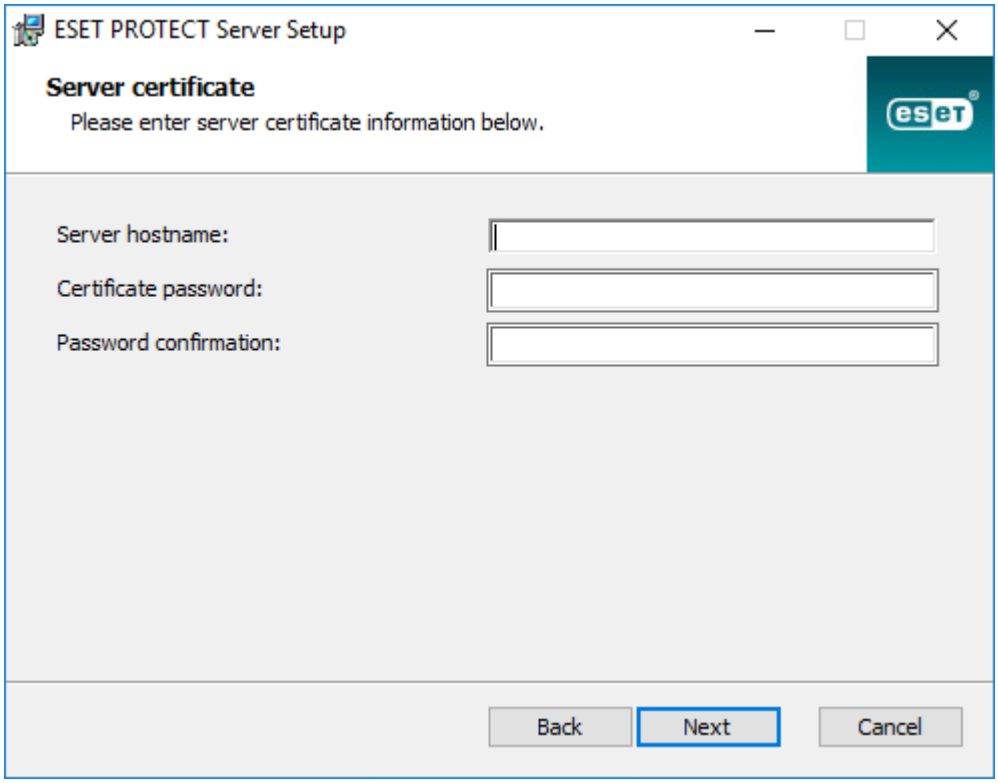
10. Siga este paso si ha seleccionado la opción **Generar certificados nuevos** en el paso anterior.

a)Especifique información adicional sobre los certificados (opcional). Si escribe la **Contraseña de la autoridad**, asegúrese de recordarla.

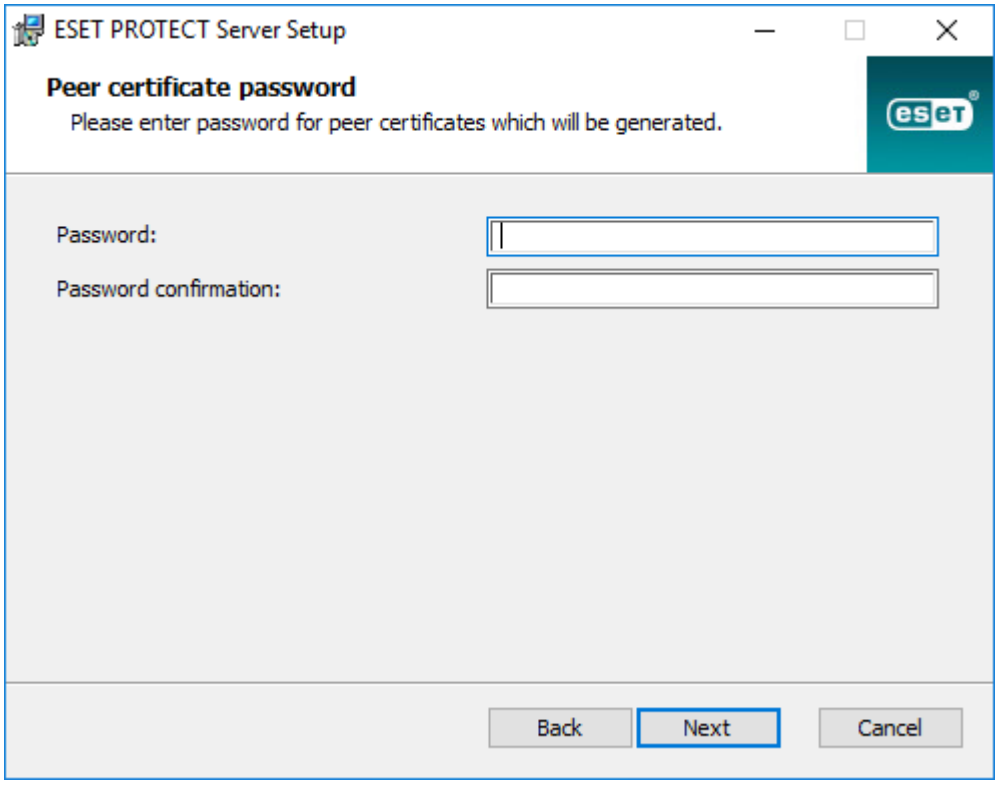


b)En el campo **Certificado del servidor**, escriba el **Nombre de Nombre de host del servidor** y la **Contraseña del certificado** (opcional).

El **Nombre de host del servidor** en el certificado del servidor no debe contener ninguna de las siguientes palabras clave: `server`, `proxy`, `agent`.

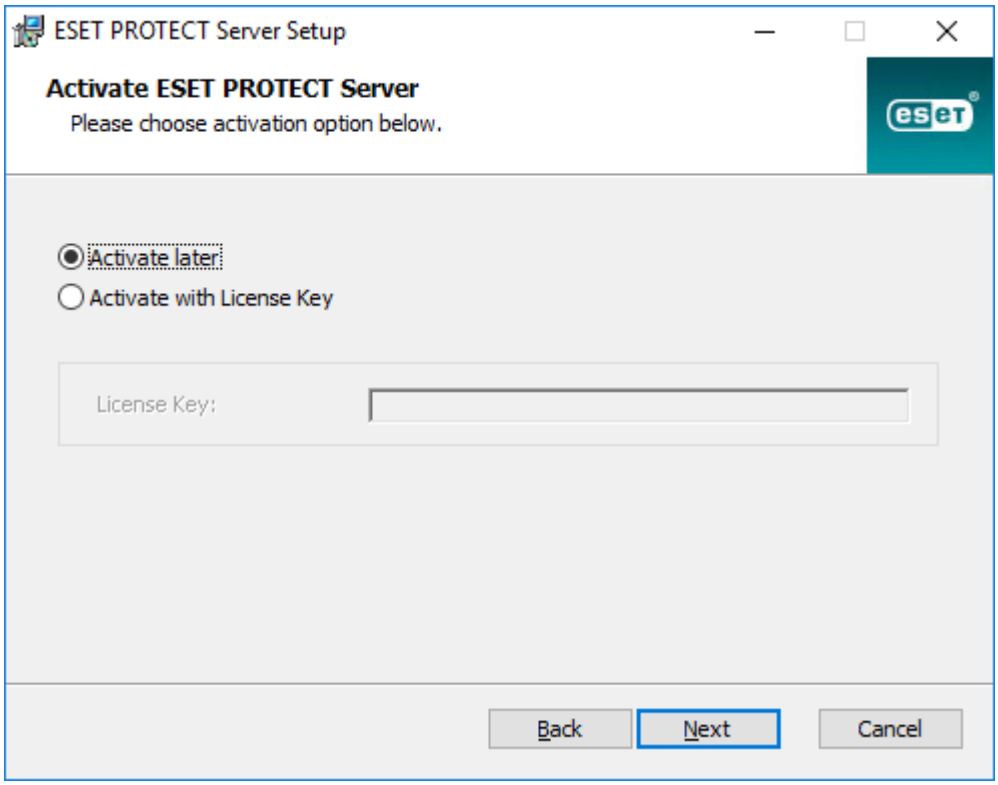


c)En el campo **Contraseña del certificado de par**, escriba la contraseña de los certificados de igual del agente y el proxy.



11. La configuración puede realizar una tarea inicial Sincronización de grupos estáticos. Seleccione el método (**No sincronizar**, **Sincronización con Windows Network**, **Sincronización con Active Directory**) y haga clic en **Siguiente**.

12. Introduzca una clave de licencia válida o seleccione **Activar más tarde**.



13. Confirme o cambie la carpeta de instalación para el servidor y haga clic en **Siguiente**.

14. Haga clic en **Instalar** para instalar el ESET PROTECT.

Cuando haya terminado de instalar ESET PROTECT Server, puede instalar ESET Management Agent en el mismo equipo (opcional) para habilitar la administración del servidor de la misma forma que administra un ordenador cliente.

Requisitos de Microsoft SQL Server

Se deben cumplir los siguientes requisitos para Microsoft SQL Server:

- Instale una versión compatible de Microsoft SQL Server. Elija el tipo de autenticación **Modo mixto** durante la instalación.

- Si ya tiene Microsoft SQL Server instalado, configure la autenticación como **Modo mixto (autenticación de SQL Server y de Windows)**. Para ello, siga las instrucciones de este artículo de la Base de conocimiento. Si desea usar la **Autenticación de Windows** para iniciar sesión en Microsoft SQL Server, siga los pasos indicados en este artículo de la Base de conocimiento.

- Permita las conexiones TCP/IP con SQL Server. Para ello, siga las instrucciones de este artículo de la Base de conocimiento desde la parte **II. Permitir las conexiones TCP/IP con la base de datos SQL**.

- Para configurar, gestionar y administrar Microsoft SQL Server (bases de datos y usuarios), descargue SQL Server Management Studio (SSMS).
- No instale SQL Server en un controlador de dominio (por ejemplo, Windows SBS o Essentials). Le recomendamos que instale ESET PROTECT en un servidor diferente o que no seleccione el componente SQL Server Express durante la instalación (necesita utilizar su SQL o MySQL Server existente para ejecutar la base de datos de ESET PROTECT).

Instalación y configuración de MySQL Server

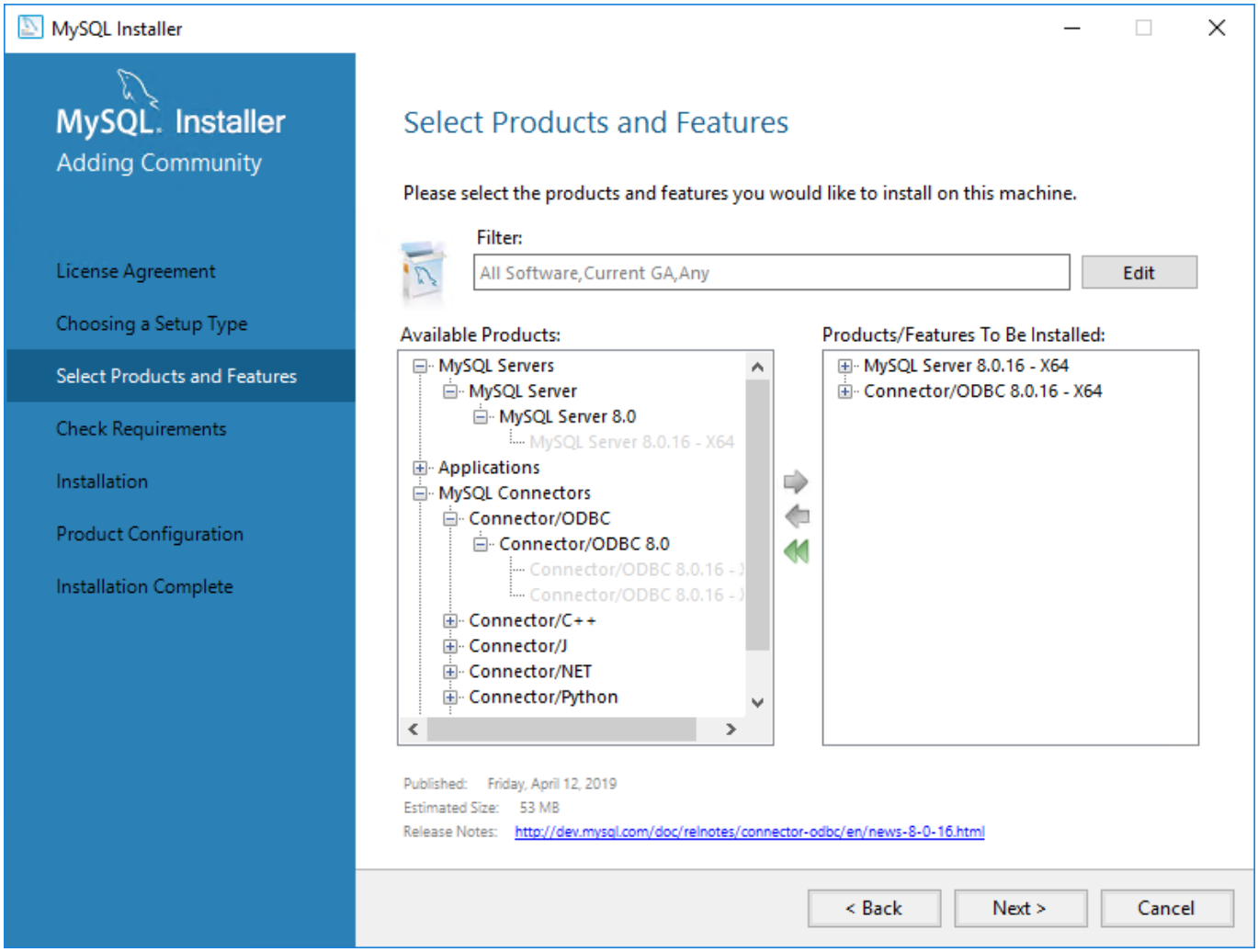
Instalación

Asegúrese de instalar una versión compatible de MySQL Server y el conector ODBC.

1. Descargue el instalador de MySQL 8 para Windows de https://dev.mysql.com/downloads/installer/ y ejecútelo.

2. Marque la casilla de verificación **Acepto los términos de licencia y** haga clic en **Siguiente**.

3. Durante la configuración de la instalación, seleccione **Personalizado** y seleccione **MySQL Server** y **Conector/ODBC** para realizar la instalación. Asegúrese de que el conector ODBC coincida con el valor de bits del MySQL Server instalado (x86 o x64).



4. Haga clic en **Siguiente** y **Ejecutar** para instalar MySQL Server y el conector ODBC.

5. Haga clic en **Siguiente**. En **Alta disponibilidad**, seleccione **MySQL Server independiente/Replicación de MySQL clásico** y haga clic en **Siguiente**.

6. En **Tipo y red**, seleccione **Ordenador servidor** en el menú desplegable **Tipo de configuración** y haga clic en **Siguiente**.

7. En **Método de autenticación,** seleccione la opción recomendada **Usar cifrado de contraseña segura para la autenticación** y haga clic en **Siguiente**.

8. En **Cuentas y roles**, escriba la **Contraseña del usuario root de MySQL** dos veces. También se recomienda crear una cuenta de usuario de base de datos dedicada.

9. En **Servicio de Windows**, conserve los valores predefinidos y haga clic en **Siguiente**.

10. Haga clic en **Ejecutar** y espere hasta que finalice la instalación de MySQL Server. Haga clic en **Finalizar**, **Siguiente** y **Finalizar** para cerrar la ventana de instalación.

Configuración

1. Abra el siguiente archivo en un editor de texto:

C:\ProgramData\MySQL\MySQL Server 8.0\my.ini

2. Localice y edite o añada la siguiente configuración a la sección `[mysqld]` del archivo *my.ini*:

- Cree la sección `[mysqld]` si no está presente en el archivo.
- Si los parámetros no están presentes en el archivo, agréguelos a la sección `[mysqld]`.
- Para determinar la versión de MySQL, ejecute el comando: `mysql --version`

Parámetro	Comentarios y valores recomendados	MySQL versión
`max_allowed_packet=33M`		Todas las versiones compatibles.
`log_bin_trust_function_creators=1`	También puede desactivar el inicio de sesión binario: `log_bin=0`	Versiones 8.x compatibles
`innodb_log_file_size=100M`	La multiplicación de los valores de estos dos parámetros debe dar como mínimo **200**. El valor mínimo de `innodb_log_files_in_group` es **2** y el valor máximo es **100**; el valor también debe ser un número entero.	Versiones 8x compatibles 5.7 5.6.22 (y posteriores 5.6.x)
`innodb_log_files_in_group=2`		
`innodb_log_file_size=200M`	Establezca el valor en **200M** como mínimo y **3000M** como máximo.	5.6.20 y 5.6.21

3. Guarde y cierre el archivo *my.ini*.

4. Abra el símbolo del sistema e introduzca los siguientes comandos para reiniciar MySQL Server y aplicar la configuración (el nombre del proceso depende de la versión de MySQL: 8.0 = mysql80, etc.):

```
net stop mysql80
net start mysql80
```

5. Introduzca el siguiente comando en el símbolo del sistema para comprobar si el servidor de MySQL está en funcionamiento:

```
sc query mysql80
```

Cuenta de usuario de base de datos dedicada

Si no desea utilizar una **cuenta SA** (MS SQL) o una **cuenta raíz** (MySQL), puede crear una **cuenta de usuario de base de datos dedicada**. Esta cuenta de usuario dedicada se utilizará para acceder únicamente a la base de datos de ESET PROTECT. Le recomendamos que cree una cuenta de usuario de base de datos dedicada en su servidor de base de datos antes de iniciar la instalación de ESET PROTECT. Asimismo, deberá crear una base de datos vacía a la que accederá ESET PROTECT utilizando esta cuenta de usuario dedicada.

Existe un conjunto mínimo de privilegios que deben otorgarse a una cuenta de usuario de base de datos dedicada:

- Privilegios de usuario de MySQL: `ALTER`, `ALTER ROUTINE`, `CREATE`, `CREATE ROUTINE`, `CREATE TEMPORARY TABLES`, `CREATE VIEW`, `DELETE`, `DROP`, `EXECUTE`, `INDEX`, `INSERT`, `LOCK TABLES`, `SELECT`, `UPDATE`, `TRIGGER`. - para obtener más información sobre los privilegios de MySQL, consulte http://dev.mysql.com/doc/refman/8.0/en/grant.html.

- Funciones a nivel de base de datos de Microsoft SQL Server: Los usuarios de las bases de datos de ESET

PROTECT deben ser miembros de la función de base de datos db_owner. Para obtener más información sobre las funciones a nivel de base de datos de Microsoft SQL Server, consulte https://msdn.microsoft.com/es-es/library/ms189121%28v=sql.100%29.aspx.

Puede encontrar una guía más detallada sobre cómo configurar su base de datos y su cuenta de usuario de MS SQL y MySQL en el artículo de nuestra Base de conocimiento.

Instalación del agente – Windows

Métodos disponibles

Existen diversos métodos de instalación e implementación disponibles para la instalación de ESET Management Agent en estaciones de trabajo Windows:

Método	Documentación	Descripción
Instalación mediante interfaz gráfica de usuario desde el instalador *.msi*	• Este capítulo • KB	• El método de instalación **estándar**. • Este método se puede ejecutar como instalación asistida por el servidor o como instalación sin conexión. • Use este método al instalar el agente en un equipo con ESET PROTECT Server.
ESET Remote Deployment Tool	• De ayuda en línea	• Recomendado para implementación en masa mediante red local. • Se puede usar para implementar el instalador todo en uno (agente y producto de seguridad de ESET)
Instalador del Agente todo en uno	• Crear instalador todo en uno del agente • KB	• El instalador también puede incluir un producto de seguridad y una política integrada. • El tamaño del instalador es de varios cientos de MB.
Script instalador del agente	• Crear instalador de scripts del agente • KB	• El instalador es un script ejecutable. Su tamaño es pequeño, pero necesita acceso a la ubicación del instalador *.msi*. • El script se puede editar para usar el instalador local y el proxy HTTP.
Implementación de SCCM y GPO	• SCCM • GPO • KB	• Método avanzado de implementación en masa remota. • Utilización de un archivo *.ini* pequeño.
Tarea del servidor - Implementación del agente	• De ayuda en línea • KB	• Una alternativa a SCCM y GPO. • No es viable mediante el proxy HTTP. • Se ejecuta con ESET PROTECT Server desde la Consola web de ESET PROTECT.

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

Instalación mediante interfaz gráfica de usuario

Siga los pasos indicados a continuación para instalar el componente ESET Management Agent localmente en Windows:

1. Visite la sección de descargas de ESET PROTECT para descargar un instalador independiente de este componente de ESET PROTECT (*agent_x86.msi*, *agent_x64.msi* o *agent_arm64.msi*).

2. Ejecute el programa de instalación de ESET Management Agent y acepte el Acuerdo de licencia para el usuario final si está de acuerdo con él.

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

4. Introduzca el **Host del servidor** (nombre de host o dirección IP de su ESET PROTECT Server) y el **Puerto del servidor** (el puerto predeterminado es el 2222, si utiliza un puerto distinto, cambie el puerto predeterminado por su número de puerto personalizado).

Asegúrese de que el **host del servidor** coincide con al menos uno de los valores (idealmente sería FQDN) que se definen en el campo **Host** de **Certificado del servidor**. De lo contrario, se mostrará el error "El certificado de servidor recibido no es válido". El uso de un comodín (*) en el campo Host del certificado del servidor permitirá que el certificado funcione con cualquier **host del servidor**.

5. Si utiliza un proxy para la conexión entre el agente y el servidor, seleccione la casilla de verificación junto a **Usar proxy**. Cuando lo seleccione, el instalador continuará con la instalación sin conexión.

Este ajuste de proxy se utiliza para la (replicación) entre ESET Management Agent y ESET PROTECT Server, no para el almacenamiento en caché de actualizaciones.
- **Nombre de host del servidor**: nombre de host o dirección IP de la máquina de proxy HTTP.
- **Puerto de proxy**: el valor predeterminado es 3128.
- **Nombre de usuario**, **Contraseña**: introduzca las credenciales utilizadas por el proxy si utiliza la autenticación.

Puede cambiar la configuración de proxy más adelante en la política. El proxy debe instalarse antes de poder configurar una conexión entre el agente y el servidor a través del proxy.

6. Seleccione una de las siguientes opciones de instalación y los pasos de la siguiente sección que se ajuste a su contexto:

- Instalación ayudada por el servidor: tendrá que facilitar las credenciales de administrador de ESET PROTECT Web Console. El instalador descargará automáticamente los certificados necesarios.

No puede utilizar un usuario con autenticación de doble factor en instalaciones ayudadas por el servidor.

- Instalación sin conexión: tendrá que facilitar un Certificado del agente y una autoridad certificadora. Ambos se pueden exportar desde ESET PROTECT. También puede usar su certificado personalizado.

Instalación mediante línea de comandos

El instalador *MSI* se puede ejecutar de forma local o remota. Descargue ESET Management Agent del sitio web de ESET.

Parámetro	Descripción y valores permitidos
P_HOSTNAME=	Nombre de host o dirección IP del ESET PROTECT Server.
P_PORT=	Puerto del servidor para conexión del agente (opcional; si no se especifica, se usa el puerto predeterminado 2222).
P_CERT_PATH=	Ruta de acceso al certificado del agente en formato Base64 en el archivo *.txt* (exportado desde la Consola web de ESET PROTECT).
P_CERT_AUTH_PATH=	Ruta de acceso a la autoridad certificadora en formato Base64 en el archivo *.txt* (exportado desde la Consola web de ESET PROTECT).
P_LOAD_CERTS_FROM_FILE_AS_BASE64=	**YES**; use este parámetro cuando haga referencia al certificado del agente y a la autoridad certificadora almacenados en archivos *.txt*.
P_CERT_PASSWORD=	Use este parámetro para facilitar una contraseña para el certificado del agente.
P_CERT_CONTENT=	Cadena del certificado del agente en formato Base64 (exportado desde la Consola web de ESET PROTECT).
P_CERT_AUTH_CONTENT=	Autoridad certificadora en formato Base64 (exportado desde la Consola web de ESET PROTECT).
PASSWORD=	Contraseña de desinstalación de un agente protegido mediante contraseña.
P_ENABLE_TELEMETRY=	**0**: desactivado (opción predeterminada); **1**: activado. Envío de informes de bloqueo y datos de telemetría a ESET (parámetro opcional).
P_INSTALL_MODE_EULA_ONLY=	**1**;use este parámetro para una instalación semisilenciosa de ESET Management Agent. Verá la ventana de instalación del agente y se le pedirá que acepte el EULA y active o desactive la telemetría (P_ENABLE_TELEMETRY se ignora cuando se especifica). El resto de ajustes de instalación del agente se recopilan de los parámetros de la línea de comandos. Verá la finalización del proceso de instalación del agente.
P_USE_PROXY=	**1**; use este parámetro para permitir el uso del proxy HTTP (que ya está instalado en su red) en la replicación entre ESET Management Agent y ESET PROTECT Server (no para el almacenamiento en caché de actualizaciones).
P_PROXY_HTTP_HOSTNAME=	Nombre de host o dirección IP del proxy HTTP.
P_PROXY_HTTP_PORT=	Proxy HTTP para la conexión del agente.

Ejemplos de instalación mediante línea de comandos

Sustituya el código naranja que aparece a continuación según corresponda.

- Instalación silenciosa (parámetro `/q`) con conexión al puerto predeterminado, telemetría activada y el certificado del agente y la autoridad certificadora almacenados en archivos:

```
Agent_x64.msi /q P_HOSTNAME=10.20.30.40 P_ENABLE_TELEMETRY=1 P_CERT_PATH=C:\Users\Ad
```

```
ministrator\Desktop\certificate.txt P_CERT_AUTH_PATH=C:\Users\Administrator\Desktop\
ca.txt P_LOAD_CERTS_FROM_FILE_AS_BASE64=YES
```

- Instalación silenciosa con cadenas proporcionadas para el certificado del agente, para la autoridad certificadora, para la contraseña del certificado del agente y los parámetros del proxy HTTP:

```
Agent_x64.msi /q P_HOSTNAME=protect_server_name P_ENABLE_TELEMETRY=1 P_CERT_CONTENT=
CJfXtf1kZqlZKAl9P48HymBHa3CkW P_CERT_PASSWORD=abcd1234EFGH P_CERT_AUTH_CONTENT=45hvk
pqayzjJZhSY8qswDQYJKoZIhvc P_USE_PROXY=1 P_PROXY_HTTP_HOSTNAME=proxy_server P_PROXY_
HTTP_PORT=3128
```

- Instalación semisilenciosa:

```
Agent_x64.msi P_INSTALL_MODE_EULA_ONLY=1 P_HOSTNAME=10.20.30.40 P_CERT_PATH=C:\Users
\Administrator\Desktop\certificate.txt P_CERT_AUTH_PATH=C:\Users\Administrator\Deskt
op\ca.txt P_LOAD_CERTS_FROM_FILE_AS_BASE64=YES
```

Instalación del agente ayudada por el servidor

Para continuar con la instalación **del agente ayudada por el servidor**, siga estos pasos:

1. Introduzca el nombre de host o la dirección IP de su ESET PROTECT Web Console (igual que en ESET PROTECT Server) en el campo **Host del servidor.** Deje el **Puerto de Web Console** establecido en el puerto predeterminado 2223 si no utiliza el puerto personalizado. Asimismo, introduzca sus credenciales de la cuenta de Web Console en los campos **Nombre de usuario y Contraseña**. Para iniciar sesión como un usuario de dominio, marque la casilla de verificación situada junto a **Iniciar sesión en el dominio**.

- Asegúrese de que el **host del servidor** coincide con al menos uno de los valores (idealmente sería FQDN) que se definen en el campo **Host** de **Certificado del servidor**. De lo contrario, se mostrará el error "El certificado de servidor recibido no es válido". La única excepción es si existe un comodín (*) en el campo Host del certificado del servidor, lo que implica que funcionará con cualquier **host del servidor**.
- No puede utilizar un usuario con autenticación de doble factor en instalaciones ayudadas por el servidor.

2. Cuando se le pregunte si desea aceptar el certificado, haga clic en **Sí**.

3. Seleccione **No cree un ordenador (el ordenador se creará automáticamente durante la primera conexión)** o **Elija grupo estático personalizado**. Si hace clic en **Elija grupo estático personalizado**, podrá seleccionar entre una lista de grupos estáticos existentes de ESET PROTECT. El ordenador se agregará al grupo que haya seleccionado.

4. Especifique la carpeta de destino de ESET Management Agent (se recomienda utilizar la ubicación predeterminada), haga clic en **Siguiente** y, a continuación, haga clic en **Instalar**.

Instalación del agente sin conexión

Para continuar con la **instalación del agente sin conexión**, siga estos pasos:

1. Si seleccionó **Usar proxy** en el paso anterior, proporcione el **Nombre de host del proxy**, el **Puerto del proxy** (el puerto predeterminado es el 3128), el **Nombre de usuario** y la **Contraseña**, y haga clic en **Siguiente**.

2. Haga clic en **Examinar** y desplácese hasta la ubicación en la que tiene almacenado su certificado de igual (el certificado de agente que exportó desde ESET PROTECT). Mantenga el campo de texto **Contraseña del certificado** en blanco, ya que este certificado no necesita contraseña. No es necesario que examine para indicar la ubicación de la **Autoridad certificadora** - mantenga este campo en blanco.

> Si está utilizando un certificado personalizado con ESET PROTECT (en lugar de los predeterminados que se generaron automáticamente durante la instalación de ESET PROTECT), utilice sus certificados personalizados según proceda.

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

3. Haga clic en **Siguiente** para instalarlo en la carpeta predeterminada o haga clic en **Cambiar** para elegir otra carpeta (se recomienda utilizar la ubicación predeterminada).

ESET Remote Deployment Tool

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

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

> ESET Remote Deployment Tool solo se utiliza para implementar ESET Management Agent en ordenadores cliente con sistemas operativos Microsoft Windows compatibles.

Para obtener más información sobre requisitos previos y uso de la herramienta, consulte el capítulo ESET Remote Deployment Tool.

Instalación de Web Console - Windows

Puede instalar ESET PROTECT Web Console en Windows de dos maneras:

- Se recomienda utilizar el instalador todo en uno
- Los usuarios avanzados pueden realizar una instalación manual

Puede seleccionar la instalación de ESET PROTECT Web Console en un ordenador distinto al ordenador donde se ha instalado ESET PROTECT Server.

Instalar Web Console con el instalador todo en uno

Requisitos previos

- ESET PROTECT Server instalado.

Puede seleccionar la instalación de ESET PROTECT Web Console en un ordenador distinto al ordenador donde se ha instalado ESET PROTECT Server. Este procedimiento requiere pasos adicionales.

- Apache Tomcat es un componente obligatorio necesario para ejecutar ESET PROTECT Web Console.
- Apache Tomcat requiere Java/OpenJDK de 64 bits. Si tiene instaladas en su sistema varias versiones de Java, le recomendamos que desinstale las versiones de Java anteriores y mantenga únicamente la versión de Java compatible.

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

Instalación

Para instalar el componente ESET PROTECT Web Console en Windows utilizando el instalador todo en uno:

Asegúrese de cumplir todos los requisitos previos de la instalación indicados anteriormente.

1. Descargue el instalador todo en uno de ESET PROTECT del sitio web de ESET y descomprima el archivo descargado.

2. Si desea instalar la versión más reciente de Apache Tomcat y el instalador todo en uno contiene una versión más antigua de Apache Tomcat (este paso es opcional, vaya al paso 4 si no necesita la versión más reciente de Apache Tomcat):

   a. Abra la carpeta *x64* y diríjase a la carpeta *installers*.

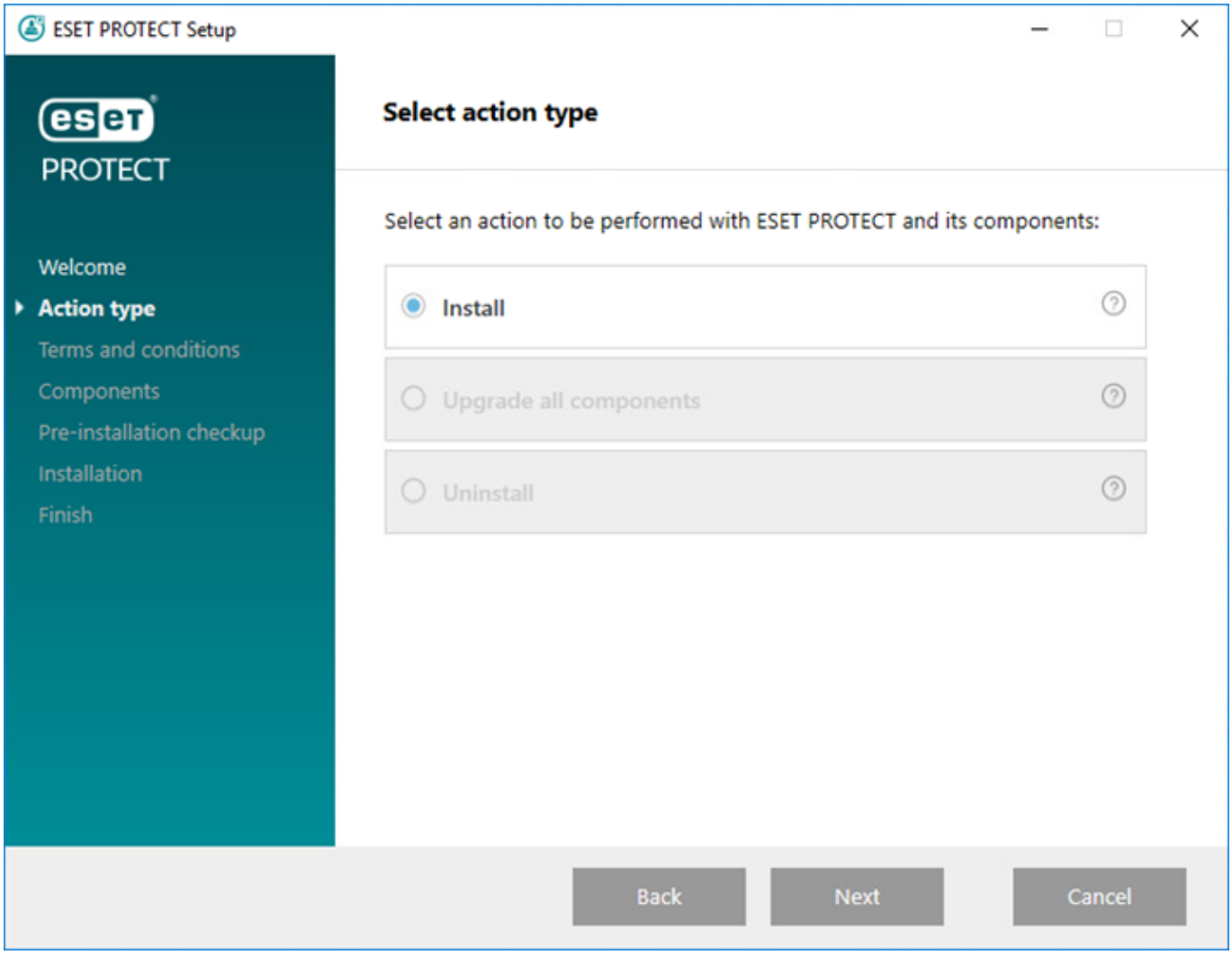
   b. Elimine el archivo *apache-tomcat-9.0.x-windows-x64.zip* situado en la carpeta *installers*.

   c. Descargue el paquete zip para Windows de 64 bits de Apache Tomcat 9.

   d. Mueva el paquete zip descargado a la carpeta *installers*.

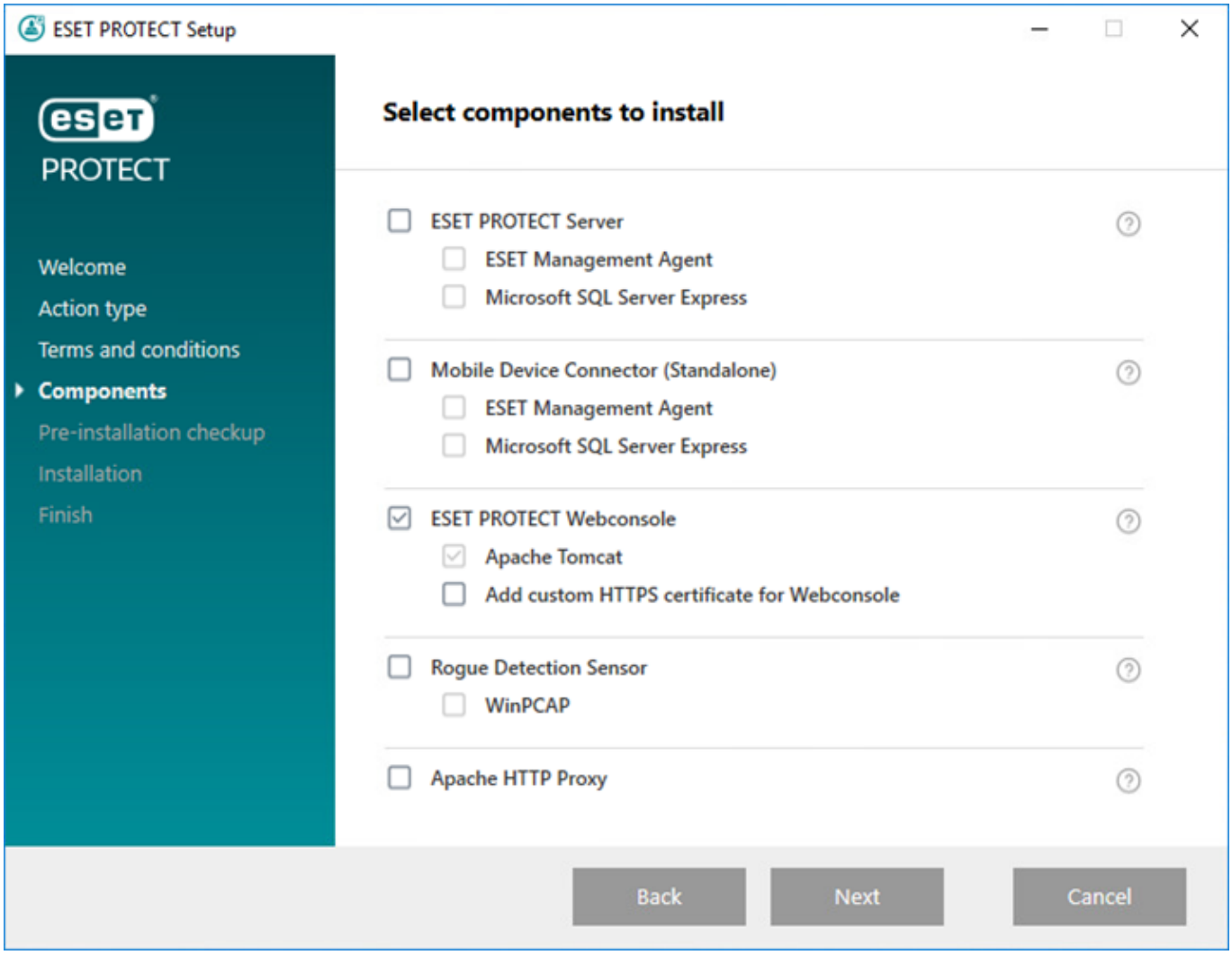
3. Para iniciar el instalador todo en uno, haga doble clic en el archivo *Setup.exe* y haga clic en **Siguiente** en la pantalla **Bienvenido**.

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



5. Tras aceptar el EULA, haga clic en **Siguiente**.

6. En **Seleccione los componentes que desea instalar**, marque solo la casilla de verificación **ESET PROTECT Web Console** y haga clic en **Siguiente**.

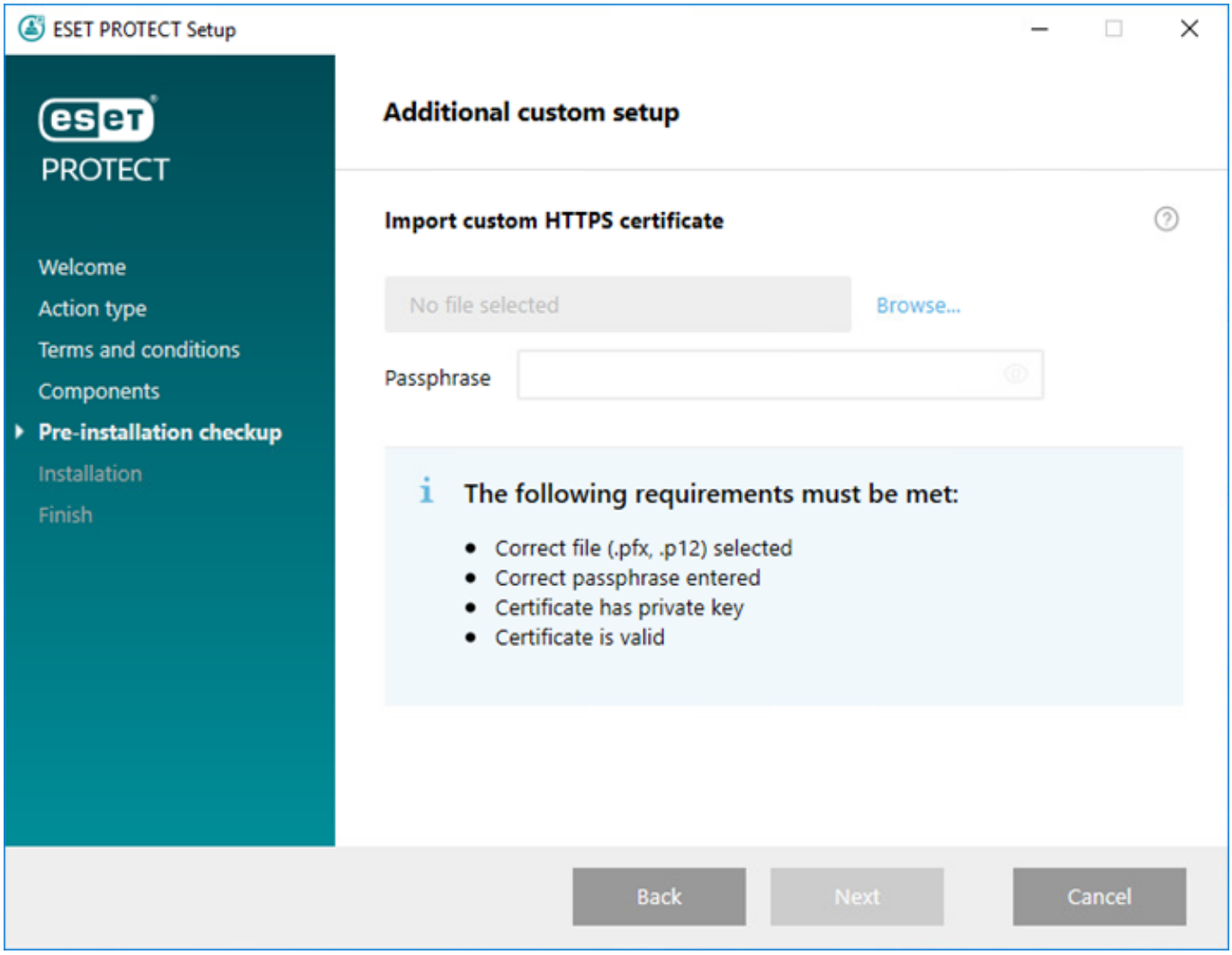


Si lo desea, marque la casilla de verificación **Agregar certificado HTTPS personalizado para la consola web**.

- Seleccione esta opción si desea usar un certificado HTTPS personalizado para ESET PROTECT Web Console.

- Si no selecciona esta opción, el instalador genera automáticamente un nuevo almacén de claves para Tomcat nuevo (un certificado HTTPS autofirmado).

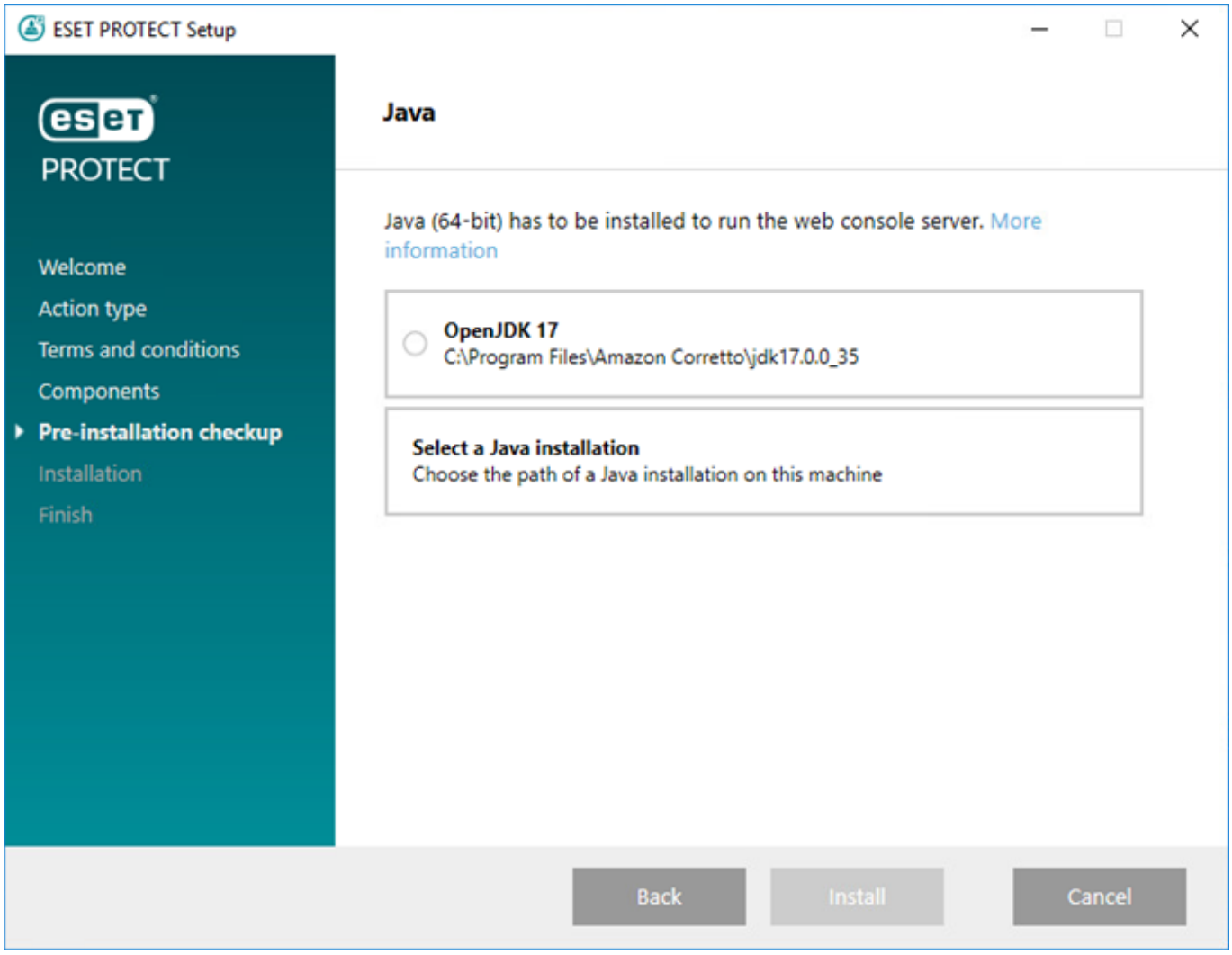
- Si ha seleccionado **Agregar certificado HTTPS personalizado para la consola web**, haga clic en **Examinar**, seleccione un certificado válido (archivo *.pfx* o .p12) y escriba la **contraseña** (o deje el campo vacío si no hay contraseña). El instalador instalará el certificado para el acceso a Web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



7. Seleccione una instalación de Java en el ordenador. Compruebe que está utilizando la versión más reciente de Java/OpenJDK.

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

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



8. Cuando finalice la instalación, haga clic en **Finalizar**.

Si ha instalado ESET PROTECT Web Console en un ordenador diferente de ESET PROTECT Server, realice estos pasos adicionales para permitir la comunicación entre ESET PROTECT Web Console y ESET PROTECT Server:
a)Detenga el servicio Apache Tomcat: Diríjase a **Inicio** > **Servicios** > haga clic con el botón derecho del ratón en el servicio Apache Tomcat y seleccione **Detener**.
b)Ejecute el Bloc de notas como administrador y edite *C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*.
c)Encuentre el `server_address=localhost`.
d)Reemplace `localhost` por la dirección IP del ESET PROTECT Server y guarde el archivo.
e) Reinicie el servicio Apache Tomcat: Diríjase a **Inicio** > **Servicios** > haga clic con el botón derecho del ratón en el servicio Apache Tomcat y seleccione **Iniciar**.

9. Abra ESET PROTECT Web Console en un navegador compatible; se mostrará una pantalla de inicio de sesión.

• Desde el ordenador en el que está alojado ESET PROTECT Web Console: *https://localhost/era*

• Desde cualquier ordenador con acceso a Internet a ESET PROTECT Web Console (sustituya *IP_ADDRESS_OR_HOSTNAME* por la dirección IP o el nombre de host de su ESET PROTECT Web Console): *https://IP_ADDRESS_OR_HOSTNAME/era*

Consulte también la configuración de Web Console adicional para soluciones empresariales o sistemas de bajo rendimiento.

Instalar Web Console manualmente

La instalación manual de ESET PROTECT Web Console es un procedimiento avanzado. Le recomendamos que instale ESET PROTECT Web Console utilizando el instalador todo en uno.

Requisitos previos

- ESET PROTECT Server instalado.

Puede seleccionar la instalación de ESET PROTECT Web Console en un ordenador distinto al ordenador donde se ha instalado ESET PROTECT Server. Este procedimiento requiere pasos adicionales.

- Apache Tomcat es un componente obligatorio necesario para ejecutar ESET PROTECT Web Console. Instale Apache Tomcat:

  a)Descargue la versión compatible más reciente del archivo del instalador de Apache Tomcat (instalador del servicio de Windows de 32/64 bits) *apache-tomcat-[versión].exe* de https://tomcat.apache.org.

  a)Ejecute el instalador.

  b)Durante la instalación, seleccione la ruta de acceso de Java (carpeta principal de las carpetas Java *bin* y *lib*), y marque la casilla de verificación **Run Apache Tomcat**.

  c)Tras la instalación, asegúrese de que el servicio Apache Tomcat está en ejecución y que el tipo de inicio está establecido en **Automático** (en **services.msc**).

- Apache Tomcat requiere Java/OpenJDK de 64 bits. Si tiene instaladas en su sistema varias versiones de Java, le recomendamos que desinstale las versiones de Java anteriores y mantenga únicamente la versión de Java compatible.

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

Instalación

Para instalar el componente ESET PROTECT Web Console en Windows, siga los pasos indicados a continuación:

Asegúrese de cumplir todos los requisitos previos de la instalación indicados anteriormente.

1. Visite la sección de descargas de ESET PROTECT para descargar un instalador independiente de este componente de ESET PROTECT (Web Console *era.war*).

2. Copie *era.war* en la carpeta de aplicaciones web de Apache Tomcat:

C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\webapps

3. Apache Tomcat extrae el archivo *era.war* automáticamente en la carpeta *era* e instala ESET PROTECT Web Console. Espere unos minutos hasta que finalice la extracción. Si no se realiza la extracción, siga los pasos de solución de problemas.

4. Si ha instalado ESET PROTECT Web Console en el mismo ordenador que ESET PROTECT Server, reinicie el servicio Apache Tomcat. Diríjase a **Inicio** > **Servicios** > haga clic con el botón derecho del ratón en el servicio Apache Tomcat y seleccione **Detener**. Espere 30 segundos y haga clic en **Inicio**.

Si ha instalado ESET PROTECT Web Console en un ordenador diferente de ESET PROTECT Server, realice estos pasos adicionales para permitir la comunicación entre ESET PROTECT Web Console y ESET PROTECT Server:
a)Detenga el servicio Apache Tomcat: Diríjase a **Inicio** > **Servicios** > haga clic con el botón derecho del ratón en el servicio Apache Tomcat y seleccione **Detener**.
b)Ejecute el Bloc de notas como administrador y edite *C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*.
c)Encuentre el `server_address=localhost`.
d)Reemplace `localhost` por la dirección IP del ESET PROTECT Server y guarde el archivo.
e) Reinicie el servicio Apache Tomcat: Diríjase a **Inicio** > **Servicios** > haga clic con el botón derecho del ratón en el servicio Apache Tomcat y seleccione **Iniciar**.

5. Abra ESET PROTECT Web Console en un navegador web compatible para ver una pantalla de inicio de sesión:

- Desde el ordenador en el que está alojado ESET PROTECT Web Console: *http://localhost:8080/era*
- Desde cualquier ordenador con acceso a Internet a ESET PROTECT Web Console (sustituya *IP_ADDRESS_OR_HOSTNAME* por la dirección IP o el nombre de host de su ESET PROTECT Web Console): *http://IP_ADDRESS_OR_HOSTNAME:8080/era*

6. Configure Web Console después de la instalación:

- El puerto HTTP predeterminado se establece en 8080 durante la instalación manual de Apache Tomcat. Le recomendamos que configure una conexión HTTPS para Apache Tomcat.
- Consulte también la configuración de Web Console adicional para soluciones empresariales o sistemas de bajo rendimiento.

Instalación del proxy HTTP

Acerca del proxy HTTP

El proxy HTTP reenvía la comunicación cifrada entre ESET Management Agent y ESET PROTECT Server. De forma predeterminada, ESET PROTECT usa el proxy HTTP Apache como proxy HTTP.

Utilice el proxy HTTP solo si sus instancias de ESET Management Agent no tienen conectividad de red con ESET PROTECT Server. El proxy HTTP no agrega la comunicación ni reduce el tráfico de red.

Se recomienda contar con el ESET Management Agent en el equipo en el que está instalado el proxy HTTP, pero no es necesario. ESET Management Agent no puede administrar (configurar) la aplicación del proxy HTTP.

- Arquitectura del proxy HTTP
- Arquitectura del proxy HTTP Apache
- Contextos avanzados para el proxy HTTP

Antes de la instalación

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

Instalación y configuración

Puede instalar el proxy HTTP Apache con un instalador independiente o con el instalador todo en uno de ESET PROTECT.

- La instalación con el instalador todo en uno requiere la descarga de todo el paquete, pero es más sencilla. Ejecute el instalador descargado y seleccione solo el **Proxy HTTP Apache** en el selector del instalador. Una vez instalado Apache, es necesario configurarlo.

- La instalación con el instalador independiente es más avanzada, pero el tamaño de la descarga es de solo unos MB. Consulte las instrucciones de instalación y configuración.

Configurar el proxy HTTP para un número elevado de clientes

Si utiliza el proxy HTTP Apache de 64 bits, puede aumentar el límite de subprocesos para su Apache HTTP Proxy. Edite el archivo de configuración *httpd.conf*, incluido en su carpeta Apache HTTP Proxy. Busque los siguientes ajustes en el archivo y actualice los valores para que coincidan con el número de clientes.

Sustituya el valor de ejemplo de `5000` con su número. El valor máximo es `32000`.

```
ThreadLimit 5000
```

```
ThreadsPerChild 5000
```

No cambie el resto del archivo.

Instalación de RD Sensor - Windows

Requisitos previos

- WinPcap: utilice la versión más reciente de WinPcap (4.1.0 como mínimo).

- La red debe estar correctamente configurada (puertos adecuados abiertos, comunicación entrante no bloqueada por un cortafuegos, etc.).

- ESET PROTECT Server es accesible

- ESET Management Agent debe estar instalado en el ordenador local para admitir todas las funciones del programa.

- Puede encontrar el archivo de registro de Rogue Detection Sensor aquí: *C:\ProgramData\ESET\Rouge Detection Sensor\Logs*

Instalación

Para instalar el componente RD Sensor en Windows, siga los pasos indicados a continuación:

Asegúrese de cumplir todos los requisitos previos de la instalación indicados anteriormente.

1. Visite la sección de descargas de ESET PROTECT para descargar un instalador independiente de este componente de ESET PROTECT (*rdsensor_x86.msi* o *rdsensor_x64.msi*).

2. Haga doble clic en el archivo de instalación del Sensor RD para iniciar la instalación.

3. Acepte el EULA y haga clic en **Siguiente**.

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

5. Seleccione la ubicación de instalación de RD Sensor y haga clic en **Siguiente** > **Instalar**.

Si hay varios segmentos de red, Rogue Detection Sensor debe instalarse por separado en cada segmento de red para generar una lista completa de todos los dispositivos de toda la red.

Herramienta Mirror: Windows

¿Es usuario de Linux?

Para las actualizaciones del motor de detección se necesita la herramienta Mirror. Si sus ordenadores cliente no tienen una conexión a Internet y necesitan actualizaciones del motor de detección, puede utilizar la herramienta Mirror para descargar archivos de actualización de servidores de actualización de ESET y almacenarlos de forma local.

La herramienta Mirror descarga únicamente actualizaciones del motor de detección y otros módulos del programa, no descarga PCU (actualizaciones de componentes del programa) ni datos de ESET LiveGrid®. También puede crear un repositorio sin conexión completo. Alternativamente, puede actualizar productos individualmente.

Requisitos previos

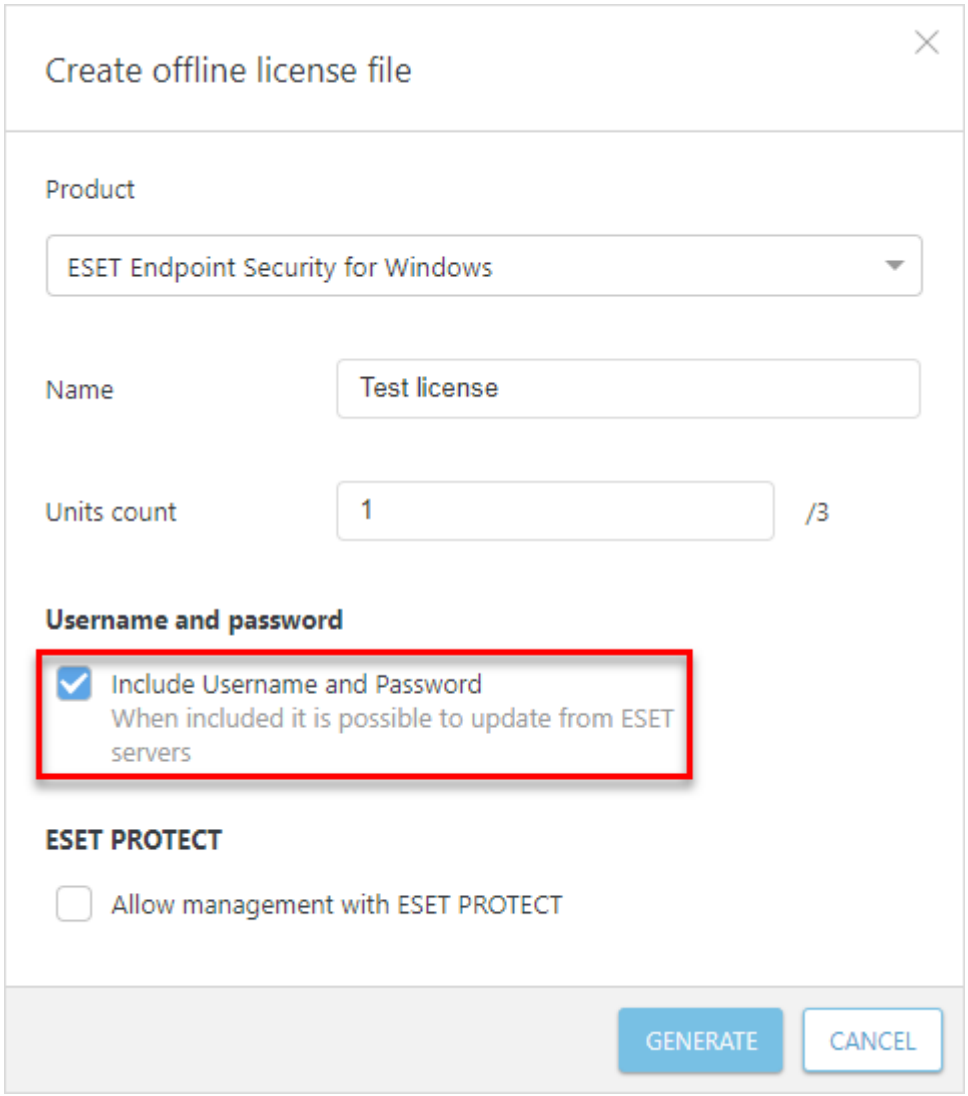
La herramienta Mirror no es compatible con Windows XP ni Windows Server 2003.

- La carpeta de destino debe estar disponible para compartir, servicio Samba/Windows o HTTP/FTP, según cómo desea que las actualizaciones estén accesibles.

  - Productos de seguridad de ESET para Windows: puede actualizarlos de forma remota mediante HTTP o una carpeta compartida.

- Productos de seguridad de ESET para Linux/macOS: solo puede actualizarlos de forma remota con HTTP. Si utiliza una carpeta compartida, debe estar en el mismo ordenador que el producto de seguridad de ESET.

- Debe tener un archivo de Licencia sin conexión válido que incluya el nombre de usuario y contraseña. Cuando genere un archivo de licencia, asegúrese de marcar la casilla de verificación situada junto a **Incluir nombre de usuario y contraseña**. Además, debe introducir un **nombre** de licencia. Se necesita un archivo de licencia sin conexión para activar la herramienta Mirror y generar el mirror de actualización.



- Antes de ejecutar la herramienta Mirror, deberá tener los siguientes paquetes instalados:
- Visual C++ Redistributable para Visual Studio 2010
- Visual C++ 2015 Redistributable x86

Uso de la herramienta Mirror

1.Descargue la herramienta Mirror de la página de descargas de ESET (sección **Instaladores independientes**).

2.Descomprima el archivo comprimido descargado.

3.Abra el símbolo del sistema y vaya a la carpeta con el archivo *MirrorTool.exe*.

4.Ejecute el comando que aparece a continuación para ver todos los parámetros disponibles de la herramienta Mirror y su versión:

```
MirrorTool.exe --help
```

```
C:\Users\                    >MirrorTool.exe --help
Mirror Tool v1.0.1294.0, Copyright (c) ESET, spol. s r.o. 1992-2021. All rights
reserved.
Allowed options:
  --mirrorType arg                      [required for module update]
                                        Type of mirror. Possible values (case
                                        insensitive): regular, pre-release,
                                        delayed.
  --intermediateUpdateDirectory arg     [required for module update]
                                        Files will be downloaded to this
                                        directory to create mirror in output
                                        directory.
  --offlineLicenseFilename arg          [required for module update]
                                        Offline license file.
  --updateServer arg                    [optional]
                                        Update server. (e.g.:
                                        http://update.eset.com/eset_upd/ep6/)
                                        Mirror will be created in output
                                        directory, only specified path in
                                        server will be mirrored.
  --outputDirectory arg                 [required for module update]
                                        Directory where mirror will be created.
  --proxyHost arg                       [optional]
                                        Http proxy address (fqdn or IP).
  --proxyPort arg                       [optional]
                                        Http proxy port.
  --proxyUsername arg                   [optional]
                                        Http proxy username.
  --proxyPassword arg                   [optional]
                                        Http proxy password.
  --networkDriveUsername arg            [optional]
                                        Username used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --networkDrivePassword arg            [optional]
                                        Password used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --excludedProducts arg                [optional]
                                        Disable creating mirror for specified
                                        products. Use --listUpdatableProducts
                                        to see possible values.
  --listUpdatableProducts               Show list of all products which modules
                                        are downloaded by default.
  --repositoryServer arg                [required for repository update]
                                        Repository server for repository
                                        creation.
  --intermediateRepositoryDirectory arg [required for repository update]
                                        Files will be downloaded to this
                                        directory to create offline mirror in
                                        output directory.
  --outputRepositoryDirectory arg       [required for repository update]
                                        Directory where offline repository will
                                        be created.
  --trustDownloadedFilesInRepositoryTemp
                                        [optional]
                                        If set, hashes on already downloaded
                                        files are not checked.
  --mirrorOnlyLevelUpdates              [optional]
                                        If set, only level upgrades will be
                                        downloaded (nano/continuous updates
                                        will not be downloaded)
  --mirrorFileFormat arg                [optional]
                                        Specifies which type of update files
                                        will be downloaded. Possible values
                                        (case insensitive): dll, dat.
  --compatibilityVersion arg            [optional]
                                        Version of compatible products.
  --filterFilePath arg                  [optional]
                                        Path to filter file in json format.
                                        Parameter compatibilityVersion has to
                                        be higher than 7.1.0.0 to run program.
  --dryRun arg                          [optional]
                                        Specifies dry run of program with path
                                        to csv file where will be saved list of
                                        products to be downloaded with current
                                        filter configuration.
  --help                                [optional]
                                        Display this help and exit
```

Todos los filtros distinguen entre mayúsculas y minúsculas.

Parámetro	Descripción
`--updateServer`	Cuando lo utilice, debe especificar la URL completa del servidor de actualización.
`--offlineLicenseFilename`	Debe especificar una ruta de su archivo de licencia sin conexión (como se mencionó anteriormente).
`--mirrorOnlyLevelUpdates`	No se necesita argumento. Si se selecciona esta opción, solo se descargarán las actualizaciones de nivel (las actualizaciones nano no se descargarán). Obtenga más información sobre los tipos de actualización en el artículo de la base de conocimiento.
`--mirrorFileFormat`	Antes de utilizar el parámetro `--mirrorFileFormat`, asegúrese de que el entorno no contenga versiones de los productos de seguridad de ESET más antiguas (6.5 y anteriores) y más recientes (6.6 y posteriores). El uso incorrecto de este parámetro puede actualizar de forma incorrecta los productos de seguridad de ESET. Puede especificar qué tipo de archivos de actualización se descargarán. Valores posibles (se distingue entre mayúsculas y minúsculas): • `dat`: utilice este valor si el entorno solo tiene versiones del producto de seguridad de ESET 6.5 y anteriores. • `dll`: utilice este valor si el entorno solo tiene versiones del producto de seguridad de ESET 6.6 y posteriores. El parámetro se ignora al crear un Mirror para productos heredados (`ep4`, `ep5`).
`--compatibilityVersion`	Este parámetro opcional se aplica a la herramienta Mirror distribuida con ESET PROTECT 8.1 y versiones posteriores. La herramienta Mirror descargará los archivos de actualización compatibles con la versión del repositorio de ESET PROTECT que haya especificado en el argumento del parámetro en formato `x.x` o `x.x.x.x`, por ejemplo: `--compatibilityVersion 9.1` o `--compatibilityVersion 8.1.13.0`.

Para reducir la cantidad de datos descargados del repositorio de ESET, se recomienda utilizar los nuevos parámetros de la herramienta Mirror distribuidos con ESET PROTECT 9: `--filterFilePath` y `--dryRun`:
1.Cree un filtro con formato *JSON* (consulte `--filterFilePath` a continuación).
2.Realice una ejecución de prueba de la herramienta Mirror con el parámetro `--dryRun` (véase a continuación) y ajuste el filtro según sea necesario.
3.Ejecute la herramienta Mirror con el parámetro `--filterFilePath` y el filtro de descarga definido, junto con los parámetros `--intermediateRepositoryDirectory` y `--outputRepositoryDirectory`.
4.Ejecute la herramienta Mirror periódicamente para utilizar siempre los instaladores más recientes.

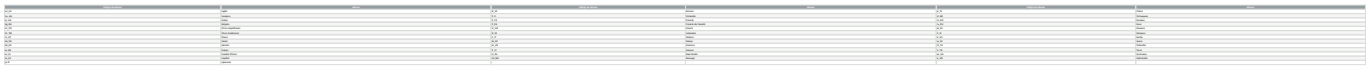
Parámetro	Descripción

`--filterFilePath`	Utilice este parámetro opcional para filtrar los productos de seguridad de ESET en función de un archivo de texto en formato *JSON* situado en la misma carpeta que la herramienta Mirror, por ejemplo: `--filterFilePath filter.txt`).
	Descripción de la configuración del filtro:
	El formato de los archivos de configuración para el filtrado de productos es *JSON* con la siguiente estructura:
	• objeto *JSON* raíz:
	o`use_legacy` (booleano, opcional): si es true, se incluirán los productos heredados.
	o`defaults` (objeto *JSON*, opcional): define las propiedades de filtro que se aplicarán a todos los productos.
	■`languages` (lista): especifica los códigos de idioma ISO de los idiomas que se van a incluir; por ejemplo, para francés, `"fr_FR"`. En la siguiente tabla puede consultar otros códigos de idioma: Para seleccionar más idiomas, sepárelos con una coma y un espacio, por ejemplo: (`["en_US", "zh_TW", "de_DE"]`)
	■`platforms` (lista): plataformas que se van a incluir (`["x64", "x86", "arm64"]`).
	⚠ Utilice el filtro `platforms` con prudencia. Por ejemplo, si la herramienta Mirror descarga solo instaladores de 64 bits y hay ordenadores de 32 bits en su infraestructura, los productos de seguridad de ESET de 64 bits no se instalarán en los ordenadores de 32 bits.
	
	■`os_types` (lista): tipos de sistema operativo que se van a incluir (`["windows"]`, `["linux"]`, `["mac"]`).
	o`products` (lista de objetos JSON, opcional): filtros que se aplican a productos específicos; anulan `defaults` para los productos especificados. Los objetos tienen las siguientes propiedades:
	■`app_id` (cadena): obligatoria si `name` no se especifica.
	■`name` (cadena): obligatoria si `app_id` no se especifica.
	■`version` (cadena): especifica la versión o la serie de versiones que se van a incluir.
	■`languages` (lista): códigos de idioma ISO de los idiomas que se van a incluir (consulte la tabla que aparece a continuación).
	■`platforms` (lista): plataformas que se van a incluir (`["x64", "x86", "arm64"]`).
	■`os_types` (lista): tipos de sistema operativo que se van a incluir (`["windows"]`, `["linux"]`, `["mac"]`).
	ℹ Para determinar los valores adecuados para los campos, ejecute la herramienta Mirror en el modo de simulacro y busque el producto correspondiente en el archivo CSV creado.
	Descripciones del formato de la cadena de versión
	Todos los números de versión están compuestos por cuatro cifras separadas por puntos (por ejemplo, `7.1.0.0`). Al introducir filtros de versión puede especificar menos cifras (por ejemplo, `7.1`) y el resto de números será cero (`7.1` será igual a `7.1.0.0`).
	La cadena de versión puede tener uno de los dos formatos siguientes:
	• [>|<|>=|<=|=]<n>.(<n>.(<n>.(<n>)))
	oSelecciona las versiones posteriores/anteriores, iguales/anteriores o iguales/iguales a la versión especificada.
	• <n>.(<n>.(<n>.(<n>))) - <n>.(<n>.(<n>.(<n>)))
	oSelecciona las versiones posteriores o iguales al límite inferior, y anteriores o iguales al límite superior.
	Se realizan comparaciones numéricas en cada parte del número de versión, de izquierda a derecha.
	Ejemplo de JSON
	✓
	`{`
	`"use_legacy": true,`
	`"defaults": {`
	`"languages": [ "en_US" ],`
	`"platforms": [ "x64", "x86" ]`
	`},`
	`"products": [`
	`{`
	`"app_id": "com.eset.apps.business.ees.windows",`
	`"version": "7.1.0.0 - 8.0.0.0"`
	`},`
	`{`
	`"app_id": "com.eset.apps.business.eea.windows",`
	`"version": ">7.1.0.0"`
	`}`
	`]`
	`}`
	El parámetro `--filterFilePath` sustituye a los parámetros `--languageFilterForRepository`, `--productFilterForRepository` y `--downloadLegacyForRepository` utilizados en versiones anteriores de la herramienta Mirror (distribuida con ESET PROTECT 8.x).

Parámetro	Descripción
`--dryRun`	Si utiliza este parámetro opcional, la herramienta Mirror no descargará ningún archivo, pero generará un archivo *.csv* con una lista de todos los paquetes que se descargarán. Puede utilizar este parámetro sin los parámetros obligatorios `--intermediateRepositoryDirectory` y `--outputRepositoryDirectory`, por ejemplo: `MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv`. Algunos instaladores de ESET son genéricos en cuanto al idioma (con el código de idioma `multilang`) y la herramienta Mirror los incluirá en el archivo *.csv* aunque se especifiquen `idiomas` en `--filterFilePath`. Si utiliza el parámetro `--dryRun` y también los parámetros `--intermediateRepositoryDirectory` y `--outputRepositoryDirectory`, la herramienta Mirror no borra el *outputRepositoryDirectory*.
`--listUpdatableProducts`	Enumerar todos los productos ESET para los que Mirror Tool puede descargar actualizaciones de los módulos (a menos que se utilice `--excludedProducts`). El parámetro está disponible en las versiones Mirror Tool: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).

La herramienta Mirror crea una estructura de carpetas distinta de la que crea el mirror de Endpoint. Cada carpeta contiene archivos de actualización para un grupo de productos. Tiene que especificar la ruta de acceso completa a la carpeta correcta en la configuración de actualización del producto usando el mirror. Por ejemplo, para actualizar ESET PROTECT 9 desde el mirror, establezca el servidor de actualización en (según la ubicación raíz de su servidor HTTP):
`http://your_server_address/mirror/eset_upd/era6`
Nota: La carpeta mirror de `era6` es común para estas soluciones de administración remota de ESET: ERA 6, ESMC 7, ESET PROTECT.

Tabla de códigos de idioma



```
MirrorTool.exe --mirrorType regular ^
--intermediateUpdateDirectory c:\temp\mirrorTemp ^
--offlineLicenseFilename c:\temp\offline.lf ^
--outputDirectory c:\temp\mirror
```

Este es un ejemplo de configuración más avanzada para un repositorio sin conexión con los productos y los idiomas seleccionados y la descarga de archivos heredados activada definida en el archivo *filter.txt* (consulte el ejemplo de contenido de archivo en los detalles de `--filterFilePath` anteriores):

```
MirrorTool.exe --repositoryServer AUTOSELECT ^
--intermediateRepositoryDirectory c:\temp\repoTemp ^
--outputRepositoryDirectory c:\temp\repository ^
--filterFilePath filter.txt
```

Herramienta Mirror y configuración de actualización

- Para automatizar la descarga de módulos, puede crear un programa para ejecutar la herramienta Mirror. Para hacerlo, abra Web Console y navegue hasta **Tareas del cliente** > **Sistema operativo** > **Ejecutar comando. Seleccione Línea de comandos para ejecutar** (incluida la ruta de acceso al archivo *MirrorTool.exe*) y un desencadenador razonable (por ejemplo, CRON para cada hora 0 0 * * * ? *). Asimismo, puede utilizar el Programador de tareas de Windows o `Cron` en Linux.

- Para configurar actualizaciones en ordenadores cliente, cree una nueva política y configure el **Servidor de actualización** para que apunte a su dirección mirror o carpeta compartida.

Si está utilizando un servidor Mirror HTTPS, tendrá que importar su certificado en el almacén raíz de confianza del equipo cliente. Consulte Instalación del certificado raíz de confianza en Windows.

Lea este artículo de la Base de conocimiento para configurar el encadenado de la Herramienta Mirror (configurar la Herramienta Mirror para descargar las actualizaciones de otra Herramienta Mirror).

Instalación del Conector del dispositivo móvil – Windows

el Conector del dispositivo móvil debe estar disponible a través de Internet para que los dispositivos móviles pueden administrarse en todo momento independientemente de su ubicación.

Le recomendamos que implemente el componente de MDM en un dispositivo host distinto al que se aloja ESET PROTECT Server.

Siga los pasos indicados a continuación para instalar el componente Mobile Device Connector para ESET PROTECT Server en Windows:

Asegúrese de cumplir todos los requisitos previos de la instalación.

1. Visite la sección de descargas de ESET PROTECT para descargar un instalador independiente de este componente de ESET PROTECT (*mdmcore_x64.msi*).

2. Ejecute el instalador del Conector de dispositivo móvil y acepte el EULA si está de acuerdo con él.

3. Haga clic en **Examinar**, diríjase hasta la ubicación de su certificado SSL para comunicación a través de HTTPS, escriba la contraseña de este certificado.

4. Especifique el **Nombre de host MDM**: este es el dominio público o la dirección IP pública de su servidor MDM, accesible para los dispositivos móviles desde Internet.

El nombre de host de MDM debe introducirse de la forma especificada en su **certificado del servidor HTTPS**; de lo contrario, el dispositivo móvil iOS rechazará la instalación del perfil MDM. Por ejemplo, si se ha especificado una dirección IP en el certificado HTTPS, escriba esta dirección IP en el campo **Nombre de host MDM**. Si se especifica un FQDN (por ejemplo, `mdm.mycompany.com`) en el certificado HTTPS, especifique este FQDN en el campo **Nombre de host MDM**. Además, si se emplea un comodín * (por ejemplo, `*.mycompany.com`) en el certificado HTTPS, puede utilizar `mdm.mycompany.com` en el campo **Nombre de host MDM**.

5. El instalador ahora debe conectarse a una base de datos existente que utilizará el Conector del dispositivo móvil. Especifique los siguientes datos de conexión:

- **Base de datos**: MySQL Server/MS SQL Server/MS SQL Server mediante autenticación de Windows
- **Controlador de ODBC**: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/MySQL ODBC 8.0 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 para SQL Server/ODBC Driver 13 para SQL Server/ODBC Driver 17 para SQL Server/ODBC Driver 18 para SQL Server
- **Nombre de la base de datos**: Se recomienda utilizar el nombre predefinido o cambiarlo si es necesario.
- **Nombre de host**: nombre del host o dirección IP del servidor de base de datos
- **Puerto**: se utiliza para conectar al servidor de base de datos
- **Nombre de usuario/Contraseña** de la cuenta admin de la base de datos
- **Usar instancia con nombre**: si está utilizando una base de datos de MS SQL, también puede marcar la casilla de verificación **Usar instancia con nombre** para usar una instancia de la base de datos personalizada. Puede configurarlo en el campo **Nombre del host** con el formato *NOMBRE_HOST**INSTANCIA_BD* (por ejemplo, *192.168.0.10**ESMC7SQL*). Para las bases de datos en clústeres utilice únicamente el nombre de clúster. Si se selecciona esta opción, no podrá cambiar el puerto de conexión de la base de datos; el sistema utilizará los puertos predeterminados que Microsoft ha definido. Para conectar ESET PROTECT Server a la base de datos de MS SQL instalada en un clúster de conmutación por error, escriba el nombre del clúster en el campo **Nombre del host**.

> Puede utilizar el mismo servidor de bases de datos que está utilizando para la base de datos de ESET PROTECT, pero se recomienda utilizar un servidor de bases de datos distinto, si tiene previsto inscribir más de 80 dispositivos móviles.

6. Especifique el usuario de la base de datos del Conector de dispositivo móvil que acaba de crear. Puede **Crear usuario nuevo** o **Usar usuario de la base de datos existente**. Escriba la contraseña del usuario de la base de datos.

7. Introduzca el **Host del servidor** (nombre o dirección IP de su ESET PROTECT Server) y el **Puerto de servidor** (el puerto predeterminado es el 2222, si utiliza un puerto distinto, cambie el puerto predeterminado por su número de puerto personalizado).

8. Conecte el Conector MDM a ESET PROTECT Server. Complete los campos **Host del servidor** y **Puerto del servidor** necesarios para la conexión a ESET PROTECT Server y seleccione **Instalación ayudada por el servidor** o **Instalación sin conexión** para continuar:

- **Instalación ayudada por el servidor**: facilite las credenciales de administrador de ESET PROTECT Web Console y el instalador descargará los certificados necesarios automáticamente. Compruebe también los permisos necesarios para la instalación ayudada por el servidor.

    1.Introduzca el nombre del **Host del servidor** o la dirección IP de ESET PROTECT Server y el **Puerto de Web Console** (si no utiliza un puerto personalizado, conserve el puerto predeterminado 2223). Facilite también las credenciales de la cuenta de administrador de Web Console (**Nombre de usuario/Contraseña**).

2.Cuando aparezca el mensaje Aceptar certificado, haga clic en **Sí**. Continúe con el paso 10.

- **Instalación sin conexión**: facilite un **Certificado del proxy** y **Autoridad certificadora** que pueda exportarse desde ESET PROTECT. También puede usar su certificado personalizado y la Autoridad certificadora adecuada.

1.Haga clic en **Examinar** junto al Certificado de igual y desplácese hasta la ubicación del **Certificado de igual** (el certificado del proxy que exportó desde ESET PROTECT). Mantenga el campo de texto **Contraseña del certificado** en blanco, ya que este certificado no necesita contraseña.

2.Repita el procedimiento para la Autoridad certificadora y continúe con el paso 10.

Si está utilizando certificados personalizados con ESET PROTECT (en lugar de los predeterminados que se generaron automáticamente durante la instalación de ESET PROTECT), se deben utilizar cuando se le pida que suministre un certificado de proxy.

9. Especifique la carpeta de destino del Conector del dispositivo móvil (se recomienda utilizar la ubicación predeterminada), haga clic en **Siguiente** y, a continuación, en **Instalar**.

10. Cuando la instalación finalice, compruebe si el Conector del dispositivo móvil funciona correctamente abriendo *https://your-mdm-hostname:enrollment-port* (por ejemplo *https://mdm.company.com:9980*) desde su navegador web o dispositivo móvil. Si la instalación se completó correctamente, se mostrará el siguiente mensaje: MDM: servidor activo y en funcionamiento

11. Ya puede activar MDM desde ESET PROTECT.

Requisitos previos del Conector del dispositivo móvil

Si el puerto o el nombre de host del servidor MDM cambia, todos los dispositivos móviles se volverán a inscribir.
Por ello, se recomienda que configure un nombre de host dedicado para el servidor MDM de forma que, si alguna vez tiene que cambiar el dispositivo host del servidor MDM, pueda hacerlo al reasignar la dirección IP del nuevo dispositivo host al nombre de host MDM de su configuración de DNS.

Se deben cumplir los siguientes requisitos para poder instalar el Conector de dispositivo móvil en Windows:

- Dirección IP pública/nombre de host o dominio público a los que puede accederse desde Internet.

Si necesita cambiar el nombre de host de su servidor MDM, tendrá que ejecutar una instalación de reparación del componente MDC. Si cambia el nombre de host de su servidor MDM, tendrá que importar un nuevo **certificado del servidor HTTPS** que incluya este nuevo nombre de host para que MDM pueda seguir funcionando correctamente.

- Puertos abiertos y disponibles, vea la lista completa de puertos aquí. Se recomienda utilizar los números de puerto predeterminados 9981 y 9980, aunque también pueden cambiarse en el archivo de configuración de su servidor MDM si es necesario. Asegúrese de que los dispositivos móviles puedan conectarse a través de puertos especificados. Cambie la configuración del cortafuegos y/o la red (si procede) para permitir esta comunicación. Más información acerca de la arquitectura MDM.

- Configuración del firewall: si instala Conector de dispositivo móvil en un sistema operativo que no es para servidores, como Windows 7 (solo con fines de evaluación), asegúrese de permitir los puertos de comunicación mediante la creación de reglas de firewall para:

C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, puerto TCP 9980

C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, puerto TCP 9981

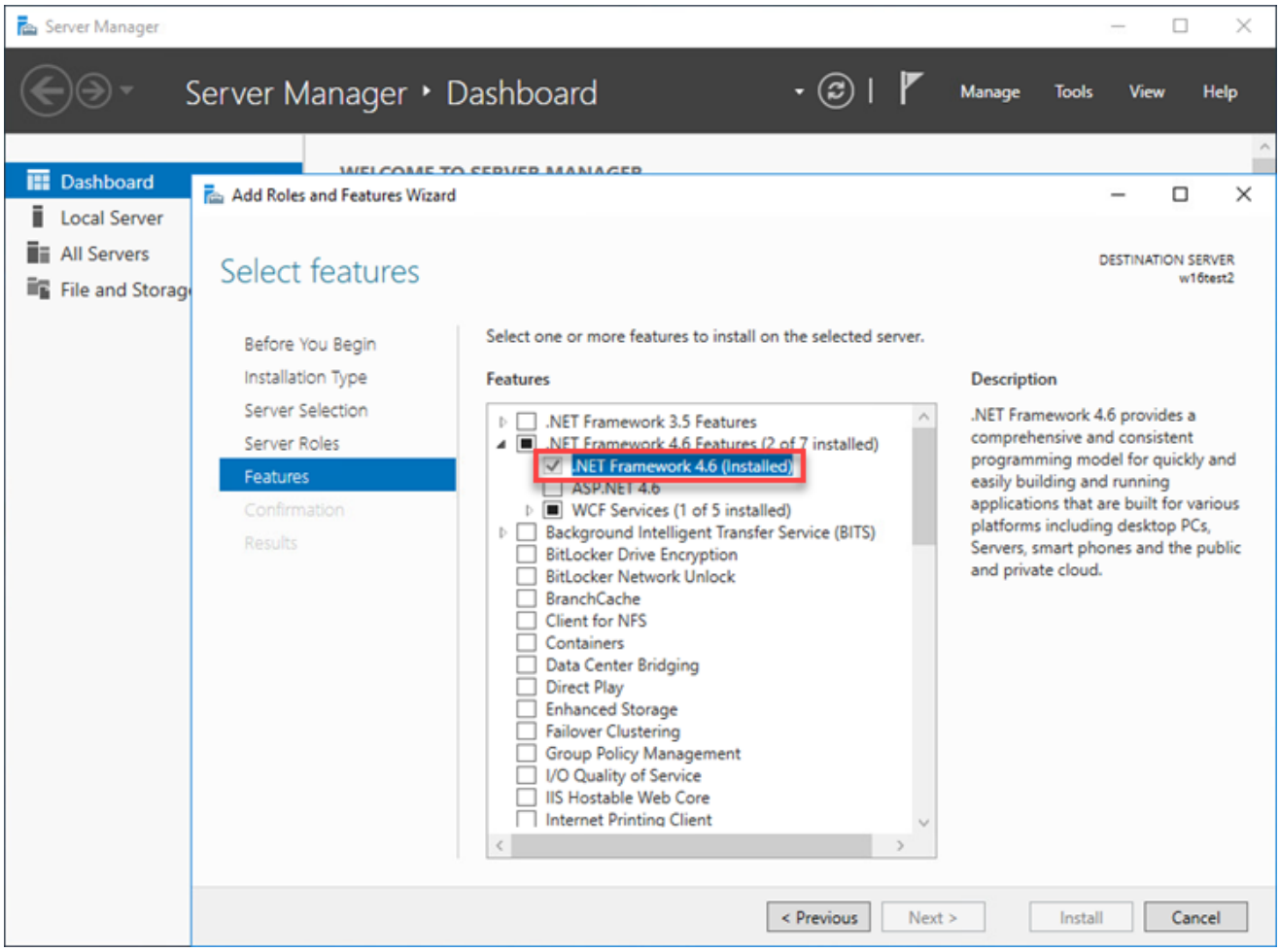
C:\Program Files\ESET\RemoteAdministrator\Server\ERAServer.exe, puerto TCP 2222

> Las rutas de acceso reales a los archivos *.exe* podrían variar en función de la ubicación de instalación de los componentes de ESET PROTECT en el sistema operativo de su cliente.

- Un servidor de base de datos ya instalado y configurado. Asegúrese de que cumple los requisitos de Microsoft SQL o MySQL.

- El uso de memoria RAM del conector MDM se ha optimizado, por lo que pueden ejecutarse hasta 48 procesos "Módulo MDMCore de ESET PROTECT" al mismo tiempo y si el usuario conecta más dispositivos, los procesos cambiarán de forma periódica en cada dispositivo que necesite actualmente utilizar los recursos.

- La instalación de MS SQL Server Express requiere Microsoft .NET Framework 4. Puede instalarlo con el **Asistente para agregar roles y características**:



Requisitos del certificado

- Necesitará un **certificado SSL** en formato *.pfx*para establecer una comunicación segura a través de HTTPS. Se recomienda utilizar el certificado proporcionado por una autoridad certificadora externa. No se recomienda el uso de certificados autofirmados (incluidos los certificados firmados por la autoridad certificadora de ESET PROTECT), ya que no todos los dispositivos móviles permiten a los usuarios aceptar

certificados autofirmados.

- Debe tener un certificado firmado por una autoridad certificadora y la clave privada correspondiente, y utilizar procedimientos estándar, para fusionarlos (tradicionalmente con OpenSSL) para combinarlos en un archivo *.pfx*:
```
openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out
httpsCredentials.pfx
```
Se trata de un procedimiento estándar para la mayoría de los servidores que utilizan certificados SSL.

- Para la instalación sin conexión, también necesitará un certificado de igual (el **certificado del agente** exportado desde ESET PROTECT). También puede usar su certificado personalizado con ESET PROTECT.

Activación del Conector del dispositivo móvil

Tras instalar el Conector del dispositivo móvil, tendrá que activarlo con la licencia de ESET Endpoint, Business u Office:

1. Agregue la licencia de ESET Endpoint, Business u Office a la Administración de licencias de ESET PROTECT.

2. Active Mobile Device Connector utilizando tareas del cliente de Activación del producto. Este procedimiento es el mismo que el de activación de cualquier producto de ESET en un ordenador cliente, solo que en este caso el ordenador cliente es el Conector del dispositivo móvil.

Función de concesión de licencias de MDM para iOS

Como ESET no ofrece una aplicación en Apple App Store, el Conector del dispositivo móvil de ESET almacena todos los datos de licencias de los dispositivos iOS.

Las licencias son por dispositivo y pueden activarse utilizando la tarea Activación del producto (igual que en Android).

Las licencias de iOS se pueden desactivar de las siguientes formas:

- Eliminación del dispositivo de la función de administración mediante la tarea Detener administración.
- Desinstalación de MDC mediante la opción **Eliminar base de datos**.
- Desactivación por otros métodos (ESET PROTECT o desactivación en EBA)

Como MDC se comunica con los servidores de licencias de ESET en nombre de los dispositivos iOS, el portal EBA refleja el estado del MDC y no el de dispositivos concretos. La información sobre el dispositivo actual está siempre disponible en ESET PROTECT Web Console.

Los dispositivos que no se activan o los dispositivos con licencias caducadas mostrarán un estado de protección rojo y el mensaje "El producto no está activado". Estos dispositivos rechazarán la gestión de tareas, el establecimiento de políticas y la entrega de registros no críticos.

Durante la desinstalación de MDM, si se selecciona **No quitar la base de datos**, las licencias en uso no se desactivarán. Estas licencias pueden reutilizarse si MDM vuelve a instalarse en esta base de datos, quitarse a través de ESET PROTECT o mediante la desactivación en EBA. Si se traslada a otro servidor MDM, deberá volver a llevar a cabo la tarea Activación del producto.

Requisitos del certificado HTTPS

Para inscribir un dispositivo móvil en el Conector del dispositivo móvil de ESET, asegúrese de que el servidor HTTPS devuelve toda la cadena del certificado.

Para que el certificado funcione correctamente se deben cumplir estos requisitos:

- El certificado HTTPS (contenedor pkcs#12/pfx) debe incluir toda la cadena del certificado, incluida la autoridad emisora del certificado raíz.
- El certificado debe ser válido durante el tiempo necesario (válido desde/válido hasta).
- El **CommonName** o los **subjectAltName** deben coincidir con el nombre de host de MDM.

Si el **Nombre de host de MDM** es, por ejemplo, hostname.mdm.domain.com, el certificado puede contener nombres como:
- hostname.mdm.domain.com
- *.mdm.domain.com

Pero no nombres como:
- *
- *.com
- *.domain.com

Básicamente, "*" no puede usarse para sustituir al "punto". Este comportamiento se confirma por la forma en la que iOS acepta los certificados de MDM.

Recuerde que algunos dispositivos tienen en cuenta su zona horaria al comprobar la validez del certificado, mientras que otros dispositivos no tienen en cuenta esta información. Para evitar posibles problemas, defina la validez del certificado uno o dos días antes de la fecha actual.

Instalación y almacenamiento en caché del proxy HTTP Apache

Acerca del proxy HTTP Apache

El proxy HTTP Apache puede usarse con varios fines:

Función	Solución proxy que proporciona esta función
Almacenamiento en caché de descargas y actualizaciones	Proxy HTTP Apache uotra solución proxy
Almacenamiento en caché de los resultados de ESET LiveGuard Advanced	Solo proxy HTTP Apache configurado
Replicación de la comunicación de las instancias de ESET Management Agent con ESET PROTECT Server	Proxy HTTP Apache uotra solución proxy

si ya tiene el proxy HTTP Apache instalado en Windows y desea actualizarlo a la versión más reciente, continúe con Actualización del proxy HTTP Apache.

Función de almacenamiento en caché del proxy HTTP Apache

Apache HTTP Proxydescarga y almacena en caché:

- Actualizaciones del módulo ESET
- Paquetes de instalación de los servidores de repositorio
- Actualizaciones del componente del producto

Los datos almacenados en caché se distribuyen a los clientes de punto de acceso de la red. El almacenamiento en caché puede reducir considerablemente el tráfico de Internet en la red.

Puede optar por instalar Squid como alternativa al proxy HTTP Apache.

Puede instalar el proxy HTTP Apache en Windows de dos maneras:

- Instalación desde el instalador todo en uno
- Instalación con el instalador independiente

Instalación con el instalador independiente

1. Visite la sección de descargas de ESET PROTECT para descargar un instalador independiente de este componente de ESET PROTECT (*apachehttp.zip*).

2. Abra *ApacheHttp.zip* y extraiga los archivos en *C:\Program Files\Apache HTTP Proxy 2.[x.xx]*

Si desea instalar el proxy HTTP Apache en una unidad de disco duro diferente, *C:\Program Files* debe sustituirse por la ruta de acceso correspondiente en las siguientes instrucciones y en el archivo *httpd.conf* ubicado en el directorio *Apache HTTP Proxy\conf*. Por ejemplo, si extrae el contenido de *ApacheHttp.zip* en *D:\Apache Http Proxy*, *C:\Program Files* deberá sustituirse por *D:\Apache Http Proxy*.

3. Abra un símbolo del sistema de administración y cambie el directorio a *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin*

4. Ejecute el siguiente comando:

```
httpd.exe -k install -n ApacheHttpProxy
```

5. Inicie el servicio de **ApacheHttpProxy** con el siguiente comando:

```
sc start ApacheHttpProxy
```

6. Puede verificar que el servicio de Apache HTTP Proxy se está ejecutando en el snap-in `services.msc` (busque **ApacheHttpProxy**). De forma predeterminada, el servicio está configurado para iniciarse automáticamente.

Tras la instalación, configure el proxy HTTP Apache para la funcionalidad que desee.

Configuración del proxy HTTP Apache

El instalador del proxy HTTP Apache proporcionado por ESET está preconfigurado. No obstante, tendrá que modificar determinados ajustes para que el servicio funcione correctamente.

Configuración del proxy HTTP Apache para replicación (agente-servidor)

1. Modifique el archivo de configuración de *Apache HTTP Proxy httpd.conf*, situado en *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf*.

    a.De forma predeterminada, se utiliza el puerto 2222 para la comunicación con ESET Management Agent. Si ha cambiado el puerto durante la instalación, utilice el número de puerto modificado. Cambie 2222 en la línea `AllowCONNECT 443 563 2222 8883 53535` por su número de puerto.

    b.Añadir otro segmento `ProxyMatch`:

        I.La dirección que sus agentes utilizan para conectarse a ESET PROTECT Server.

        II.El resto de direcciones posibles de su ESET PROTECT Server (IP, FQDN)
        (agregue todo el código que aparece a continuación; la dirección IP 10.1.1.10 y el nombre de host `hostname.example` son simplemente ejemplos que debe sustituir con sus direcciones. También puede generar la expresión `ProxyMatch` como se explica en este artículo de la Base de conocimiento.)

```
<ProxyMatch ^(hostname\.example(:[0-9]+)?(\/.*)?|10\.1\.1\.10(:[0-9]+)?(\/.*)?)$>
Allow from all
</ProxyMatch>
```

    c.Reinicie el servicio *Apache HTTP Proxy*.

2. Configure una política de agente adecuada para que sus agentes utilicen el proxy para la replicación.

Configuración del proxy HTTP Apache para el almacenamiento en caché

1. Detener el servicio de **ApacheHttpProxy** con el siguiente comando:

```
sc stop ApacheHttpProxy
```

2. Abra el archivo *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf* en un editor de texto simple. Agregue las siguientes líneas al final del archivo:

```
ServerRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]"
DocumentRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs">
Options Indexes FollowSymLinks
```

```
AllowOverride None

Require all granted

</Directory>

CacheRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\cache"
```

3. Guarde el archivo e inicie el servicio Apache.

```
sc start ApacheHttpProxy
```

> Si desea que el directorio de caché esté ubicado en otro lugar (por ejemplo, en otra unidad de disco, como `D:\Apache HTTP Proxy\cache`), en la última línea del código anterior, cambie `"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\cache"` por `"D:\Apache HTTP Proxy\cache"`.

Configuración del proxy HTTP Apache para el nombre de usuario y la contraseña

El ajuste de nombre de usuario y contraseña solo se puede usar para el almacenamiento en caché. La autenticación no es compatible con el protocolo de replicación que se usa en la comunicación entre el agente y el servidor.

1. Detenga el servicio **ApacheHttpProxy** abriendo un símbolo del sistema elevado y ejecutando el siguiente comando:

```
sc stop ApacheHttpProxy
```

2. Verifique la presencia de los siguientes módulos en *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf*:

```
LoadModule authn_core_module modules\mod_authn_core.dll

LoadModule authn_file_module modules\mod_authn_file.dll

LoadModule authz_groupfile_module modules\mod_authz_groupfile.dll

LoadModule auth_basic_module modules\mod_auth_basic.dll
```

3. Añada las siguientes líneas a *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf* debajo de `<Proxy *>`:

```
AuthType Basic

AuthName "Password Required"

AuthUserFile password.file

AuthGroupFile group.file

Require group usergroup
```

4. Utilice el comando `htpasswd` para crear un archivo llamado `password.file` en la carpeta *Apache HTTP Proxy\bin* (se le pedirá la contraseña):

```
htpasswd.exe -c ..\password.file username
```

5. Cree manualmente el archivo `group.file` en la carpeta *Apache HTTP Proxy* con el siguiente contenido:

```
usergroup:username
```

6. Inicie el servicio **ApacheHttpProxy** ejecutando el siguiente comando en un símbolo del sistema elevado:

```
sc start ApacheHttpProxy
```

7. Pruebe la conexión con el proxy HTTP; para ello acceda a la siguiente URL desde su navegador:

http://[IP address]:3128/index.html

Una vez instalado el proxy HTTP Apache correctamente, tiene la opción de permitir únicamente la comunicación de ESET y bloquear el resto del tráfico (opción predeterminada) o la opción de permitir todo el tráfico. Realice en la configuración los cambios necesarios que se describen a continuación:

- Reenvío solo para la comunicación de ESET
- Encadenado de proxy (todo el tráfico)

Visualizar una lista del contenido que está almacenado en la caché

"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\htcacheclean.exe" -a -p "C:\ProgramData\Apache HTTP Proxy\cache"

Utilice la herramienta htcacheclean para limpiar la caché del disco. Consulte el comando recomendado a continuación (configuración del tamaño de la memoria caché en 20 GB y el límite de los archivos almacenados en la memoria caché en ~128.000):

```
"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\htcacheclean.exe" -n -t^
-p"C:\ProgramData\Apache HTTP Proxy\cache" -l20000M -L128000
```

Para programar la limpieza de la memoria caché cada hora:

```
schtasks /Create /F /RU "SYSTEM" /SC HOURLY /TN ESETApacheHttpProxyCleanTask^
/TR "\"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\htcacheclean.exe\"^
-n -t -p \"C:\ProgramData\Apache HTTP Proxy\cache\" -l20000M -L128000"
```

Si opta por permitir todo el tráfico, los comandos recomendados son:

```
"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\htcacheclean.exe" -n -t^
-p"C:\ProgramData\Apache HTTP Proxy\cache" -l20000M

schtasks /Create /F /RU "SYSTEM" /SC HOURLY /TN ESETApacheHttpProxyCleanTask^
/TR "\"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\htcacheclean.exe\"^
-n -t -p \"C:\ProgramData\Apache HTTP Proxy\cache\" -l20000M"
```

El carácter ^ situado justo después del final de la línea en los comandos anteriores es esencial y, si no se incluye, el comando no se ejecutará correctamente.

Para obtener más información, visite nuestro artículo de la base de conocimiento o la documentación sobre autenticación y autorización de Apache.

Squid instalación en Windows y caché del proxy HTTP

Squid es una alternativa al proxy HTTP Apache. Para instalar Squid en Windows, siga estos pasos:

1. Descargue el instalador de Squid MSI e instale Squid.

2. Haga clic en el icono de **Squid for Windows** en el menú de la bandeja y seleccione **Stop Squid Service**.

3. Vaya a la carpeta de instalación de Squid, por ejemplo, C:\Squid\bin, y ejecute el siguiente comando en la línea de comandos:

```
squid.exe -z -F
```

Esto crea los directorios de intercambio para la caché.

4. Haga clic en el icono de **Squid for Windows** en el menú de la bandeja y seleccione **Open Squid Configuration**.

5. Cambie `http_access deny all` por `http_access allow all`.

6. Añada esta línea para activar el almacenamiento en caché en el disco:

```
cache_dir aufs /cygdrive/c/Squid/var/cache 3000 16 256
```

i
- Puede cambiar la ubicación del directorio de la caché según sus propias preferencias. En este ejemplo, el directorio de la caché es `C:\Squid\var\cache` (observe el formato de la ruta de acceso en el comando).
- También puede cambiar el tamaño total de la caché (3000 MB en el ejemplo) y el número de subdirectorios de primer nivel (16 en el ejemplo) y de subdirectorios de segundo nivel (256 en el ejemplo) en el directorio de la caché.

7. Guarde y cierre el archivo de configuración de Squid *squid.conf*.

8. Haga clic en el icono de **Squid for Windows** en el menú de la bandeja y seleccione **Start Squid Service**.

9. Puede verificar que el servicio Squid se está ejecutando en el complemento `services.msc` (busque **Squid for Windows**).

Repositorio sin conexión - Windows

Puede utilizar la herramienta Mirror para crear un repositorio sin conexión (en Windows). Normalmente esto es necesario en redes de ordenadores cerradas o redes con acceso limitado a Internet. La herramienta Mirror se puede usar para crear un clon del repositorio de ESET en una carpeta local. Este repositorio clonado puede moverse posteriormente (por ejemplo, a un disco externo) a una ubicación de la red cerrada. Puede copiar el repositorio en una ubicación segura de la red local y permitir el acceso al mismo a través del servidor HTTP.

Para actualizar el repositorio sin conexión, ejecute el mismo comando con los mismos parámetros empleados

para la creación del repositorio sin conexión. Se utilizarán los datos anteriores presentes en la carpeta intermediaria y solo se descargarán los archivos obsoletos.

Tenga en cuenta que el tamaño del repositorio crece y el directorio intermedio tendrá el mismo tamaño. Asegúrese de tener un mínimo de **1,2 TB** de espacio libre antes de iniciar este procedimiento.

Prácticas recomendadas

Consulte también el artículo de la base de conocimiento de ESET Prácticas recomendadas para usar ESET PROTECT en un entorno sin conexión.

Ejemplo para Windows

I. Crear clon del repositorio

1. Descargue la herramienta Mirror.

2. Extraiga la herramienta Mirror del archivo *.zip* descargado.

3. Prepare (cree) carpetas para:

   - archivos intermediarios
   - repositorio final

4. Abra el símbolo del sistema y cambie el directorio a la carpeta en la que se extrajo la herramienta Mirror (comando `cd`).

5. Ejecute el siguiente comando (cambie los directorios intermediarios y del repositorio de salida a las carpetas del paso 3):

```
MirrorTool.exe --repositoryServer AUTOSELECT ^
--intermediateRepositoryDirectory C:\Intermediary ^
--outputRepositoryDirectory C:\Repository
```

6. Una vez copiado el repositorio en la carpeta `outputRepositoryDirectory`, mueva la carpeta y su contenido a otro ordenador desde el que pueda acceder a su red cerrada.

II. Configurar el servidor HTTP

7. Debe haber un servidor HTTP ejecutándose en el ordenador de la red cerrada. Puede utilizar:

   - Apache HTTP Proxy del sitio de descargas de ESET (este caso)
   - otro servidor HTTP

8. Abra *apachehttp.zip* y extraiga los archivos en *C:\Program Files\Apache HTTP Proxy 2.[x.xx]*

9. Abra un símbolo del sistema de administración y cambie el directorio a *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin* (comando `cd`).

10. Ejecute el siguiente comando:

```
httpd.exe -k install -n ApacheHttpProxy
```

11. Con un editor de texto sencillo, abra el archivo *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf* y añada las siguientes líneas al final del archivo:

```
Listen 80
ServerRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]"
DocumentRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs">
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
CacheRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\cache"
```

12. Inicie el servicio de **ApacheHttpProxy** con el siguiente comando:

```
sc start ApacheHttpProxy
```

13. Compruebe si el servicio se está ejecutando abriendo *http://YourIPaddress:80/index.html* en su navegador web (sustituya *YourIPaddress* por la dirección IP de su ordenador).

III. Ejecutar el repositorio sin conexión

14. Cree una carpeta nueva para el repositorio sin conexión, por ejemplo, *C:\Repository.*

15. En el archivo *httpd.conf*, sustituya las siguientes líneas

```
DocumentRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs">
```

por la dirección de la carpeta del repositorio, como se indica a continuación:

```
DocumentRoot "C:\Repository"
<Directory "C:\Repository">
```

16. Copie el repositorio descargado en *C:\Repository* .

17. Reinicie el servicio de **ApacheHttpProxy** con el siguiente comando:

```
sc restart ApacheHttpProxy
```

18. Su repositorio sin conexión ya se ejecuta en la dirección *http://YourIPaddress* (por ejemplo, *http://10.1.1.10*).

19. Configure la nueva dirección del repositorio utilizando ESET PROTECT Web Console :

a.ESET PROTECT Server: haga clic en **Más** > **Configuración** > **Configuración avanzada** > **Repositorio** e introduzca la dirección del repositorio sin conexión en el campo **Servidor**.

b.ESET Management Agente: haga clic en **Políticas,** haga clic en la política del Agent > **Editar** > **Configuración** > **Configuración avanzada** > **Repositorio** > introduzca la dirección del repositorio sin conexión en el campo **Servidor**.

c.Productos ESET Endpoint (para Windows: haga clic en **Políticas**, haga clic en la política **ESET Endpoint para Windows** > **Editar** > **Configuración** > **Actualizar** > **Perfiles** > **Actualizaciones** > **Actualizaciones de módulos** > desmarque **Elegir automáticamente** e introduzca la dirección del repositorio sin conexión en el campo **Servidor personalizado**.

Clúster de conmutación por error - Windows

Los pasos de alto nivel necesarios para instalar ESET PROTECT en un entorno de clúster de conmutación por error son los siguientes.

Consulte también este artículo de la Base de conocimiento sobre la instalación de clústeres de ESET PROTECT Server.

1. Cree un clúster de conmutación por error con un disco compartido:

   - Instrucciones de creación de un clúster de conmutación por error en Windows Server 2016 e 2019
   - Instrucciones de creación de un clúster de conmutación por error en Windows Server 2012 e 2012 R2

2. En **Crear asistente de clúster**, introduzca el nombre de host (cree uno) y la dirección IP que desee.

3. Conecte el disco compartido del clúster en el nodo1 e instale ESET PROTECT Server utilizando el instalador independiente en el mismo. Asegúrese de seleccionar la opción **Esta es una instalación de clúster** durante la instalación, y seleccione el disco compartido como almacenamiento de datos de la aplicación. Cree un nombre de host e introdúzcalo en el certificado del servidor de ESET PROTECT Server junto a los nombres de host predefinidos. Recuerde este nombre de host y utilícelo en el paso n.º 6 cuando cree la función de ESET PROTECT Server en el administrador de clústeres.

4. Detenga ESET PROTECT Server en el nodo1, conecte el disco compartido del clúster en el nodo2 e instale ESET PROTECT Server utilizando el instalador independiente en el mismo. Asegúrese de que la opción **Esta es una instalación de clúster** esté seleccionada durante la instalación. Elija el disco compartido como almacenamiento de datos de la aplicación. No modifique la información de la conexión con la base de datos y el certificado, se configuró durante la instalación de ESET PROTECT Server en el nodo1.

5. Configure el firewall para permitir las conexiones entrantes en todos los puertos que utiliza ESET PROTECT Server.

6. En el administrador de configuración del clúster, cree e inicie un rol (**Configurar función** > **Seleccionar función** > **Servicio genérico**) para el servicio ESET PROTECT Server. Seleccione el servicio **ESET PROTECT Server** en la lista de servicios disponibles. Es muy importante utilizar el mismo nombre de host para la función, ya que se utilizó en el paso 3 del certificado del servidor.

7. Instale ESET Management Agent en todos los nodos del clúster utilizando el instalador independiente. Utilice en las pantallas **Configuración del agente** y **Conexión con ESET PROTECT Server** el nombre de host que utilizó en el paso número 6. Almacene los datos del agente en el nodo local (no en el disco del clúster).

8. El servidor web (Apache Tomcat) no es compatible con un clúster, por lo que debe instalarse en un disco que no esté en clúster o en un equipo diferente:

a.Instale Web Console en un ordenador independiente y configúrelo correctamente para conectarse al rol del clúster de ESET PROTECT Server.

b.Cuando se instale Web Console, localice su archivo de configuración en: *C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*

c.Abra el archivo con el Bloc de notas o con cualquier otro editor de texto. En la línea `server_address=localhost`, cambie localhost por la dirección IP o el nombre de host del rol del clúster de ESET PROTECT Server.

Instalación de componentes en Linux

En la mayoría de las situaciones de instalación, es necesario instalar los diferentes componentes de ESET PROTECTen diferentes máquinas para dar cabida a diferentes arquitecturas de red, cumplir con los requisitos de rendimiento, o por otras razones.

Siga las instrucciones de instalación de ESET PROTECT paso a paso.

Instalación de componentes principales

- ESET PROTECT Server
- ESET PROTECT Web Console – Puede seleccionar la instalación de ESET PROTECT Web Console en un ordenador distinto al ordenador donde se ha instalado ESET PROTECT Server.
- ESET Management Agent
- Un servidor de base de datos

Instalación de componentes opcionales

- RD Sensor
- Conector del dispositivo móvil
- Proxy HTTP Apache
- Herramienta Mirror

Si desea actualizar ESET PROTECT para Linux a la versión más reciente, consulte el capítulo Tarea Actualización de componentes o nuestro artículo de la base de conocimiento.

Instalación paso a paso del ESET PROTECT en Linux

En este contexto de instalación vamos a simular la instalación paso a paso de ESET PROTECT Server y ESET PROTECT Web Console. Vamos a simular el proceso de instalación con MySQL.

Instrucciones de instalación para distribuciones Linux concretas
Puede seguir los artículos de nuestra base de conocimiento con instrucciones específicas de cada distribución:
- CentOS 7
- Debian 10
- SUSE Linux Enterprise Server (SLES)

Antes de la instalación

1. Compruebe que el servidor de base de datos esté presente en su red y asegúrese de tener acceso al mismo en su servidor local/remoto. Si no hay ningún servidor de base de datos instalado, instale y configure uno nuevo.

2. Descargue los componentes independientes para Linux de ESET PROTECT (Agente, Servidor, Web Console). Puede encontrar estos archivos de instalación en la categoría Instaladores independientes de ESET PROTECT, disponible en el sitio web de ESET.

Proceso de instalación

Debe poder utilizar el comando `sudo` o realizar la instalación con privilegios `root` para completar la instalación.

1. Instale los paquetes necesarios para ESET PROTECT Server.

2. Configure la conexión al servidor de MySQL como se muestra en el tema Configuración de MySQL.

3. Compruebe la configuración del controlador ODBC de MySQL. Consulte Instalación y configuración de ODBC) para obtener más información.

4. Personalice los parámetros de instalación y ejecute la instalación de ESET PROTECT Server. Consulte Instalación del servidor - Linux para obtener más información.

5. Instale los paquetes de Java y Tomcat necesarios y, a continuación, instale ESET PROTECT Web Console. Si tiene problemas con la conexión HTTPS a ESET PROTECT Web Console, consulte Configuración de la conexión HTTPS/SSL.

6. Instale ESET Management Agent en el equipo servidor.

ESET le recomienda eliminar los comandos que contienen datos confidenciales (por ejemplo, una contraseña) del historial de la línea de comandos:
1.Ejecute `history` para ver una lista de todos los comandos del historial.
2.Ejecutar `history -d line_number` (especifique el número de línea del comando). También puede ejecutar `history -c` para eliminar todo el historial de la línea de comandos.

Instalación y configuración de MySQL

Instalación

Asegúrese de instalar una versión compatible de MySQL Server y el conector ODBC.

Si ya ha instalado y configurado MySQL, vaya a Configuración.

1. Agregue el repositorio MySQL:

Debian, Ubuntu	Ejecute los siguientes comandos en el terminal:
	`a)wget https://dev.mysql.com/get/mysql-apt-config_0.8.15-1_all.deb`
	`b)sudo dpkg -i mysql-apt-config_0.8.15-1_all.deb`
	Puede seleccionar las versiones de los componentes que desea instalar durante la instalación del paquete. Le recomendamos que seleccione las opciones predeterminadas. Consulte también Añadir el repositorio MySQL APT

CentOS, Red Hat	Añadir el repositorio MySQL Yum
OpenSuse, SUSE Linux Enterprise Server	Añadir el repositorio MySQL SLES

2. Actualice la caché del repositorio local:

Debian, Ubuntu	`sudo apt-get update`
CentOS, Red Hat	`sudo yum update`
OpenSuse, SUSE Linux Enterprise Server	`sudo zypper update`

3. La instalación de MySQL varía en función de la distribución Linux y de la versión utilizadas:

Linux distribución:	MySQL Comando de instalación del servidor:	MySQL Instalación avanzada del servidor:
Debian, Ubuntu	`sudo apt-get install mysql-server`	Instalación de MySQL desde el origen con el repositorio MySQL APT
CentOS, Red Hat	`sudo yum install mysql-community-server`	Instalación de MySQL en Linux con el repositorio MySQL Yum
OpenSuse, SUSE Linux Enterprise Server	`sudo zypper install mysql-community-server`	Pasos para una instalación nueva de MySQL

Descargue MySQL Community Server si desea realizar la instalación manualmente.

Configuración

1. Abra el archivo de configuración *my.cnf* en un editor de texto:

```
sudo nano /etc/my.cnf
```

Si no tiene el archivo, pruebe con `/etc/mysql/my.cnf` o `/etc/my.cnf.d/community-mysql-server.cnf` o `/etc/mysql/mysql.conf.d/mysqld.cnf`.

2. Busque la siguiente configuración en la sección `[mysqld]` del archivo configuración *my.cnf* y modifique los valores:

> - Cree la sección `[mysqld]` si no está presente en el archivo.
> - Si los parámetros no están presentes en el archivo, agréguelos a la sección `[mysqld]`.
> - Para determinar la versión de MySQL, ejecute el comando: `mysql --version`

Parámetro	Comentarios y valores recomendados	MySQL versión
`max_allowed_packet=33M`		Todas las versiones compatibles.
`log_bin_trust_function_creators=1`	También puede desactivar el inicio de sesión binario: `log_bin=0`	Versiones 8.x compatibles
`innodb_log_file_size=100M`	La multiplicación de los valores de estos dos parámetros debe dar como mínimo **200**. El valor mínimo de `innodb_log_files_in_group` es **2** y el valor máximo es **100**; el valor también debe ser un número entero.	Versiones 8x compatibles 5.7 5.6.22 (y posteriores 5.6.x)
`innodb_log_files_in_group=2`		
`innodb_log_file_size=200M`	Establezca el valor en **200M** como mínimo y **3000M** como máximo.	5.6.20 y 5.6.21

3. Pulse **CTRL + X** y escriba **Y** para guardar los cambios y cerrar el archivo.

4. Reinicie el servidor MySQL y aplique la configuración (en algunos casos, el nombre del servicio es `mysqld`):

```
sudo systemctl restart mysql
```

5. Configure los privilegios y la contraseña de MySQL (este paso es opcional y podría no funcionar en algunas distribuciones Linux):

a)Revele la contraseña temporal de MySQL: `sudo grep 'temporary password' /var/log/mysql/mysqld.log`

b)Copie y guarde la contraseña.

c)Establezca una contraseña nueva mediante una de las siguientes opciones:

- Ejecute `/usr/bin/mysql_secure_installation` y escriba la contraseña temporal. A continuación se le solicitará que cree una contraseña nueva.

- Ejecute `mysql -u root -p` y escriba la contraseña temporal. Ejecute `ALTER USER 'root'@'localhost' IDENTIFIED BY 'strong_new_password';` para cambiar la contraseña raíz (sustituya `strong_new_password` por su contraseña) y escriba `Quit`.

Consulte también Mejorar la seguridad de la instalación de MySQL en el Manual de referencia de MySQL.

6. Compruebe que el servicio mySQL Server se esté ejecutando:

```
sudo systemctl status mysql
```

Instalación y configuración de ODBC

Asegúrese de instalar una versión compatible de MySQL Server y el conector ODBC.

Puede instalar MS ODBC Driver (versión 13 y posteriores) para conectar ESET PROTECT Server en Linux con MS SQL Server en Windows. Para obtener más información, visite este artículo de la Base de conocimiento.

Instale el controlador ODBC de MySQL con el terminal. Siga los pasos indicados para su distribución Linux:

- Debian, Ubuntu
- CentOS 7
- Otras distribuciones de Linux compatibles

Debian, Ubuntu

1. Instalando unixODBC controladores:

```
sudo apt-get install unixodbc
```

2. Descargue el conector ODBC:

Ubuntu 16	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu16.04-x86-64bit.tar.gz`
Ubuntu 18	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu18.04-x86-64bit.tar.gz`
Ubuntu 20	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz`
Debian 10	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-debian10-x86-64bit.tar.gz`

- Seleccionar y descargar la versión compatible con su distribución y versión de Linux.
- Puede descargar el conector ODBC para MySQL del sitio oficial de MySQL.

3. Descomprima el archivo comprimido del controlador ODBC (el nombre del paquete cambia en función del vínculo utilizado):

```
gunzip mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz
```

4. Extraiga el controlador ODBC (el nombre del paquete cambia en función del vínculo utilizado):

```
tar xvf mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar
```

5. Vaya a la carpeta del controlador ODBC (el nombre del paquete cambia en función del vínculo utilizado):

```
cd mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit
```

6. Copie los archivos del controlador ODBC:

```
sudo cp bin/* /usr/local/bin
sudo cp lib/* /usr/local/lib
```

7. Registre el controlador de ODBC.

- En las nuevas versiones de Linux, como Ubuntu 20.x, se recomienda utilizar el controlador Unicode:

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0 Driver" -t
"Driver=/usr/local/lib/libmyodbc8w.so"
```

- En otros sistemas, o cuando el controlador Unicode no funciona:

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0" -t
"Driver=/usr/local/lib/libmyodbc8a.so"
```

8. Enumere los controladores instalados:

```
sudo myodbc-installer -d -l
```

Si desea obtener más información, consulte: https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-tarball.html.

CentOS 7

1. Instalando unixODBC controladores:

```
sudo yum install unixODBC -y
```

2. Descargue el conector ODBC:

```
wget
https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-1.e
l7.x86_64.rpm
```

- No instale el conector ODBC con YUM, ya que instalaría la versión no compatible más reciente.
- Seleccionar y descargar la versión compatible con su distribución y versión de Linux.
- Puede descargar el conector ODBC para MySQL del sitio oficial de MySQL.

3. Instalar ODBC controlador:

```
sudo rpm -ivh mysql-connector-odbc-8.0.17-1.e17.x86_64.rpm --nodeps
```

4. Configure el controlador ODBC:

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0.17" -t
"Driver=/usr/lib64/libmyodbc8w.so"
```

5. Enumere los controladores instalados:

```
sudo myodbc-installer -d -l
```

Otras distribuciones de Linux compatibles

- Seleccionar y descargar la versión compatible con su distribución y versión de Linux.
- Puede descargar el conector ODBC para MySQL del sitio oficial de MySQL.

1. Siga estas instrucciones para instalar el controlador ODBC:

- **OpenSuse, SUSE Linux Enterprise Server**: `sudo zypper install unixODBC`. Consulte también https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-rpm.html

- Instalación del conector/ODBC desde una distribución de tarball binario

2. Ejecute el siguiente comando para abrir el archivo *odbcinst.ini* en un editor de texto:

```
sudo nano /etc/odbcinst.ini
```

o `sudo nano/etc/unixODBC/odbcinst.ini`

3. Copie la siguiente configuración en el archivo *odbcinst.ini* (asegúrese de que las rutas de acceso a **Driver** y **Setup** sean correctas) y, a continuación, guarde y cierre el archivo:

```
[MySQL]
Description = ODBC for MySQL
Driver = /usr/lib/x86_64-linux-gnu/odbc/libmyodbc.so
Setup = /usr/lib/x86_64-linux-gnu/odbc/libodbcmyS.so
FileUsage = 1
```

El controlador podría encontrarse en un sitio diferente en algunas distribuciones. Puede encontrar el archivo utilizando el siguiente comando:

```
sudo find /usr -iname "*libmyodbc*"
```

4. Actualice los archivos de configuración que controlan el acceso de ODBC a servidores de bases de datos en el host actual ejecutando el siguiente comando:

```
sudo odbcinst -i -d -f /etc/odbcinst.ini
```

o `sudo odbcinst -i -d -f /etc/unixODBC/odbcinst.ini`

Instalación del servidor - Linux

Instrucciones de instalación para distribuciones Linux concretas
Puede seguir los artículos de nuestra base de conocimiento con instrucciones específicas de cada distribución:
- CentOS 7
- Debian 10
- SUSE Linux Enterprise Server (SLES)

Instalación

Siga los pasos indicados a continuación para instalar el componente ESET PROTECT Server en Linux con un comando de terminal:

Asegúrese de cumplir todos los requisitos previos de la instalación.

1. Descargue el componente ESET PROTECT Server:

```
wget https://download.eset.com/com/eset/apps/business/era/server/linux/latest/server
-linux-x86_64.sh
```

2. Haga que el archivo descargado sea ejecutable:

```
chmod +x server-linux-x86_64.sh
```

3. Puede preparar un script de instalación y luego ejecutarlo usando `sudo`.

Ejecute el script de instalación según el ejemplo mostrado a continuación (las líneas nuevas se dividen con "\" para copiar todo el comando en el terminal):

```
sudo ./server-linux-x86_64.sh \
--skip-license \
--db-type="MySQL Server" \
--db-driver="MySQL ODBC 8.0 Driver" \
```

```
--db-hostname=localhost \
--db-port=3306 \
--db-admin-username=root \
--db-admin-password=password \
--server-root-password=password \
--db-user-username=root \
--db-user-password=password \
--cert-hostname="hostname, IP, FQDN"
```

Puede modificar los siguientes atributos:

Atributo	Descripción	Requerido
`--uninstall`	Desinstala el producto.	-
`--keep-database`	La base de datos no se eliminará durante la desinstalación.	-
`--locale`	El identificador de configuración regional (LCID) del servidor instalado (el valor predeterminado es `en_US`). Consulte los idiomas compatibles para ver las opciones disponibles. **i** Si no especifica `--locale`, el ESET PROTECT Server se instalará en inglés. Tras la instalación de ESET PROTECT, puede definir un idioma para cada sesión de ESET PROTECT Web Console. Tenga en cuenta que no todos los elementos de la consola web cambiarán después del cambio de idioma. Algunos de los elementos (paneles predeterminados, políticas, tareas, etc.) se crean durante la instalación de ESET PROTECT y su idioma no puede cambiarse.	Sí
`--skip-license`	La instalación no pedirá al usuario la confirmación del acuerdo de licencia.	-
`--skip-cert`	Omita la generación de certificados (usar con el parámetro `--server-cert-path`).	-
`--license-key`	Clave de licencia de ESET. Puede facilitar la clave de licencia más tarde.	-
`--server-port`	Puerto del servidor de ESET PROTECT (el valor predeterminado es `2222`).	-
`--console-port`	Puerto de consola de ESET PROTECT (el valor predeterminado es `2223`)	-
`--server-root-password`	Contraseña de inicio de sesión en Web Console del usuario "administrador", debe tener 8 caracteres como mínimo.	Sí
`--db-type`	Tipo de base de datos que se utilizará (valores posibles: `"MySQL Server"`, `"MS SQL Server"`). No se admite MS SQL Server en Linux. Sin embargo, puede conectar ESET PROTECT Server en Linux a MS SQL Server en Windows.	-
`--db-driver`	Controlador ODBC utilizado para la conexión a la base de datos especificada en el archivo *odbcinst.ini* (el comando `odbcinst -q -d` ofrece una lista de los controladores disponibles; puede utilizar por ejemplo uno de estos controladores: `--db-driver="MySQL ODBC 8.0 Driver"`, `--db-driver="MySQL ODBC 8.0 Unicode Driver"` o `--db-driver="MySQL ODBC 8.0.17"`).	Sí
`--db-hostname`	Nombre del ordenador o dirección IP del servidor de base de datos. No se admiten instancias de base de datos con nombre.	Sí

Atributo	Descripción	Requerido
`--db-port`	Puerto del servidor de base de datos (el valor predeterminado es `3306`).	Sí
`--db-name`	Nombre de la base de datos de ESET PROTECT Server (el valor predeterminado es `era_db`).	-
`--db-admin-username`	Nombre de usuario del administrador de la base de datos (lo utiliza la instalación para crear y modificar la base de datos). Puede omitir este parámetro si hay un usuario de base de datos creado anteriormente definido en `--db-user-username` y `--db-user-password`.	Sí
`--db-admin-password`	Contraseña del administrador de la base de datos. Puede omitir este parámetro si hay un usuario de base de datos creado anteriormente definido mediante `--db-user-username` y `--db-user-password`.	Sí
`--db-user-username`	Nombre de usuario del usuario de ESET PROTECT Server (lo utiliza ESET PROTECT Server para conectarse a la base de datos); no debe tener más de 16 caracteres.	Sí
`--db-user-password`	Contraseña del usuario de la base de datos de ESET PROTECT Server.	Sí
`--cert-hostname`	Contiene todos los posibles nombres o direcciones IP del ordenador de ESET PROTECT Server. El valor debe coincidir con el nombre de servidor especificado en el certificado de agente que intenta conectarse con el servidor.	Sí
`--server-cert-path`	Ruta al certificado de igual del servidor (utilice esta opción si también ha especificado `--skip-cert`)	-
`--server-cert-password`	Contraseña del certificado de igual del servidor	-
`--agent-cert-password`	Contraseña del certificado de igual del agente	-
`--cert-auth-password`	Contraseña de la autoridad certificadora	-
`--cert-auth-path`	Ruta de acceso del archivo de la autoridad certificadora del servidor	-
`--cert-auth-common-name`	Nombre común de la autoridad certificadora (utilice `""`)	-
`--cert-organizational-unit`	-	-
`--cert-organization`	-	-
`--cert-locality`	-	-
`--cert-state`	-	-
`--cert-country`	-	-
`--cert-validity`	Validez del certificado en días o años (especificar en el argumento `--cert-validity-unit`)	-
`--cert-validity-unit`	Unidad para la validez del certificado, los valores posibles son "Años" o "Días" (el valor predeterminado es `Years`)	-
`--ad-server`	Servidor de Active Directory	-
`--ad-user-name`	Nombre del usuario que tiene derecho a buscar en la red AD	-
`--ad-user-password`	Contraseña de usuario de Active Directory	-
`--ad-cdn-include`	Ruta del árbol de Active Directory para el que se sincronizará; utilice las comillas vacías "" para sincronizar un árbol entero	-
`--enable-imp-program`	Activar el programa para la mejora del producto.	-

Atributo	Descripción	Requerido
`--disable-imp-program`	Desactivar el programa para la mejora del producto.	-

ESET le recomienda eliminar los comandos que contienen datos confidenciales (por ejemplo, una contraseña) del historial de la línea de comandos:
1.Ejecute `history` para ver una lista de todos los comandos del historial.
2.Ejecutar `history -d line_number` (especifique el número de línea del comando). También puede ejecutar `history -c` para eliminar todo el historial de la línea de comandos.

4. La instalación le pregunta si quiere participar en el programa para la mejora del producto. Pulse **Y** si acepta enviar informes de bloqueo y datos de telemetría a ESET o pulse **N** para no enviar ningún dato.

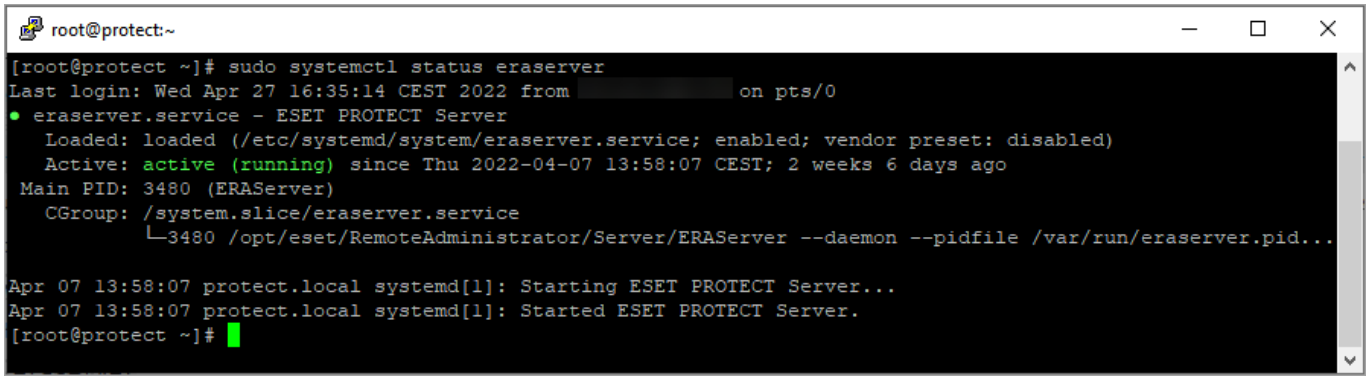
5. ESET PROTECT Server y el servicio `eraserver` se instalarán en la siguiente ubicación:

/opt/eset/RemoteAdministrator/Server

La instalación puede concluir con **SELinux policy... failure**. Puede ignorarlo si no utiliza SELinux.

6. Después de la instalación, compruebe que el servicio ESET PROTECT Server se está ejecutando utilizando el comando que se indica a continuación:

```
sudo systemctl status eraserver
```



Registro del instalador

El registro del instalador puede resultar útil para solucionar problemas y puede encontrarlo en Archivos de registro.

Requisitos previos del servidor - Linux

Para instalar ESET PROTECT Server en Linux, asegúrese de cumplir los siguientes requisitos previos:

- Debe disponer de una licencia válida.
- Debe tener un sistema operativo Linux compatible.
- Los puertos necesarios deben estar abiertos y disponibles; consulte la lista completa de puertos aquí.
- Debe instalarse un servidor de bases de datos y configurarse con una cuenta raíz. No es necesario crear una cuenta de usuario antes de la instalación. El instalador puede crear la cuenta. No se admite MS SQL Server en Linux. Sin embargo, puede conectar ESET PROTECT Server en Linux a MS SQL Server en Windows.

ESET PROTECT Server almacena grandes blobs de datos en la base de datos. Configure MySQL para que acepte paquetes de gran tamaño y ESET PROTECT funcione correctamente.

- **ODBC Driver**: ODBC Driver se utiliza para establecer conexión con el servidor de la base de datos (MySQL).

- Configure el archivo de instalación del servidor como un ejecutable con el comando de terminal:

```
chmod +x server-linux-x86_64.sh
```

- Se recomienda usar la **versión más reciente de OpenSSL 1.1.1**. OpenSSL 3.x no es compatible. La versión mínima compatible de OpenSSL para Linux es openssl-1.0.1e-30. Puede haber más versiones de OpenSSL instaladas en un sistema a la vez. En su sistema debe haber al menos una versión compatible.

    - Use el comando `openssl version` para mostrar la versión predeterminada actual.

    - Puede enumerar todas las versiones de OpenSSL presentes en su sistema. Vea las extensiones de nombre de archivo con el comando `sudo find / -iname *libcrypto.so*`

    - Puede comprobar si su cliente Linux es compatible utilizando el siguiente comando: `openssl s_client -connect google.com:443 -tls1_2`

- **Xvfb**: se requiere para la impresión correcta del informe (Generar informe) en los sistemas de servidor Linux sin una interfaz gráfica.

- **Xauth**: el paquete se instala junto con **xvfb**. Debe instalar **xauth** si no instala **xvfb**.

- **cifs-utils**: se requiere para la correcta implementación del agente en un sistema operativo Windows.

- **Bibliotecas Qt4 WebKit**: se utilizan para la impresión de informes en formato PDF y PS (debe ser la versión 4.8, no la 5). El resto de dependencias Qt4 se instalarán automáticamente. Si el paquete no está disponible en el repositorio del sistema operativo, puede compilarlo usted mismo en el equipo de destino o instalarlo en el repositorio de un tercero (por ejemplo, los repositorios EPEL): Instrucciones para CentOS 7, instrucciones para Ubuntu 20.04.

- **kinit + klist**: Kerberos se utiliza para autenticar un usuario del dominio al iniciar sesión y para la tarea de sincronización de Active Directory. Asegúrese de configurar Kerberos correctamente (*/etc/krb5.conf*). ESET PROTECT 9.1 admite la sincronización con varios dominios.

- **ldapsearch**: se utiliza para la tarea de sincronización de AD y para la autorización.

- **snmptrap**: opcional; se utiliza para enviar capturas de SNMP. SNMP también requiere configuración.

- **Paquete SELinux devel**: se utiliza durante la instalación del producto para crear módulos de política de SELinux. Solo se requiere en sistemas con SELinux activado (CentOS, RHEL). SELinux podría provocar problemas con otras aplicaciones. En el caso de ESET PROTECT Server no es necesario.

- **lshw** - Instale el paquete `lshw` en el equipo cliente/servidor Linux para que ESET Management Agent informe correctamente del inventario de hardware.

En la siguiente tabla se incluyen los comandos de terminal adecuados para cada paquete descrito anteriormente para las diversas distribuciones de Linux (ejecute los comandos como `sudo` o `root`):

Paquete	Distribuciones Debian y Ubuntu	Distribuciones CentOS y Red Hat	Distribución OpenSUSE
Controlador de ODBC	Consulte el capítulo Instalación y configuración de ODBC.		
OpenSSL	`apt-get install openssl`	`yum install openssl -y`	`zypper install openssl`
xvfb	`apt-get install xvfb`	`yum install xorg-x11-server-Xvfb -y`	`zypper install xorg-x11-server-extra`
cifs-utils	`apt-get install cifs-utils`	`yum install cifs-utils`	`zypper install cifs-utils`

Bibliotecas Qt4 WebKit	`apt-get install libqtwebkit4`
	Consulte las instrucciones de Ubuntu 20.04.
		Qt4 WebKit no está en el repositorio CentOS estándar. Instale los siguientes paquetes:
		`yum install -y epel-release`
		`yum install qtwebkit-devel`
		También puede instalar el paquete desde los repositorios Fedora.
			`zypper install libqtwebkit4`

kinit+klist: opcional (necesario para el servicio Active Directory)	`apt-get install krb5-user`	`yum install krb5-workstation`	`zypper install krb5-client`
ldapsearch	`apt-get install ldap-utils libsasl2-modules-gssapi-mit`	`yum install openldap-clients cyrus-sasl-gssapi cyrus-sasl-ldap -y`	`zypper install openldap2-client cyrus-sasl-gssapi cyrus-sasl-ldap-auxprop`
snmptrap	`apt-get install snmp`	`yum install net-snmp-utils net-snmp`	`zypper install net-snmp`
Paquete SELinux devel (opcional; no es necesario para ESET PROTECT Server; SELinux podría provocar problemas con otras aplicaciones).	`apt-get install selinux-policy-dev`	`yum install policycoreutils-devel`	`zypper install selinux-policy-devel`
samba (opcional; solo es necesario para la implementación remota)	`apt-get install samba`	`yum install samba samba-winbind-clients`	`zypper install samba samba-client`
lshw	`apt-get install -y lshw`	`yum install -y lshw`	`zypper install lshw`

Instalación del agente- Linux

Requisitos previos

- Se recomienda usar la **versión más reciente de OpenSSL 1.1.1**. OpenSSL 3.x no es compatible. La versión mínima compatible de OpenSSL para Linux es openssl-1.0.1e-30. Puede haber más versiones de OpenSSL instaladas en un sistema a la vez. En su sistema debe haber al menos una versión compatible.
  - Use el comando `openssl version` para mostrar la versión predeterminada actual.
  - Puede enumerar todas las versiones de OpenSSL presentes en su sistema. Vea las extensiones de nombre de archivo con el comando `sudo find / -iname *libcrypto.so*`
  - Puede comprobar si su cliente Linux es compatible utilizando el siguiente comando: `openssl s_client -connect google.com:443 -tls1_2`
- Instale el paquete `lshw` en el equipo cliente/servidor Linux para que ESET Management Agent informe correctamente del inventario de hardware.

Distribución Linux	Comando de terminal
Debian, Ubuntu	`sudo apt-get install -y lshw`
Red Hat, CentOS, RHEL	`sudo yum install -y lshw`
OpenSUSE	`sudo zypper install lshw`

- Para Linux CentOS, se recomienda instalar el paquete `policycoreutils-devel`. Ejecute el comando para instalar el paquete:

```
yum install policycoreutils-devel
```

- Instalación del agente ayudada por el servidor:
  - El ordenador servidor debe estar accesible desde la red y tener ESET PROTECT Server y ESET PROTECT Web Console instalados.
- Instalación del agente sin conexión:
  - El ordenador servidor debe estar accesible desde la red y tener ESET PROTECT Server instalado.
  - Debe haber presente un certificado para el agente.
  - Debe haber presente un archivo de clave pública de la autoridad certificadora del servidor.

Instalación

Siga los pasos indicados a continuación para instalar el componente ESET Management Agent en Linux con un comando de terminal:

Asegúrese de cumplir todos los requisitos previos de la instalación indicados anteriormente.

1. Descargue el script de instalación del agente:

```
wget https://download.eset.com/com/eset/apps/business/era/agent/latest/agent-linux-x86_64.sh
```

2. Haga que el archivo sea ejecutable:

```
chmod +x agent-linux-x86_64.sh
```

3. Ejecute el script de instalación según el ejemplo mostrado a continuación (las líneas nuevas se dividen con "\" para copiar todo el comando en el terminal):

> Para obtener más información, consulte Parámetros a continuación.

Instalación ayudada por el servidor

```
sudo ./agent-linux-x86_64.sh \
--skip-license \
--hostname=10.1.0.1 \
--port=2222 \
--webconsole-user=Administrator \
--webconsole-password=aB45$45c \
--webconsole-port=2223
```

Instalación fuera de línea

```
sudo ./agent-linux-x86_64.sh \
--skip-license \
--cert-path=/home/admin/Desktop/agent.pfx \
--cert-auth-path=/home/admin/Desktop/CA.der \
--cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 \
--port=2222
```

> ESET le recomienda eliminar los comandos que contienen datos confidenciales (por ejemplo, una contraseña) del historial de la línea de comandos:
> 1.Ejecute `history` para ver una lista de todos los comandos del historial.
> 2.Ejecutar `history -d line_number` (especifique el número de línea del comando). También puede ejecutar `history -c` para eliminar todo el historial de la línea de comandos.

4. Cuando se le solicite, pulse **y** para aceptar el certificado. Puede ignorar los posibles errores de SELinux que indique el instalador.

5. Tras la instalación, compruebe que el servicio ESET Management Agent se está ejecutando:

```
sudo systemctl status eraagent
```

6. Configure el servicio **eraagent** para que se inicie al arrancar: `sudo systemctl enable eraagent`

> **Registro del instalador**
> El registro del instalador puede ser útil para la resolución de problemas. Lo encontrará en Archivos de registro.

Parámetros

La conexión a ESET PROTECT Server se resuelve utilizando los parámetros --hostname y --port (el puerto no se utiliza cuando se proporciona un registro SRV). Formatos posibles de conexión.

- **Nombre de host** y **puerto**
- **Dirección IPv4** y **puerto**
- **Dirección IPv6** y **puerto**

- Registro de servicio (registro SRV): para configurar el registro de recurso de DNS en Linux, el ordenador debe estar en un dominio con un servidor DNS en funcionamiento. Consulte Registro de recurso de DNS. El registro SRV debe empezar por el prefijo "_NAME._tcp" donde "NAME" representa la nomenclatura personalizada (por ejemplo, "era").

Atributo	Descripción	Requerido
`--hostname`	Nombre de host o dirección IP del ESET PROTECT Server con el que se debe establecer conexión.	Sí
`--port`	Puerto del servidor de ESET PROTECT (el valor predeterminado es `2222`).	Sí
`--cert-path`	Ruta de acceso local del archivo de certificado del agente (más información sobre el certificado).	Sí (fuera de línea)
`--cert-auth-path`	Ruta de acceso del archivo de la autoridad certificadora del servidor (más información sobre la autoridad).	Sí (fuera de línea)
`--cert-password`	Contraseña del certificado del agente.	Sí (fuera de línea)
`--cert-auth-password`	Contraseña de la autoridad certificadora.	Sí (si se usa)
`--skip-license`	La instalación no pedirá al usuario la confirmación del acuerdo de licencia.	No
`--cert-content`	Contenido con codificación Base64 del certificado de clave pública con codificación PKCS12 más la clave privada utilizada para configurar canales de comunicación segura con el servidor y los agentes. Utilice una de las dos opciones, `--cert-path` o `--cert-content`.	No
`--cert-auth-content`	Contenido con codificación Base64 del certificado de clave privada de la autoridad certificadora con codificación DER utilizado para verificar los iguales remotos (proxy o servidor). Utilice una de las dos opciones, `--cert-auth-path` o `--cert-auth-content`.	No
`--webconsole-hostname`	Nombre de host o dirección IP que Web Console emplea para conectarse al servidor (si se deja en blanco, el instalador copiará el valor del campo "nombre de host").	No
`--webconsole-port`	Puerto que usa Web Console para conectarse al servidor (el valor predeterminado es `2223`).	No

Atributo	Descripción	Requerido
`--webconsole-user`	Nombre de usuario que usa Web Console para conectarse al servidor (el valor predeterminado es `Administrator`). No puede utilizar un usuario con autenticación de doble factor en instalaciones ayudadas por el servidor.	No
`--webconsole-password`	Contraseña que Web Console emplea para conectarse al servidor.	Sí (ayudada por el servidor)
`--proxy-hostname`	Nombre de host del proxy HTTP. Use este parámetro para permitir el uso del proxy HTTP (que ya está instalado en su red) en la replicación entre ESET Management Agent y ESET PROTECT Server (no para el almacenamiento en caché de actualizaciones).	Si se usa proxy
`--proxy-port`	Puerto del proxy HTTP para conectar al servidor.	Si se usa proxy
`--enable-imp-program`	Activar el programa para la mejora del producto.	No
`--disable-imp-program`	Desactivar el programa para la mejora del producto.	No

Conexión a certificados

- **Conexión a ESET PROTECT Server** debe facilitarse: `--hostname`, `--port` (el puerto no es necesario si se proporciona el registro del servicio, el valor de puerto predeterminado es `2222`)
- Facilite esta información de conexión para la **Instalación ayudada por el servidor**: `--webconsole-port, --webconsole-user, --webconsole-password`
- Facilite la información del certificado para **Instalación sin conexión**: `--cert-path`, `--cert-password`. Los parámetros de instalación `--cert-path` y `--cert-auth-path` requieren archivos de certificación (*.pfx* y *.der*) que pueden exportarse desde la Consola web de ESET PROTECT. (descubra cómo exportar el archivo .pfx y el archivo .der).

Parámetros de tipo de contraseña

Los parámetros de tipo de contraseña pueden proporcionarse como variables de entorno, archivo, leerse de `stdin` o facilitarse como texto sin formato. Es decir:

`--password=env:SECRET_PASSWORD` donde `SECRET_PASSWORD` es una variable de entorno con contraseña

`--password=file:/opt/secret` donde la primera línea del archivo `/opt/secret` regular contiene la contraseña

`--password=stdin` indica al instalador que lea la contraseña de una entrada estándar

`--password="pass:PASSWORD"` es igual a `--password="PASSWORD"` y es obligatorio si la contraseña real es `"stdin"` (entrada estándar) o la cadena comienza por `"env:"`, `"file:"` o `"pass:"`

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

Conexión con proxy HTTP

Si está utilizando el proxy HTTP para la replicación entre ESET Management Agent y ESET PROTECT Server (y no para almacenar en caché las actualizaciones), puede especificar los parámetros de conexión en `--proxy-hostname` y `--proxy-port`.

EJEMPLO: instalación del agente sin conexión con la conexión con proxy HTTP

```
./agent-linux-x86_64.sh \
--skip-license \
--cert-path=/home/admin/Desktop/agent.pfx \
--cert-auth-path=/home/admin/Desktop/CA.der \
--cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 \
--port=2222 \
--proxy-hostname=10.1.180.3 \
--proxy-port=3333 \
```

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

Actualización y reparación de la instalación del agente en Linux

Si ejecuta la instalación del agente manualmente en un sistema en el que el agente ya está instalado, se pueden dar las siguientes circunstancias:

- **Actualizar**: ejecuta una versión posterior del instalador.
  - Instalación ayudada por el servidor: la aplicación se actualiza, pero sigue utilizando los certificados anteriores.
  - Instalación sin conexión: la aplicación se actualiza y se utilizan certificados nuevos.
- **Reparar**: ejecuta la misma versión del instalador. Puede utilizar esta opción para migrar el agente a un ESET PROTECT Server distinto.
  - Instalación ayudada por el servidor: la aplicación se reinstala y obtiene los certificados actuales de ESET PROTECT Server (definidos por el parámetro `hostname`).
  - Instalación sin conexión: la aplicación se reinstala y se utilizan certificados nuevos.

Si está migrando el agente de una versión de Server antigua a un ESET PROTECT Server más moderno manualmente y está utilizando la instalación ayudada por el servidor, ejecute el comando de instalación dos

veces. El primero actualizará el agente y el segundo obtendrá los nuevos certificados para que el agente se pueda conectar al ESET PROTECT Server.

Instalación de Web Console: Linux

Siga estos pasos para instalar ESET PROTECT Web Console:

> Puede seleccionar la instalación de ESET PROTECT Web Console en un ordenador distinto al ordenador donde se ha instalado ESET PROTECT Server. Este procedimiento requiere pasos adicionales.

1. Instale los paquetes Apache Tomcat y Java. Los ejemplos de nombres de paquetes que se indican a continuación pueden ser distintos de los paquetes del repositorio de su distribución Linux.

Distribución Linux	Comandos de terminal
Distribuciones Debian y Ubuntu	`sudo apt-get update` `sudo apt-get install openjdk-17-jdk tomcat9`
Distribuciones CentOS y Red Hat	`yum update` `yum install java-17-openjdk tomcat`
OpenSUSE	`zypper refresh` `sudo zypper install java-17-openjdk tomcat9`

2. Descargue el archivo de Web Console (*era.war*):

```
wget https://download.eset.com/com/eset/apps/business/era/webconsole/latest/era.war
```

3. Copie el archivo *era.war* en la carpeta Tomcat:

Debian, Ubuntu	`sudo cp era.war /var/lib/tomcat9/webapps/`
CentOS, Red Hat	`sudo cp era.war /var/lib/tomcat/webapps/`
OpenSUSE	`sudo cp era.war /usr/share/tomcat/webapps/`

4. Reinicie el servicio Tomcat para implementar el archivo *era.war*:

Debian, Ubuntu	`sudo systemctl restart tomcat9`
CentOS, Red Hat	`sudo systemctl restart tomcat`
OpenSUSE	`sudo systemctl restart tomcat`

5. Compruebe que la carpeta Tomcat contiene la carpeta *era*:

Debian, Ubuntu	`ls /var/lib/tomcat9/webapps`
CentOS, Red Hat	`ls /var/lib/tomcat/webapps`
OpenSUSE	`ls /usr/share/tomcat/webapps`

La salida debe tener el siguiente formato: `era era.war`

6. Configure el servicio Tomcat para que se inicie al arrancar: `sudo systemctl enable tomcat` (o `tomcat9` según el nombre del servicio)

7. Si ha instalado ESET PROTECT Web Console en un ordenador diferente de ESET PROTECT Server, realice estos pasos adicionales para permitir la comunicación entre ESET PROTECT Web Console y ESET PROTECT Server:

a)Detenga el servicio Tomcat: `sudo systemctl stop tomcat`

b)Modifique el archivo *EraWebServerConfig.properties*:

```
sudo nano /var/lib/tomcat/webapps/era/WEB-
INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.prop
erties
```

Si el archivo *EraWebServerConfig.properties* no está ubicado en la ruta anterior, puede utilizar el siguiente comando para encontrar el archivo en el sistema:

```
find / -iname "EraWebServerConfig.properties"
```

c)Encuentre el `server_address=localhost`

d)Reemplace `localhost` por la dirección IP del ESET PROTECT Server y guarde el archivo.

e)Reinicie el servicio Tomcat: `sudo systemctl restart tomcat` (o `tomcat9` según el nombre del servicio)

f)Configure el servicio Tomcat para que se inicie al arrancar: `sudo systemctl enable tomcat` (o `tomcat9` según el nombre del servicio)

8. Abra ESET PROTECT Web Console en un navegador web compatible para ver una pantalla de inicio de sesión:

• Desde el ordenador en el que está alojado ESET PROTECT Web Console: *http://localhost:8080/era*

• Desde cualquier ordenador con acceso a Internet a ESET PROTECT Web Console (sustituya *IP_ADDRESS_OR_HOSTNAME* por la dirección IP o el nombre de host de su ESET PROTECT Web Console): *http://IP_ADDRESS_OR_HOSTNAME:8080/era*

9. Configure Web Console después de la instalación:

• El puerto HTTP predeterminado se establece en 8080 durante la instalación manual de Apache Tomcat. Le recomendamos que configure una conexión HTTPS para Apache Tomcat.

• Consulte también la configuración de Web Console adicional para soluciones empresariales o sistemas de bajo rendimiento.

Instalación de rogue detection sensor – Linux

Si hay varios segmentos de red, Rogue Detection Sensor debe instalarse por separado en cada segmento de red para generar una lista completa de todos los dispositivos de toda la red.

Requisitos previos

- Se puede buscar en la red (los puertos están abiertos, el cortafuegos no está bloqueando la comunicación entrante, etc.).
- El ordenador servidor es accesible.
- ESET Management Agent debe estar instalado en el ordenador local para admitir todas las funciones del programa.
- El terminal está abierto.
- Configure el archivo de instalación de RD Sensor como un ejecutable:

```
chmod +x rdsensor-linux-x86_64.sh
```

Instalación

Siga los pasos indicados a continuación para instalar el componente RD Sensor en Linux con un comando de terminal:

Asegúrese de cumplir todos los requisitos previos de la instalación indicados anteriormente.

1. Utilice el siguiente comando para ejecutar el archivo de instalación como sudo:

```
sudo ./rdsensor-linux-x86_64.sh
```

2. Lea el Acuerdo de licencia para el usuario final. Use la **barra espaciadora** para ir a la siguiente página del Acuerdo de licencia para el usuario final.
El instalador le preguntará si acepta el acuerdo. Pulse **Y** en el teclado si la acepta. De lo contrario, pulse **N**.

3. Pulse **Y** si desea participar en el programa de mejora del producto. De lo contrario, pulse **N**.

4. ESET Rogue Detection Sensor se iniciará una vez finalizado el proceso de instalación.

5. Para ver si la instalación se ha realizado correctamente, compruebe que el servicio está en funcionamiento ejecutando el siguiente comando:

```
sudo systemctl status rdsensor
```

6. Encontrará el archivo de registro de Rogue Detection Sensor en los archivos de registro:

/var/log/eset/RogueDetectionSensor/trace.log

Instalación del Conector de dispositivo móvil: Linux

Puede instalar el Conector de dispositivo móvil en un servidor distinto al servidor en el que ESET PROTECT Server está en ejecución. Por ejemplo, puede utilizar esta situación de instalación para que pueda accederse al Mobile Device Connector desde Internet para administrar los dispositivos móviles de los usuarios en todo momento.

Siga los pasos indicados a continuación para instalar el componente Mobile Device Connector en Linux con un

comando de terminal:

Asegúrese de cumplir todos los requisitos previos de la instalación.

1. Descargue el script de instalación de Mobile Device Connector:

```
wget https://download.eset.com/com/eset/apps/business/era/mdm/latest/mdmcore-linux-x86_64.sh
```

2. Ejecute el script de instalación según el ejemplo mostrado a continuación (las líneas nuevas se dividen con "\" para copiar todo el comando en el terminal):

```
sudo ./mdmcore-linux-x86_64.sh \
--https-cert-path="full_path/proxycert.pfx" \
--https-cert-password="123456789" \
--port=2222 \
--db-type="MySQL Server" \
--db-driver="MySQL ODBC 8.0 Driver" \
--db-admin-username="root" \
--db-admin-password=123456789 \
--db-user-password=123456789 \
--db-hostname="127.0.0.1" \
--webconsole-password=123456789 \
--hostname=username.LOCAL \
--mdm-hostname=username.LOCAL
```

Si desea consultar una lista completa de los parámetros disponibles (imprimir mensaje de ayuda), utilice:

```
--help
```

ESET le recomienda eliminar los comandos que contienen datos confidenciales (por ejemplo, una contraseña) del historial de la línea de comandos:
1.Ejecute `history` para ver una lista de todos los comandos del historial.
2.Ejecutar `history -d line_number` (especifique el número de línea del comando). También puede ejecutar `history -c` para eliminar todo el historial de la línea de comandos.

Parámetros necesarios del comando de instalación

Existen numerosos parámetros de instalación opcionales, pero algunos de ellos son obligatorios:

- Certificado de igual: el certificado de igual de ESET PROTECT se puede obtener de dos formas:

  • **Instalación ayudada por el servidor**: tendrá que facilitar las credenciales de administrador de ESET PROTECT Web Console (el programa de instalación descargará los certificados necesarios automáticamente).

  • **Instalación sin conexión**: necesitará proporcionar un certificado de igual (el certificado del proxy exportado desde ESET PROTECT). También puede usar su certificado personalizado.

  oEn el caso de una **Instalación ayudada por el servidor** se debe incluir como mínimo:

```
--webconsole-password=
```

- En el caso de una **Instalación sin conexión** se debe incluir:

```
--cert-path=
--cert-password=
```

(El certificado de agente predeterminado creado durante la instalación de ESET PROTECT Server no necesita contraseña).

- Certificado HTTPS (proxy):

  - Si ya tiene un certificado HTTPS:

```
--https-cert-path=
--https-cert-password=
```

  - Para generar un nuevo certificado HTTPS:

```
--https-cert-generate
--mdm-hostname=
```

- Conexión con ESET PROTECT Server (nombre o dirección IP):

```
--hostname=
```

- Conexión con la base de datos:

  - Para una base de datos MySQL, incluya:

```
--db-type="MySQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

  - Para una base de datos de MS SQL, incluya:

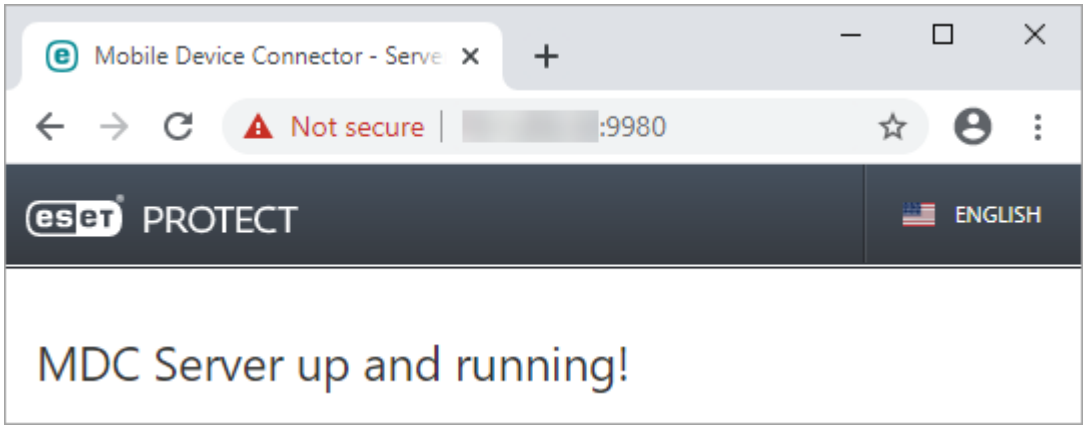
```
--db-type="Microsoft SQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
```

```
--db-user-password=
```

Registro del instalador

El registro del instalador puede resultar útil para solucionar problemas y puede encontrarlo en Archivos de registro.

Una vez completada la instalación, compruebe si el Conector del dispositivo móvil funciona correctamente; para ello abra *https://su-nombre de host-mdm:puerto-inscripción* (por ejemplo, *https://eramdm:9980*) en el navegador web. Si la instalación se completó correctamente, se mostrará el siguiente mensaje:



También puede usar esta URL para comprobar la disponibilidad del servidor del Conector de dispositivo móvil desde Internet (en caso de estar configurado para ello) visitándola desde un dispositivo móvil. Si no puede conectar con la página, revise la configuración del cortafuegos y de la infraestructura de red.

Requisitos del Conector de dispositivo móvil: Linux

Se deben cumplir los siguientes requisitos para poder instalar el Conector de dispositivo móvil en Linux:

- Un servidor de base de datos ya instalado y configurado, con una cuenta raíz (no es necesario crear una cuenta de usuario antes de la instalación, el instalador puede crearla).
- Un controlador ODBC para la conexión con el servidor de base de datos (MySQL/MS SQL) instalado en el ordenador. Consulte el capítulo Instalación y configuración de ODBC.

> Debe usar el paquete `unixODBC_23` (no el `unixODBC` predeterminado) para que MDC se conecte a la base de datos MySQL sin problemas. Esta instrucción adquiere especial relevancia en SUSE Linux.

> Le recomendamos que implemente el componente de MDM en un dispositivo host distinto al que se aloja ESET PROTECT Server.

- Archivo de instalación de MDMCore configurado como un ejecutable.

```
chmod +x mdmcore-linux-x86_64.sh
```

- Tras la instalación, asegúrese de que el servicio MDMCore se esté ejecutando.

```
sudo systemctl status eramdmcore
```

- Se recomienda usar la **versión más reciente de OpenSSL 1.1.1**. OpenSSL 3.x no es compatible. La versión

mínima compatible de OpenSSL para Linux es openssl-1.0.1e-30. Puede haber más versiones de OpenSSL instaladas en un sistema a la vez. En su sistema debe haber al menos una versión compatible.

- Use el comando `openssl version` para mostrar la versión predeterminada actual.
- Puede enumerar todas las versiones de OpenSSL presentes en su sistema. Vea las extensiones de nombre de archivo con el comando `sudo find / -iname *libcrypto.so*`
- Puede comprobar si su cliente Linux es compatible utilizando el siguiente comando: `openssl s_client -connect google.com:443 -tls1_2`

> Si la base de datos de MDM de MySQL es demasiado grande (miles de dispositivos), el valor `innodb_buffer_pool_size` predeterminado será demasiado pequeño. Para obtener más información sobre la optimización de la base de datos, consulte: https://dev.mysql.com/doc/refman/5.6/en/optimizing-innodb-diskio.html

Requisitos del certificado

- Necesitará un **certificado SSL** en formato *.pfx*para establecer una comunicación segura a través de HTTPS. Se recomienda utilizar el certificado proporcionado por una autoridad certificadora externa. No se recomienda el uso de certificados autofirmados (incluidos los certificados firmados por la autoridad certificadora de ESET PROTECT), ya que no todos los dispositivos móviles permiten a los usuarios aceptar certificados autofirmados.

- Debe tener un certificado firmado por una autoridad certificadora y la clave privada correspondiente, y utilizar procedimientos estándar, para fusionarlos (tradicionalmente con OpenSSL) para combinarlos en un archivo *.pfx*:
```
openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out httpsCredentials.pfx
```
Se trata de un procedimiento estándar para la mayoría de los servidores que utilizan certificados SSL.

- Para la instalación sin conexión, también necesitará un certificado de igual (el **certificado del agente** exportado desde ESET PROTECT). También puede usar su certificado personalizado con ESET PROTECT.

Instalación del proxy HTTP Apache - Linux

Los agentes de ESET Management pueden conectarse a ESET PROTECT Server a través del Apache HTTP Proxy. Obtenga más información sobre cómo funciona el proxy con las instancias de ESET Management Agent.

Apache HTTP Proxy se suele distribuir como un paquete `apache2` o `httpd`.

Seleccione los pasos de instalación del proxy HTTP Apache según la distribución Linux que utilice en el servidor: Si quiere usar el Apache para almacenar en caché también los resultados de ESET LiveGuard Advanced, consulte también la documentación relacionada.

Instalación en Linux (genérica para todas las distribuciones) del proxy HTTP Apache

1. Instale el servidor HTTP Apache (como mínimo la versión 2.4.10).

2. Asegúrese de que están cargados los siguientes módulos:

```
access_compat, auth_basic, authn_core, authn_file, authz_core, authz_groupfile,
authz_host, proxy, proxy_http, proxy_connect, cache, cache_disk
```

3. Agregue la configuración de almacenamiento en caché:

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 500000000
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. Si el directorio */var/cache/apache2/mod_cache_disk* no existe, créelo y asigne privilegios a Apache (r,w,x).

5. Agregue la configuración del proxy:

```
AllowCONNECT 443 563 2222 8883 53535


ProxyRequests On
ProxyVia On


CacheLock on

CacheLockMaxAge 10

ProxyTimeOut 900


SetEnv proxy-initial-not-pooled 1


<VirtualHost *:3128>

ProxyRequests On

</VirtualHost>


<VirtualHost *:3128>

ServerName r.edtd.eset.com


<If "%{REQUEST_METHOD} == 'CONNECT'">

Require all denied

</If>


ProxyRequests Off
```

```
CacheEnable disk /

SSLProxyEngine On


RequestHeader set Front-End-Https "On"

ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=On ttl=100 max=100 smax=1
0

ProxyPassReverse / http://r.edtd.eset.com/ keepalive=On

</VirtualHost>


<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

6. De forma predeterminada, se utiliza el puerto 2222 para la comunicación con ESET Management Agent. Si ha cambiado el puerto durante la instalación, utilice el número de puerto modificado. Cambie 2222 en la línea `AllowCONNECT 443 563 2222 8883 53535` por su número de puerto.

7. Active el proxy y la configuración de almacenamiento en caché agregada (si el archivo de configuración principal de Apache contiene la configuración, este paso puede omitirse).

8. En caso de ser necesario, cambie el puerto de escucha al puerto que desee (está configurado el puerto 3128 de forma predeterminada).

9. Autenticación básica opcional:

- Agregue la configuración de autenticación a la directiva del proxy:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile /etc/apache2/password.file
AuthGroupFile /etc/apache2/group.file
Require group usergroup
```

- Cree un archivo de contraseña con `/etc/httpd/.htpasswd -c`
- Cree manualmente un archivo denominado group.file con `usergroup:username`

10. Reinicie el servidor HTTP Apache.

Instalación del proxy HTTP Apache en Ubuntu Server y en otras distribuciones Linux basadas en Debian

1. Instale la versión más reciente del servidor HTTP Apache desde el repositorio apt:

```
sudo apt-get install apache2
```

2. Ejecute el siguiente comando para cargar los módulos de Apache necesarios:

```
sudo a2enmod access_compat auth_basic authn_core authn_file authz_core\

authz_groupfile authz_host proxy proxy_http proxy_connect cache cache_disk
```

3. Edite el archivo de configuración del almacenamiento en caché de Apache:

```
sudo vim /etc/apache2/conf-available/cache_disk.conf
```

y copie y pegue la siguiente configuración:

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 500000000
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. Este paso no debería ser necesario, pero si falta el directorio de almacenamiento en caché, ejecute los siguientes comandos:

```
sudo mkdir /var/cache/apache2/mod_cache_disk
sudo chown www-data /var/cache/apache2/mod_cache_disk
sudo chgrp www-data /var/cache/apache2/mod_cache_disk
```

5. Edite el archivo de configuración del proxy de Apache:

```
sudo vim /etc/apache2/conf-available/proxy.conf
```

y copie y pegue la siguiente configuración:

```
AllowCONNECT 443 563 2222 8883 53535


ProxyRequests On
ProxyVia On


CacheLock on

CacheLockMaxAge 10

ProxyTimeOut 900


SetEnv proxy-initial-not-pooled 1


<VirtualHost *:3128>

ProxyRequests On

</VirtualHost>


<VirtualHost *:3128>
```

```
        ServerName r.edtd.eset.com


<If "%{REQUEST_METHOD} == 'CONNECT'">

Require all denied

</If>


ProxyRequests Off

CacheEnable disk /

SSLProxyEngine On


RequestHeader set Front-End-Https "On"

ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=On ttl=100 max=100 smax=1
0

ProxyPassReverse / http://r.edtd.eset.com/ keepalive=On

</VirtualHost>


<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

6. De forma predeterminada, se utiliza el puerto 2222 para la comunicación con ESET Management Agent. Si ha cambiado el puerto durante la instalación, utilice el número de puerto modificado. Cambie 2222 en la línea `AllowCONNECT 443 563 2222 8883 53535` por su número de puerto.

7. Active los archivos de configuración que modificó en los pasos anteriores:

```
sudo a2enconf cache_disk.conf proxy.conf
```

8. Cambie el puerto de recepción de conexiones del servidor HTTP Apache a 3128. Modifique el archivo */etc/apache2/ports.conf* y sustituya `Listen 80` por `Listen 3128`.

9. Autenticación básica opcional:

```
sudo vim /etc/apache2/mods-enabled/proxy.conf
```

- Copie y pegue la configuración de autenticación antes de `</Proxy>`:

```
  AuthType Basic
  AuthName "Password Required"
  AuthUserFile /etc/apache2/password.file
  AuthGroupFile /etc/apache2/group.file
  Require group usergroup
```

- Instale apache2-utils y cree un archivo de contraseña nuevo (por ejemplo, con el nombre de usuario u

```
ser y el grupo usergroup):

sudo apt-get install apache2-utils
sudo htpasswd -c /etc/apache2/password.file user

oCree un archivo llamado group:

sudo vim /etc/apache2/group.file

y copie y pegue la siguiente línea:

usergroup:user
```

10. Reinicie el servidor HTTP Apache con el siguiente comando:

```
sudo systemctl restart apache2
```

Reenvío solo para la comunicación de ESETPara permitir el reenvío de la comunicación de ESET únicamente, quite lo siguiente:

```
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

Y añada también lo siguiente:

```
<Proxy *>

Deny from all

</Proxy>


#*.eset.com:

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[c,C][o,O][m,M](:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>


#*.eset.eu:

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[e,E][u,U](:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>


#*.eset.systems:
```

```
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-
]{0,63}\.[e,E][s,S][e,E][t,T]\.[s,S][y,Y][s,S][t,T][e,E][m,M][s,S](:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>



#Antispam module (ESET Mail Security only):

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(ds1-uk-rules-1.mailshell.net|ds1-uk-rules-2.mailshell.net|ds1-uk-rules-3.mailshell.net|fh-uk11.mailshell.net)(:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>



#Services (activation)

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(edf-pcs.cloudapp.net|edf-pcs2.cloudapp.net|edfpcs.trafficmanager.net)(:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>



#ESET servers accessed directly via IP address:

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(91.228.165.|91.228.166.|91.228.167.|38.90.226.)([0-9]+)(:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>



#AV Cloud over port 53535

<ProxyMatch ^.*e5.sk.*$>

Allow from all

</ProxyMatch>
```

Reenvío para toda la comunicación

Para permitir el reenvío de todas las comunicaciones, añada lo siguiente:

```
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

y quite también lo siguiente:

```
<Proxy *>

Deny from all

</Proxy>


#*.eset.com:

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-
Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[c,C][o,O][m,M](:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>


#*.eset.eu:

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-
Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[e,E][u,U](:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>


#*.eset.systems:

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-
Z0-9-
]{0,63}\.[e,E][s,S][e,E][t,T]\.[s,S][y,Y][s,S][t,T][e,E][m,M][s,S](:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>


#Antispam module (ESET Mail Security only):

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(ds1-uk-
rules-1.mailshell.net|ds1-uk-rules-2.mailshell.net|ds1-uk-rules-3.mailshell.net|fh-
uk11.mailshell.net)(:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>


#Services (activation)

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(edf-pcs.cloudapp.net|edf-
pcs2.cloudapp.net|edfpcs.trafficmanager.net)(:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>


#ESET servers accessed directly via IP address:

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(91.228.165.|91.228.166.|91.2
28.167.|38.90.226.)([0-9]+)(:[0-9]+)?(/.*)?$>

Allow from all
```

```
</ProxyMatch>

#AV Cloud over port 53535
<ProxyMatch ^.*e5.sk.*$>
Allow from all
</ProxyMatch>
```

Encadenado de proxy (todo el tráfico)

ESET PROTECT no admite el encadenado de proxy cuando estos requieren autenticación. Puede utilizar su propia solución de proxy web transparente, pero podría ser necesario configurar otros elementos además de los mencionados en el presente documento. Añada lo siguiente a la configuración del proxy (la contraseña solo funciona en el proxy secundario):

```
<VirtualHost *:3128>
ProxyRequests On
ProxyRemote * http://IP_ADDRESS:3128
</VirtualHost>
```

Al usar el encadenado de proxy en el dispositivo virtual de ESET PROTECT se debe modificar la política SELinux. Abra el terminal en el dispositivo virtual de ESET PROTECT y ejecute el siguiente comando:

```
/usr/sbin/setsebool -P httpd_can_network_connect 1
```

Configurar el proxy HTTP para un número elevado de clientes

Si utiliza el proxy HTTP Apache de 64 bits, puede aumentar el límite de subprocesos para su Apache HTTP Proxy. Edite el archivo de configuración *httpd.conf*, incluido en su carpeta Apache HTTP Proxy. Busque los siguientes ajustes en el archivo y actualice los valores para que coincidan con el número de clientes.

Sustituya el valor de ejemplo de `5000` con su número. El valor máximo es `32000`.

```
ThreadLimit 5000
ThreadsPerChild 5000
```

No cambie el resto del archivo.

Configure el proxy HTTP Apache para que reenvíe las conexiones entre agente y servidor

1. En el equipo proxy, abra el archivo

    i. Distribuciones Debian
    `/etc/apache2/mods-available/proxy.conf`

    ii. Distribuciones Red Hat

```
/etc/httpd/conf/httpd.conf
```

2.Agregue las siguientes líneas al final del archivo:
```
AllowCONNECT 443 563 2222 8883 53535
```

3.En el equipo proxy, abra el archivo

i.Distribuciones Debian
```
/etc/apache2/apache2.conf
```

ii.Distribuciones Red Hat
```
/etc/httpd/conf/httpd.conf
```

4.Busque la línea:
```
Listen 80
```
y cámbiela a
```
Listen 3128
```

5.Si ha agregado restricciones para direcciones IP en la configuración de su proxy (paso 1), deberá permitir el acceso a ESET PROTECT Server:

Añadir otro segmento `ProxyMatch`:

I.La dirección que sus agentes utilizan para conectarse a ESET PROTECT Server.

II.El resto de direcciones posibles de su ESET PROTECT Server (IP, FQDN)
(agregue todo el código que aparece a continuación; la dirección IP 10.1.1.10 y el nombre de host `hostname.example` son simplemente ejemplos que debe sustituir con sus direcciones. También puede generar la expresión `ProxyMatch` como se explica en este artículo de la Base de conocimiento.)

```
<ProxyMatch ^(hostname\.example(:[0-9]+)?(\/.*)?|10\.1\.1\.10(:[0-9]+)?(\/.*)?)$>

Allow from all

</ProxyMatch>
```

6.Reinicie el servicio *Apache HTTP Proxy*.

Configurar almacenamiento en caché

Puede utilizar htcachceclean para configurar el tamaño y la desinfección de la caché de Apache HTTP Proxy. Consulte las instrucciones de configuración de la caché para el dispositivo virtual ESET PROTECT.

Configuración de SELinux

Al usar proxy en el dispositivo virtual de ESET PROTECT, se debe modificar la política SELinux (otras distribuciones de Linux podrían tener el mismo requisito). Abra el terminal en el dispositivo virtual de ESET PROTECT y ejecute el siguiente comando:

```
/usr/sbin/setsebool -P httpd_can_network_connect 1

sudo semanage port -a -t http_port_t -p tcp 2222
```

Instalación del proxy HTTP Squid en Ubuntu Server

En Ubuntu Server puede utilizar el proxy Squid en lugar de Apache. Siga los pasos indicados a continuación para instalar y configurar Squid en Ubuntu Server (y en distribuciones Linux similares basadas en Debian):

1. Instale el paquete Squid3:

```
sudo apt-get install squid3
```

2. Edite el archivo de configuración de Squid */etc/squid3/squid.conf* y reemplace:

```
#cache_dir ufs /var/spool/squid3 100 16 256
```

por:

```
cache_dir ufs /var/spool/squid3 3000 16 256 max-size=200000000
```

> • También puede cambiar el tamaño total de la caché (3000 MB en el ejemplo) y el número de subdirectorios de primer nivel (16 en el ejemplo) y de subdirectorios de segundo nivel (256 en el ejemplo) en el directorio de la caché.
> • El parámetro `max-size` define el tamaño de archivo almacenado en caché máximo, en bytes.

3. Detenga el servicio squid3.

```
sudo systemctl stop squid3
sudo squid3 –z
```

4. Edite de nuevo el archivo de configuración de Squid y agregue `http_access allow all` antes de `http_access deny all` para permitir que todos los clientes accedan al proxy.

5. Reinicie el servicio squid3:

```
sudo systemctl restart squid3
```

Herramienta Mirror: Linux

¿Es usuario de Windows?

Para las actualizaciones del motor de detección se necesita la herramienta Mirror. Si sus ordenadores cliente no tienen una conexión a Internet y necesitan actualizaciones del motor de detección, puede utilizar la herramienta Mirror para descargar archivos de actualización de servidores de actualización de ESET y almacenarlos de forma local.

> La herramienta Mirror descarga únicamente actualizaciones del motor de detección y otros módulos del programa, no descarga PCU (actualizaciones de componentes del programa) ni datos de ESET LiveGrid®. También puede crear un repositorio sin conexión completo. Alternativamente, puede actualizar productos individualmente.

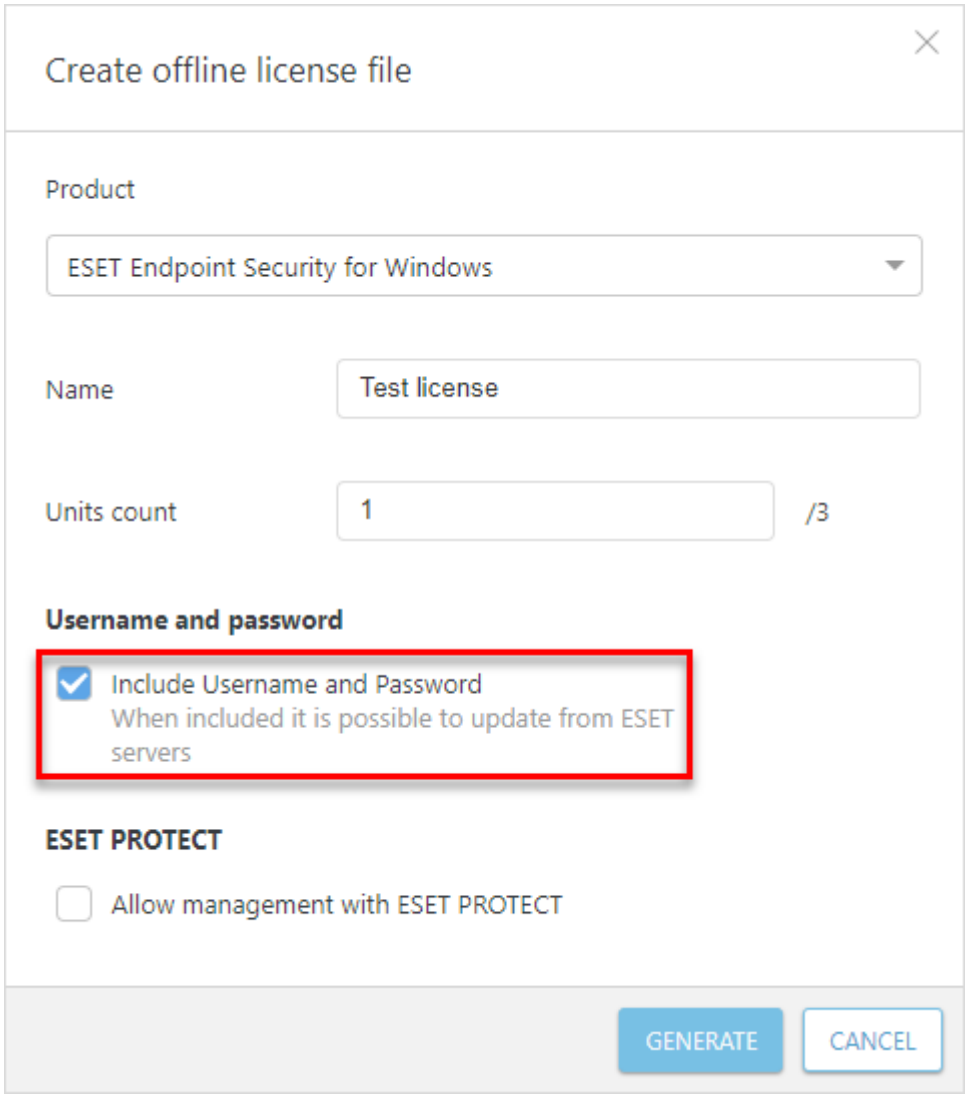
Requisitos previos

• La carpeta de destino debe estar disponible para compartir, servicio Samba/Windows o HTTP/FTP, según cómo desea que las actualizaciones estén accesibles.

oProductos de seguridad de ESET para Windows: puede actualizarlos de forma remota mediante HTTP o una carpeta compartida.

oProductos de seguridad de ESET para Linux/macOS: solo puede actualizarlos de forma remota con HTTP. Si utiliza una carpeta compartida, debe estar en el mismo ordenador que el producto de seguridad de ESET.

• Debe tener un archivo de Licencia sin conexión válido que incluya el nombre de usuario y contraseña. Cuando genere un archivo de licencia, asegúrese de marcar la casilla de verificación situada junto a **Incluir nombre de usuario y contraseña**. Además, debe introducir un **nombre** de licencia. Se necesita un archivo de licencia sin conexión para activar la herramienta Mirror y generar el mirror de actualización.



Uso de la herramienta Mirror

1.Descargue la herramienta Mirror de la página de descargas de ESET (sección **Instaladores independientes**).

2.Descomprima el archivo comprimido descargado.

3.Abra el terminal en la carpeta con el archivo *MirrorTool* y haga el archivo ejecutable:

```
chmod +x MirrorTool
```

4.Ejecute el comando que aparece a continuación para ver todos los parámetros disponibles de la herramienta Mirror y su versión:

```
./MirrorTool --help
```

```
root@ubuntu:/home/user/Desktop/x86_64/x86_64# ./MirrorTool --help
Mirror Tool v1.0.2226.0, Copyright (c) ESET, spol. s r.o. 1992-2021. All rights reserved.
Allowed options:
  --mirrorType arg                      [required for module update]
                                        Type of mirror. Possible values (case
                                        insensitive): regular, pre-release,
                                        delayed.
  --intermediateUpdateDirectory arg     [required for module update]
                                        Files will be downloaded to this
                                        directory to create mirror in output
                                        directory.
  --offlineLicenseFilename arg          [required for module update]
                                        Offline license file.
  --updateServer arg                    [optional]
                                        Update server. (e.g.:
                                        http://update.eset.com/eset_upd/ep6/)
                                        Mirror will be created in output
                                        directory, only specified path in
                                        server will be mirrored.
  --outputDirectory arg                 [required for module update]
                                        Directory where mirror will be created.
  --proxyHost arg                       [optional]
                                        Http proxy address (fqdn or IP).
  --proxyPort arg                       [optional]
                                        Http proxy port.
  --proxyUsername arg                   [optional]
                                        Http proxy username.
  --proxyPassword arg                   [optional]
                                        Http proxy password.
  --networkDriveUsername arg            [optional]
                                        Username used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --networkDrivePassword arg            [optional]
                                        Password used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --excludedProducts arg                [optional]
                                        Disable creating mirror for specified
                                        products. Use --listUpdatableProducts
                                        to see possible values.
  --listUpdatableProducts               Show list of all products which modules
                                        are downloaded by default.
  --repositoryServer arg                [required for repository update]
                                        Repository server for repository
                                        creation.
  --intermediateRepositoryDirectory arg [required for repository update]
                                        Files will be downloaded to this
                                        directory to create offline mirror in
                                        output directory.
  --outputRepositoryDirectory arg       [required for repository update]
                                        Directory where offline repository will
                                        be created.
  --trustDownloadedFilesInRepositoryTemp
                                        [optional]
                                        If set, hashes on already downloaded
                                        files are not checked.
  --mirrorOnlyLevelUpdates              [optional]
                                        If set, only level upgrades will be
                                        downloaded (nano/continuous updates
                                        will not be downloaded)
  --mirrorFileFormat arg                [optional]
                                        Specifies which type of update files
                                        will be downloaded. Possible values
                                        (case insensitive): dll, dat.
  --compatibilityVersion arg            [optional]
                                        Version of compatible products.
  --filterFilePath arg                  [optional]
                                        Path to filter file in json format.
                                        Parameter compatibilityVersion has to
                                        be higher than 7.1.0.0 to run program.
  --dryRun arg                          [optional]
                                        Specifies dry run of program with path
                                        to csv file where will be saved list of
                                        products to be downloaded with current
                                        filter configuration.
  --help                                [optional]
                                        Display this help and exit
```

Todos los filtros distinguen entre mayúsculas y minúsculas.

Parámetro	Descripción
`--updateServer`	Cuando lo utilice, debe especificar la URL completa del servidor de actualización.
`--offlineLicenseFilename`	Debe especificar una ruta de su archivo de licencia sin conexión (como se mencionó anteriormente).
`--mirrorOnlyLevelUpdates`	No se necesita argumento. Si se selecciona esta opción, solo se descargarán las actualizaciones de nivel (las actualizaciones nano no se descargarán). Obtenga más información sobre los tipos de actualización en el artículo de la base de conocimiento.
`--mirrorFileFormat`	⚠ Antes de utilizar el parámetro `--mirrorFileFormat`, asegúrese de que el entorno no contenga versiones de los productos de seguridad de ESET más antiguas (6.5 y anteriores) y más recientes (6.6 y posteriores). El uso incorrecto de este parámetro puede actualizar de forma incorrecta los productos de seguridad de ESET. Puede especificar qué tipo de archivos de actualización se descargarán. Valores posibles (se distingue entre mayúsculas y minúsculas): • `dat`: utilice este valor si el entorno solo tiene versiones del producto de seguridad de ESET 6.5 y anteriores. • `dll`: utilice este valor si el entorno solo tiene versiones del producto de seguridad de ESET 6.6 y posteriores. El parámetro se ignora al crear un Mirror para productos heredados (`ep4`, `ep5`).
`--compatibilityVersion`	Este parámetro opcional se aplica a la herramienta Mirror distribuida con ESET PROTECT 8.1 y versiones posteriores. La herramienta Mirror descargará los archivos de actualización compatibles con la versión del repositorio de ESET PROTECT que haya especificado en el argumento del parámetro en formato `x.x` o `x.x.x.x`, por ejemplo: `--compatibilityVersion 9.1` o `--compatibilityVersion 8.1.13.0`.

ℹ Para reducir la cantidad de datos descargados del repositorio de ESET, se recomienda utilizar los nuevos parámetros de la herramienta Mirror distribuidos con ESET PROTECT 9: `--filterFilePath` y `--dryRun`:
1.Cree un filtro con formato *JSON* (consulte `--filterFilePath` a continuación).
2.Realice una ejecución de prueba de la herramienta Mirror con el parámetro `--dryRun` (véase a continuación) y ajuste el filtro según sea necesario.
3.Ejecute la herramienta Mirror con el parámetro `--filterFilePath` y el filtro de descarga definido, junto con los parámetros `--intermediateRepositoryDirectory` y `--outputRepositoryDirectory`.
4.Ejecute la herramienta Mirror periódicamente para utilizar siempre los instaladores más recientes.

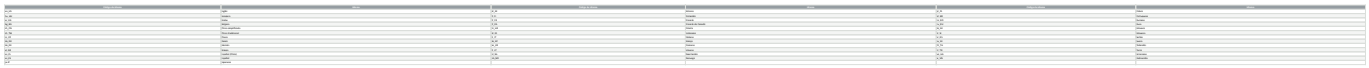
Parámetro	Descripción

`--filterFilePath`	Utilice este parámetro opcional para filtrar los productos de seguridad de ESET en función de un archivo de texto en formato *JSON* situado en la misma carpeta que la herramienta Mirror, por ejemplo: `--filterFilePath filter.txt`).
	Descripción de la configuración del filtro:
	El formato de los archivos de configuración para el filtrado de productos es *JSON* con la siguiente estructura:
	• objeto *JSON* raíz:
	o`use_legacy` (booleano, opcional): si es true, se incluirán los productos heredados.
	o`defaults` (objeto *JSON*, opcional): define las propiedades de filtro que se aplicarán a todos los productos.
	■`languages` (lista): especifica los códigos de idioma ISO de los idiomas que se van a incluir; por ejemplo, para francés, `"fr_FR"`. En la siguiente tabla puede consultar otros códigos de idioma: Para seleccionar más idiomas, sepárelos con una coma y un espacio, por ejemplo: (`["en_US", "zh_TW", "de_DE"]`)
	■`platforms` (lista): plataformas que se van a incluir (`["x64", "x86", "arm64"]`).
	⚠ Utilice el filtro `platforms` con prudencia. Por ejemplo, si la herramienta Mirror descarga solo instaladores de 64 bits y hay ordenadores de 32 bits en su infraestructura, los productos de seguridad de ESET de 64 bits no se instalarán en los ordenadores de 32 bits.
	■`os_types` (lista): tipos de sistema operativo que se van a incluir (`["windows"]`, `["linux"]`, `["mac"]`).
	o`products` (lista de objetos JSON, opcional): filtros que se aplican a productos específicos; anulan `defaults` para los productos especificados. Los objetos tienen las siguientes propiedades:
	■`app_id` (cadena): obligatoria si `name` no se especifica.
	■`name` (cadena): obligatoria si `app_id` no se especifica.
	■`version` (cadena): especifica la versión o la serie de versiones que se van a incluir.
	■`languages` (lista): códigos de idioma ISO de los idiomas que se van a incluir (consulte la tabla que aparece a continuación).
	■`platforms` (lista): plataformas que se van a incluir (`["x64", "x86", "arm64"]`).
	■`os_types` (lista): tipos de sistema operativo que se van a incluir (`["windows"]`, `["linux"]`, `["mac"]`).
	ℹ Para determinar los valores adecuados para los campos, ejecute la herramienta Mirror en el modo de simulacro y busque el producto correspondiente en el archivo CSV creado.
	Descripciones del formato de la cadena de versión
	Todos los números de versión están compuestos por cuatro cifras separadas por puntos (por ejemplo, `7.1.0.0`). Al introducir filtros de versión puede especificar menos cifras (por ejemplo, `7.1`) y el resto de números será cero (`7.1` será igual a `7.1.0.0`).
	La cadena de versión puede tener uno de los dos formatos siguientes:
	• [>|<|>=|<=|=]<n>.(<n>.(<n>.(<n>)))
	oSelecciona las versiones posteriores/anteriores, iguales/anteriores o iguales/iguales a la versión especificada.
	• <n>.(<n>.(<n>.(<n>))) - <n>.(<n>.(<n>.(<n>)))
	oSelecciona las versiones posteriores o iguales al límite inferior, y anteriores o iguales al límite superior.
	Se realizan comparaciones numéricas en cada parte del número de versión, de izquierda a derecha.
	Ejemplo de JSON
	✓
	`{`
	`"use_legacy": true,`
	`"defaults": {`
	`"languages": [ "en_US" ],`
	`"platforms": [ "x64", "x86" ]`
	`},`
	`"products": [`
	`{`
	`"app_id": "com.eset.apps.business.ees.windows",`
	`"version": "7.1.0.0 - 8.0.0.0"`
	`},`
	`{`
	`"app_id": "com.eset.apps.business.eea.windows",`
	`"version": ">7.1.0.0"`
	`}`
	`]`
	`}`
	El parámetro `--filterFilePath` sustituye a los parámetros `--languageFilterForRepository`, `--productFilterForRepository` y `--downloadLegacyForRepository` utilizados en versiones anteriores de la herramienta Mirror (distribuida con ESET PROTECT 8.x).

Parámetro	Descripción
`--dryRun`	Si utiliza este parámetro opcional, la herramienta Mirror no descargará ningún archivo, pero generará un archivo *.csv* con una lista de todos los paquetes que se descargarán. Puede utilizar este parámetro sin los parámetros obligatorios `--intermediateRepositoryDirectory` y `--outputRepositoryDirectory`, por ejemplo: `MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv`. Algunos instaladores de ESET son genéricos en cuanto al idioma (con el código de idioma `multilang`) y la herramienta Mirror los incluirá en el archivo *.csv* aunque se especifiquen `idiomas` en `--filterFilePath`. Si utiliza el parámetro `--dryRun` y también los parámetros `--intermediateRepositoryDirectory` y `--outputRepositoryDirectory`, la herramienta Mirror no borra el *outputRepositoryDirectory*.
`--listUpdatableProducts`	Enumerar todos los productos ESET para los que Mirror Tool puede descargar actualizaciones de los módulos (a menos que se utilice `--excludedProducts`). El parámetro está disponible en las versiones Mirror Tool: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).

La herramienta Mirror crea una estructura de carpetas distinta de la que crea el mirror de Endpoint. Cada carpeta contiene archivos de actualización para un grupo de productos. Tiene que especificar la ruta de acceso completa a la carpeta correcta en la configuración de actualización del producto usando el mirror. Por ejemplo, para actualizar ESET PROTECT 9 desde el mirror, establezca el servidor de actualización en (según la ubicación raíz de su servidor HTTP):
`http://your_server_address/mirror/eset_upd/era6`
Nota: La carpeta mirror de `era6` es común para estas soluciones de administración remota de ESET: ERA 6, ESMC 7, ESET PROTECT.

Tabla de códigos de idioma



```
sudo ./MirrorTool --mirrorType regular \
--intermediateUpdateDirectory /tmp/mirrorTool/mirrorTemp \
--offlineLicenseFilename /tmp/mirrorTool/offline.lf \
--outputDirectory /tmp/mirrorTool/mirror
```

Este es un ejemplo de configuración más avanzada para un repositorio sin conexión con los productos y los idiomas seleccionados y la descarga de archivos heredados activada definida en el archivo *filter.txt* (consulte el ejemplo de contenido de archivo en los detalles de `--filterFilePath` anteriores):

```
sudo ./MirrorTool --repositoryServer AUTOSELECT \
--intermediateRepositoryDirectory /tmp/repoTemp \
--outputRepositoryDirectory /var/lib/tomcat9/webapps/mirrorRepo \
--filterFilePath filter.txt
```

ESET le recomienda eliminar los comandos que contienen datos confidenciales (por ejemplo, una contraseña) del historial de la línea de comandos:
1.Ejecute `history` para ver una lista de todos los comandos del historial.
2.Ejecutar `history -d line_number` (especifique el número de línea del comando). También puede ejecutar `history -c` para eliminar todo el historial de la línea de comandos.

Herramienta Mirror y configuración de actualización

- Para automatizar la descarga de módulos, puede crear un programa para ejecutar la herramienta Mirror. Para hacerlo, abra Web Console y navegue hasta **Tareas del cliente** > **Sistema operativo** > **Ejecutar comando. Seleccione Línea de comandos para ejecutar** (incluida la ruta de acceso al archivo *MirrorTool.exe*) y un desencadenador razonable (por ejemplo, CRON para cada hora 0 0 * * * ? *). Asimismo, puede utilizar el Programador de tareas de Windows o `Cron` en Linux.

- Para configurar actualizaciones en ordenadores cliente, cree una nueva política y configure el **Servidor de actualización** para que apunte a su dirección mirror o carpeta compartida.

Instalación de componentes en macOS

En la mayoría de las situaciones de instalación, es necesario instalar los diferentes componentes de ESET PROTECTen diferentes máquinas para dar cabida a diferentes arquitecturas de red, cumplir con los requisitos de rendimiento, o por otras razones.

macOS solo se admite como cliente. Los productos ESET Management Agent y ESET para macOS se pueden instalar en macOS. Sin embargo, ESET PROTECT Server no se puede instalar en macOS.

Instalación del agente: macOS

Puede instalar ESET Management Agent en macOS de dos maneras:

- De forma remota: con la tarea del servidor **Implementación del agente**. Si tiene problemas al implementar ESET Management Agent de forma remota (la tarea de Server **Implementación del agente** termina con un estado de error), consulte Resolución de problemas de implementación del agente.

- Localmente: consulte las instrucciones que se indican a continuación.

Requisitos previos

- ESET PROTECT Server y ESET PROTECT Web Console se instalan (en un ordenador servidor).

- Se ha creado y preparado un certificado de agente en la unidad local.

- Hay una autoridad certificadora preparada en su unidad local (solo es necesaria para los certificados sin firmar).

Instalación

Siga los pasos indicados a continuación para instalar el componente ESET Management Agent localmente en

macOS:

Asegúrese de cumplir todos los requisitos previos de la instalación indicados anteriormente.

1. Obtenga el archivo de instalación (instalador del agente independiente *.dmg*) desde el sitio de descargas de ESET o el administrador del sistema.

2. Haga doble clic en el archivo *Agent-MacOSX-x86_64.dmg* y, a continuación, de nuevo en el archivo *.pkg* para iniciar la instalación.

3. Proceda con la instalación. Cuando se le solicite, introduzca los datos de **Conexión del servidor**:

- **Nombre de host del servidor**: nombre de host o dirección IP del servidor ESET PROTECT
- **Puerto del servidor**: puerto para la comunicación entre el agente y el servidor; el valor predeterminado es 2222.
- **Usar Proxy**: haga clic en esta opción si desea utilizar el proxy HTTP para la conexión entre el agente y el servidor.

Este ajuste de proxy se utiliza para la (replicación) entre ESET Management Agent y ESET PROTECT Server, no para el almacenamiento en caché de actualizaciones.
- **Nombre de host del servidor**: nombre de host o dirección IP de la máquina de proxy HTTP.
- **Puerto de proxy**: el valor predeterminado es 3128.
- **Nombre de usuario**, **Contraseña**: introduzca las credenciales utilizadas por el proxy si utiliza la autenticación.

Puede cambiar la configuración de proxy más adelante en la política. El proxy debe instalarse antes de poder configurar una conexión entre el agente y el servidor a través del proxy.

4. Seleccione un certificado de igual y una contraseña para este certificado. Opcionalmente, puede agregar una autoridad certificadora.

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

5. Revise la ubicación de la instalación y haga clic en **Instalar**. El agente se instalará en el ordenador.

6. El archivo de registro de ESET Management Agent se encuentra en el siguiente directorio:

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/
/Users/%user%/Library/Logs/EraAgentInstaller.log

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

Imagen ISO

El archivo de imagen ISO es uno de los formatos en los que puede descargar (categoría de instaladores todo en uno) los instaladores ESET PROTECT. La imagen ISO contiene lo siguiente:

- Paquete de instalación de ESET PROTECT
- Instaladores independientes para cada componente

Este formato es útil cuando se quiere mantener todos los instaladores de ESET PROTECT en un solo lugar. También elimina la necesidad de descargar los instaladores desde el sitio web de ESET cada vez que necesita ejecutar la instalación. La imagen ISO también es útil cuando se quiere instalar ESET PROTECT en una máquina virtual.

Registro de servicio de DNS

Para configurar un registro de recursos de DNS:

1.En el servidor de DNS (servidor de DNS de su controlador de dominio), vaya a **Panel de control** > **Herramientas administrativas**.

2.Seleccione el valor de DNS.

3.En el Administrador de DNS, seleccione _tcp en el árbol y cree un registro nuevo de **Ubicación del servicio (SRV)**.

4.Escriba el nombre del servicio en el campo **Servicio** de acuerdo con las reglas estándar de DNS, escriba un guion bajo (_) delante del nombre del servicio (utilice el nombre de su propio servicio, por ejemplo **_era**).

5.Introduzca el protocolo tcp en el campo **Protocolo** en el siguiente formato:_tcp.

6.Especifique el puerto 2222 en el campo **Número de puerto**.

7.Escriba el nombre de dominio completo (FQDN) de ESET PROTECT Server en el campo **Host que ofrece este de servicio**.

8.Haga clic en **Aceptar** > **Listo** para guardar el registro. El registro se mostrará en la lista.

Para verificar el registro de DNS:

1.Inicie sesión en cualquier ordenador de su dominio y abra una ventana del Símbolo del sistema (cmd.exe).

2.Escriba `nslookup` en el símbolo del sistema y pulse **Entrar**.

3.Escriba `set querytype=srv` y pulse **Entrar**.

4.Escriba `_era._tcp.domain.name` y pulse **Entrar**. La ubicación del servicio se muestra correctamente.

No olvide cambiar el valor "Host que ofrece este servicio:" al FQDN de su nuevo servidor cuando instala ESET PROTECT Server en un ordenador diferente.

Situación de instalación sin conexión de ESET PROTECT

Para instalar ESET PROTECT y sus componentes en entornos que no disponen de acceso a Internet, siga las instrucciones de instalación de alto nivel (con ESET PROTECT instalado en Windows).

En un ordenador con conexión a Internet

1. Cree una carpeta de red compartida.

2. Descargue los siguientes instaladores en la carpeta compartida:

   - Instalador todo en uno ESET PROTECT
   - Un paquete JDK compatible (necesario para Web Console).
   - Instalador de ESET Management Agent
   - Instaladores de productos de seguridad de ESET (por ejemplo, ESET Endpoint Security)

En un ordenador Windows sin conexión en la misma red local

1. Copie los instaladores de la carpeta compartida de red en un ordenador Windows sin conexión en el que desee instalar ESET PROTECT.

2. Instale el paquete JDK.

3. Instale ESET PROTECT en Windows con el instalador todo en uno. Seleccione **Activar más tarde** durante la instalación.

4. Active ESET PROTECT con una licencia sin conexión.

5. Implemente ESET Management Agent en ordenadores de su entorno sin conexión mediante Script instalador del agente. Modifique el script de instalación para utilizar la nueva URL y así acceder al paquete de instalación del agente desde la carpeta de red compartida.

6. Implemente los productos de seguridad ESET en las estaciones de trabajo mediante una Tarea de instalación de software. Seleccione **<Choose package>** y proporcione una URL personalizada para el paquete de instalación.

7. Active los puntos de conexión administrados con una licencia sin conexión.

8. Desactive ESET LiveGrid®.

Le recomendamos encarecidamente que mantenga actualizada la infraestructura de ESET sin conexión utilizando un repositorio de actualizaciones local. Actualice los módulos de los productos de seguridad de ESET con regularidad. Si los módulos no se actualizan, ESET PROTECT Web Console marca los ordenadores como **No actualizados**. Para silenciar esta advertencia de Web Console, haga clic en el ordenador de la lista y seleccione **Silenciar** en el menú contextual.

Para obtener instrucciones de actualización de ESET PROTECT, consulte Actualizar los componentes de ESET PROTECT en un entorno sin conexión.

Procedimientos de actualización

Existen diferentes formas de actualizar su ESET PROTECT Server y otros componentes de ESET PROTECT. Consulte también los procedimientos de migración y reinstalación.

Asegúrese de que tiene un sistema operativo compatible antes de actualizar a ESET PROTECT 9.1.
Si tiene una base de datos anterior no compatible instalada (MySQL 5.5 o MS SQL 2008/2012), actualice la base de datos a una versión de base de datos compatible antes de actualizar ESET PROTECT Server.

Actualización desde ERA 5 o 6.5

La actualización directa no es compatible; consulte Migración desde ERA 5.x o Actualización desde ERA 6.x.

Actualización desde ESMC 7.2 a la versión ESET PROTECT 9.1

Seleccione uno de los procedimientos de actualización:

Procedimientos de actualización	Sistema operativo	Comentario
Tarea Actualización de componentes en Web Console	Windows/Linux	
Instalador todo en uno ESET PROTECT 9.1	Windows	El instalador todo en uno es la opción de actualización recomendada si la instalación existente se realizó con el instalador todo en uno (tiene instalaciones predeterminadas de la base de datos de MS SQL y Apache Tomcat).
Actualización manual basada en componentes	Linux	Instrucciones para Linux para usuarios avanzados.
Actualizar el dispositivo virtual de ESET PROTECT	(Dispositivo virtual) Linux	

Para consultar la versión de cada componente de ESET PROTECT que está ejecutando, compruebe la versión de su instancia de ESET PROTECT Server. Vaya a la página Acerca de en ESET PROTECT Web Console y consulte la lista de todas las versiones de componentes de ESET PROTECT.

Tarea Actualización de componentes ESET PROTECT

Recomendaciones antes de actualizar

Le recomendamos que utilice la tarea ESET PROTECTActualización de componentes disponible en ESET PROTECT Web Console para actualizar su infraestructura de ESET PROTECT. Revise detenidamente las instrucciones indicadas aquí antes de actualizar.

Si la actualización de los componentes falla en un equipo en el que se ejecuta ESET PROTECT Server o Web Console, es posible que no pueda iniciar sesión en Web Console de forma remota. Recomendamos configurar el acceso físico al servidor antes de realizar esta actualización. Si no puede disponer de acceso físico al equipo, asegúrese de que puede iniciar sesión en él con privilegios de administrador a través de una sesión de escritorio remoto. Le recomendamos que realice una copia de seguridad de las bases de datos de ESET PROTECT Server y del Conector del dispositivo móvil antes de realizar esta operación. Para realizar una copia de seguridad del dispositivo virtual, cree una instantánea o clone su máquina virtual.

¿Está actualizando desde ESMC dispositivo virtual de ?

¿La instancia de ESET PROTECT Server está instalada en un clúster de conmutación por error?

Si su instancia de ESET PROTECT Server se encuentra instalada en un clúster de conmutación por error, debe actualizar el componente ESET PROTECT Server en cada nodo del clúster de forma manual. Tras actualizar ESET PROTECT Server, ejecute la tarea Actualización de componentes para actualizar el resto de su infraestructura (por ejemplo, los ESET Management Agent en ordenadores cliente).

Instrucciones importantes antes de actualizar el proxy HTTP Apache en Microsoft Windows

Si utiliza el proxy HTTP Apache y tiene una configuración personalizada en el archivo *httpd.conf* (como su nombre de usuario y contraseña), realice una copia de seguridad del archivo *httpd.conf* original (ubicado en *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf*). Si no está utilizando una configuración personalizada, no tendrá que realizar una copia de seguridad del archivo *httpd.conf*. Actualice a la versión más reciente del proxy HTTP Apache utilizando cualquiera de los métodos indicados en Actualización del proxy HTTP Apache.

después de actualizar Apache HTTP Proxy en Windows y de tener la configuración personalizada en el archivo *httpd.conf* original (como su nombre de usuario y contraseña), copie la configuración del archivo *httpd.conf* de copia de seguridad y aplique la configuración personalizada solo en el nuevo archivo *httpd.conf*. No utilice el archivo *httpd.conf* original con la versión actualizada del Apache HTTP Proxy, ya que no funcionará correctamente. Copie solo la configuración personalizada del mismo y utilice el nuevo archivo *httpd.conf*. Asimismo, puede personalizar el archivo *httpd.conf* nuevo de forma manual, la configuración se describe en Instalación del proxy HTTP Apache: Windows.

Instrucciones importantes antes de actualizar el proxy HTTP Apache en el dispositivo virtual

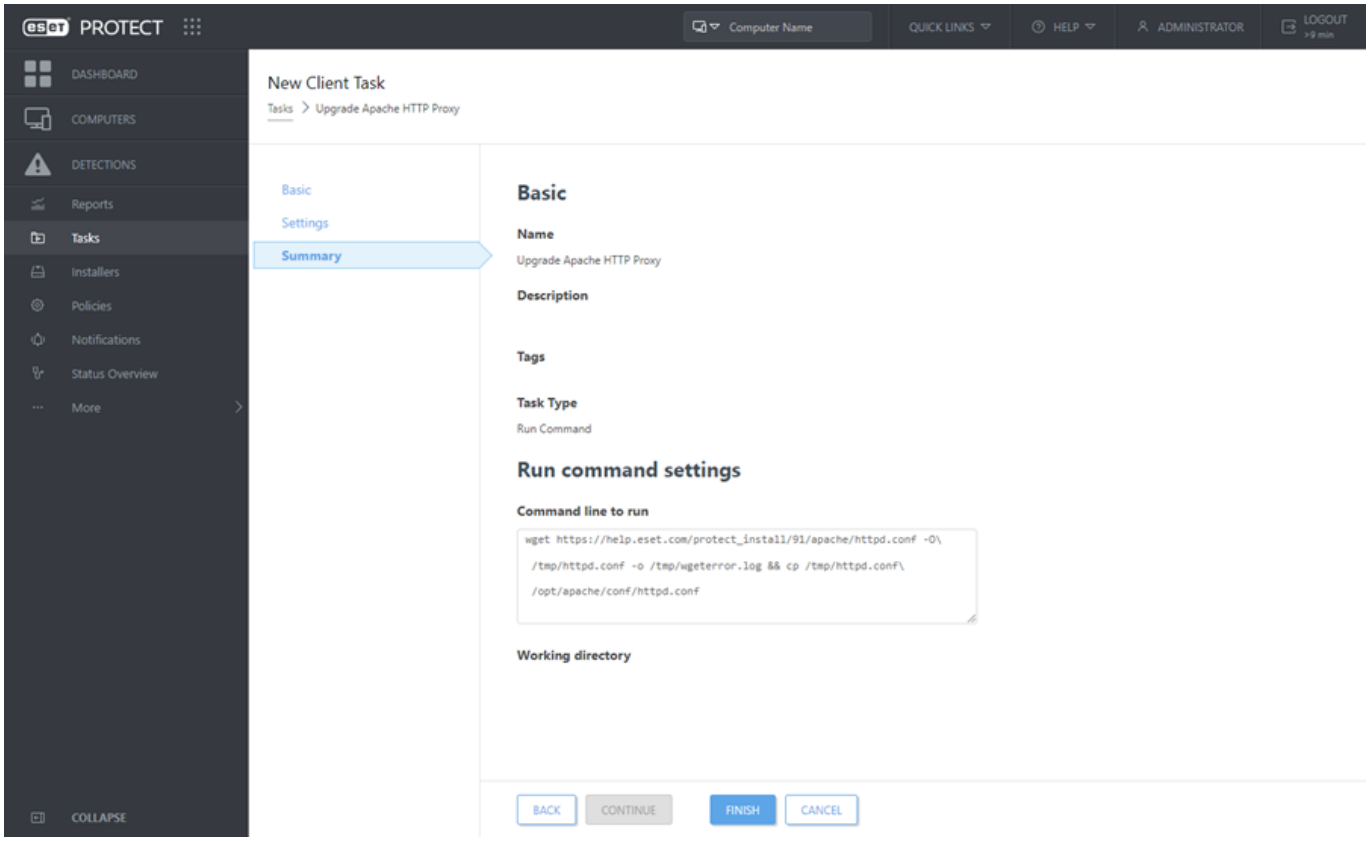
Si utiliza el **proxy HTTP Apache** y tiene una configuración personalizada en su archivo *httpd.conf* (como su nombre de usuario y su contraseña), realice una copia de seguridad del archivo *httpd.conf* original (ubicado en */opt/apache/conf/*) y, a continuación, ejecute la tarea **Actualización de componentes de ESET PROTECT** para actualizar el **proxy HTTP Apache**. Si no utiliza una configuración personalizada, no tendrá que crear una copia de seguridad de *httpd.conf*.

Cuando se complete correctamente la tarea Actualización de componentes, ejecute el siguiente comando. Asígnelo al equipo en el que está instalado el proxy HTTP Apache. Utilice la tarea del cliente Ejecutar comando para actualizar el archivo *httpd.conf* (es necesario para que la versión actualizada del proxy HTTP Apache se ejecute correctamente):

```
wget https://help.eset.com/protect_install/91/apache/httpd.conf -O\
```

```
/tmp/httpd.conf -o /tmp/wgeterror.log && cp /tmp/httpd.conf\

/opt/apache/conf/httpd.conf
```



Si el proxy HTTP Apache se está ejecutando en el equipo del dispositivo virtual, puede ejecutar el mismo comando directamente desde la consola del dispositivo virtual de ESET PROTECT. Otra opción es sustituir el archivo de configuración del proxy HTTP Apache httpd.conf de forma manual.

Si tiene una configuración personalizada en el archivo *httpd.conf* original (como su nombre de usuario y su contraseña), copie la configuración del archivo *httpd.conf* de copia de seguridad y añada solo la configuración personalizada al nuevo archivo *httpd.conf*. No utilice el archivo *httpd.conf* original con la nueva versión actualizada del proxy HTTP Apache, ya que no funcionará correctamente. Copie solo la configuración personalizada del mismo y utilice el nuevo archivo *httpd.conf*. Asimismo, puede personalizar el archivo *httpd.conf* manualmente. Consulte la configuración detallada en Instalación del proxy HTTP Apache - Linux.

Puede actualizar a ESET PROTECT 9.1 solo desde ESMC versión 7.2 y posteriores.
ESET PROTECT 9 le envía automáticamente una notificación cuando hay una nueva versión de ESET PROTECT Server disponible.
Haga una copia de seguridad de los siguientes datos antes de ejecutar la actualización:
• Todos los certificados (Autoridad certificadora, Certificado del servidor, Certificado del proxy y del agente).
• Exporte sus Certificados de autoridades certificadoras de un ESET PROTECT Server antiguo a un archivo *.der* y guárdelos en un sistema de almacenamiento externo.
• Exporte sus Certificados de iguales (para ESET Management Agent, ESET PROTECT Server) y el archivo *.pfx* de clave privada de un ESET PROTECT Server antiguo y guárdelos en un sistema de almacenamiento externo.
• Su base de datos de ESMC/ESET PROTECT. Si tiene una base de datos anterior no compatible instalada (MySQL 5.5 o MS SQL 2008/2012), actualice la base de datos a una versión de base de datos compatible antes de actualizar ESET PROTECT Server.

Asegúrese de que tiene un sistema operativo compatible antes de actualizar a ESET PROTECT 9.1.
Para actualizar los productos de seguridad ESET, ejecute la tarea Instalación de software con el paquete instalador más reciente para realizar la instalación de la versión más reciente sobre el producto existente.

Procedimiento de actualización recomendado

1. Actualizar ESET PROTECT Server: seleccione solo el equipo con ESET PROTECT Server como destino para la tarea **Actualización de componentes de ESET PROTECT**.

2. Seleccione algunos ordenadores cliente (como muestra de prueba: al menos un cliente de cada sistema operativo y valor de bits) y ejecute la tarea **Actualización de componentes de ESET PROTECT** en esos ordenadores.

Recomendamos utilizar el proxy HTTP Apache (o cualquier otro proxy web transparente con el almacenamiento en caché activado) para limitar la carga de la red. Los equipos cliente de prueba desencadenarán la descarga o el almacenamiento en caché de los instaladores. La próxima vez que se ejecute la tarea, los instaladores se distribuirán en los ordenadores cliente directamente desde la caché.

3. Cuando los ordenadores con ESET Management Agent actualizado se conecten correctamente a ESET PROTECT Server, siga actualizando el resto de clientes.

Para actualizar ESET Management Agents de todos los ordenadores administrados de la red, seleccione el grupo estático **Todos** como destino de la tarea **Actualización de componentes de ESET PROTECT**. La tarea omitirá los ordenadores que ya estén ejecutando la versión más reciente de ESET Management Agent.
ESET PROTECT 9.1 admite la actualización automática de ESET Management Agent en ordenadores administrados.

Componentes actualizados automáticamente:

- ESET PROTECT Server
- ESET Management Agent
- ESET PROTECT Web Console: solo se aplica cuando Apache Tomcat se ha instalado en su carpeta de instalación predeterminada en las distribuciones Windows y Linux, incluido el dispositivo virtual de ESET PROTECT (por ejemplo: */var/lib/tomcat8/webapps/*, */var/lib/tomcat7/webapps/*, */var/lib/tomcat/webapps/*).

Limitaciones de actualización de Web Console

- Apache Tomcat no se actualiza durante la actualización de ESET PROTECT Web Console mediante la tarea Actualización de componentes.
- La actualización de ESET PROTECT Web Console no funciona si Apache Tomcat se ha instalado en una ubicación personalizada.
- Si está instalada una versión personalizada de Apache Tomcat (instalación manual del servicio Tomcat), no se admite la actualización de ESET PROTECT Web Console con el instalador todo en uno ni con la tarea de actualización de componentes.

- ESET PROTECT Conector del dispositivo móvil

Componentes que requieren una actualización manual:

Componentes de ESET

- ESET Rogue Detection Sensor: utilice la tarea Instalación del software para la actualización. Asimismo, puede instalar la versión más reciente sobre una versión anterior (siga las instrucciones de instalación para Windows o Linux). Si instaló RD Sensor con la versión ESMC 7.2 y posteriores, no tendrá que actualizarlo, puesto que no hay versiones nuevas de RD Sensor.

Componentes de terceros

Además de los componentes de ESET, ESET PROTECT utiliza componentes de terceros que pueden quedar obsoletos y requerir una actualización manual.

En ESET PROTECT Web Console, haga clic en **Vínculos rápidos** > **Componentes obsoletos** para ver los componentes de terceros obsoletos.

El dispositivo virtual de ESET PROTECT no informa de componentes de terceros obsoletos.

ESET PROTECT informa como obsoletas de versiones anteriores a las indicadas a continuación:

Componente de terceros:	Versión:
Microsoft SQL Server	2019 (compilación 15.0.4223.0)1
MySQL	8.0.0.0
Sistema operativo2	Windows Server 2016
Apache Tomcat	9.0.62
Java	17.0

1 Determine su versión y su edición de SQL Server Database Engine e instale la actualización acumulativa más reciente.

2 ESET PROTECT no informa de un sistema operativo Linux obsoleto.

Siga las instrucciones de actualización de los componentes de terceros:

- Servidor de base de datos
- Sistema operativo
- Apache Tomcat

- Java Runtime Environment
- Proxy HTTP Apache

Resolución de problemas

- Compruebe si puede acceder al repositorio de ESET PROTECT desde un ordenador actualizado.
- Ejecutar la tarea Actualización de componentes de ESET PROTECT nuevo no funcionará si hay al menos un componente que ya se ha actualizado a una versión más reciente.
- Si no hay un motivo de fallo claro, puede actualizar los componentes de forma manual. Consulte nuestras instrucciones para Windows o Linux.
- Para ver más sugerencias sobre cómo resolver problemas de actualización, consulte Información general sobre la resolución de problemas.

Usar el instalador todo en uno de ESET PROTECT 9.1 para actualizar

Utilice el instalador todo en uno de ESET PROTECT 9.1 para actualizar ESMC 7.2 o una versión anterior de ESET PROTECT a la versión más reciente de ESET PROTECT 9.1.

El instalador todo en uno es la opción de actualización recomendada si la instalación existente se realizó con el instalador todo en uno (tiene instalaciones predeterminadas de la base de datos de MS SQL y Apache Tomcat).

El instalador todo en uno de ESET PROTECT 9.1 instala Microsoft SQL Server Express 2019 de forma predeterminada.

- Si utiliza una versión anterior de Windows (Server 2012 o SBS 2011), Microsoft SQL Server Express 2014 se instalará de forma predeterminada.
- El instalador genera automáticamente una contraseña aleatoria para la autenticación de la base de datos (almacenada en *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

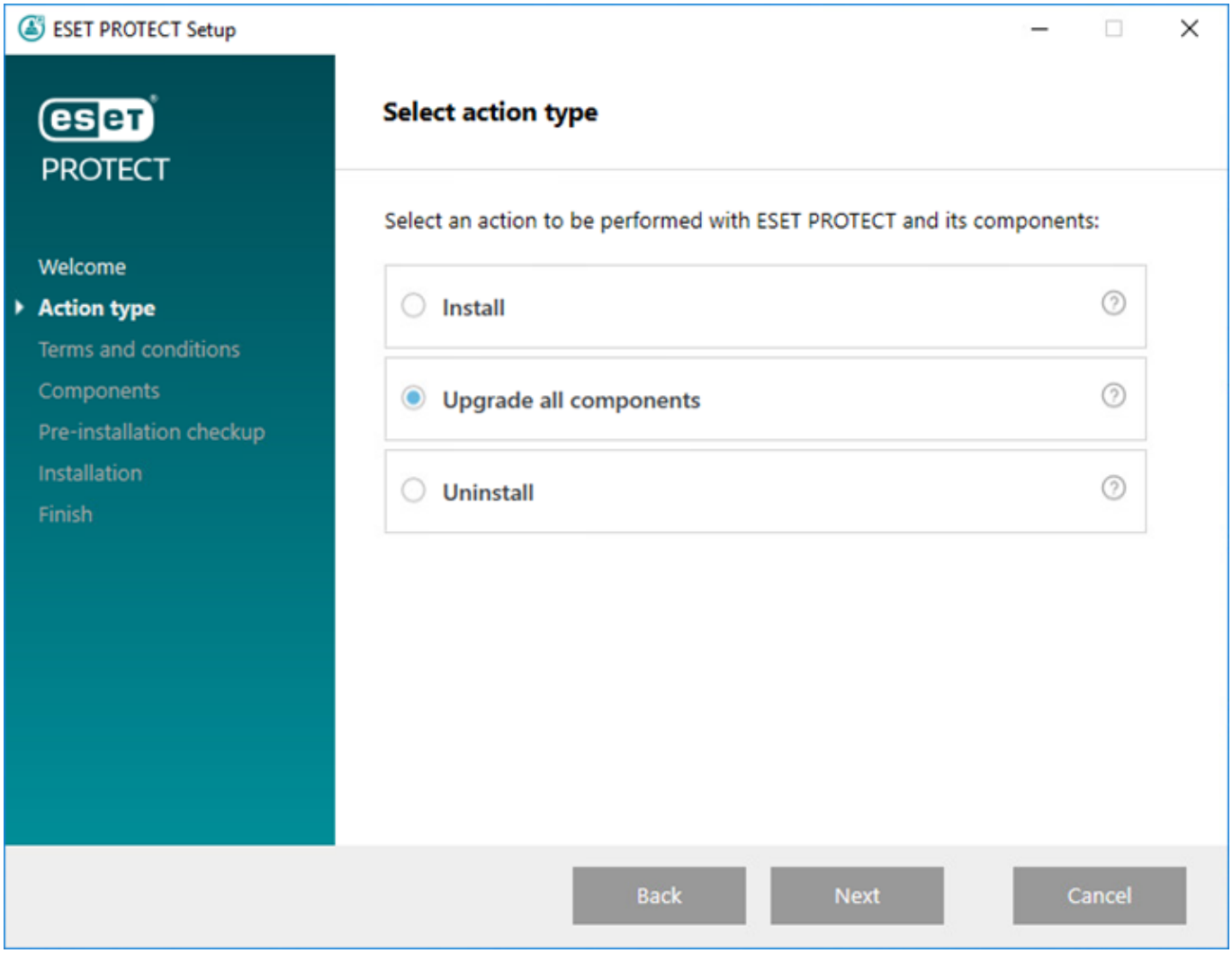
> ⚠ Microsoft SQL Server Express tiene un límite de tamaño de 10 GB en cada base de datos relacional. No recomendamos el uso de Microsoft SQL Server Express:
> - En entornos empresariales o redes de gran tamaño.
> - Si desea usar ESET PROTECT con ESET Inspect.

Puede actualizar a ESET PROTECT 9.1 solo desde ESMC versión 7.2 y posteriores.
Haga una copia de seguridad de los siguientes datos antes de ejecutar la actualización:
• Todos los certificados (Autoridad certificadora, Certificado del servidor, Certificado del proxy y del agente).
• Exporte sus Certificados de autoridades certificadoras de un ESET PROTECT Server antiguo a un archivo *.der* y guárdelos en un sistema de almacenamiento externo.
• Exporte sus Certificados de iguales (para ESET Management Agent, ESET PROTECT Server) y el archivo *.pfx* de clave privada de un ESET PROTECT Server antiguo y guárdelos en un sistema de almacenamiento externo.
• Su base de datos de ESMC/ESET PROTECT. Si tiene una base de datos anterior no compatible instalada (MySQL 5.5 o MS SQL 2008/2012), actualice la base de datos a una versión de base de datos compatible antes de actualizar ESET PROTECT Server.
Asegúrese de que tiene un sistema operativo compatible antes de actualizar a ESET PROTECT 9.1.

1.Ejecute *Setup.exe*.

2.Seleccione el idioma y haga clic en **Siguiente**.

3.Seleccione **Actualizar todos los componentes** y haga clic en **Siguiente**.



4.Lea el **Acuerdo de licencia para el usuario final**, acéptelo y haga clic en **Siguiente**.

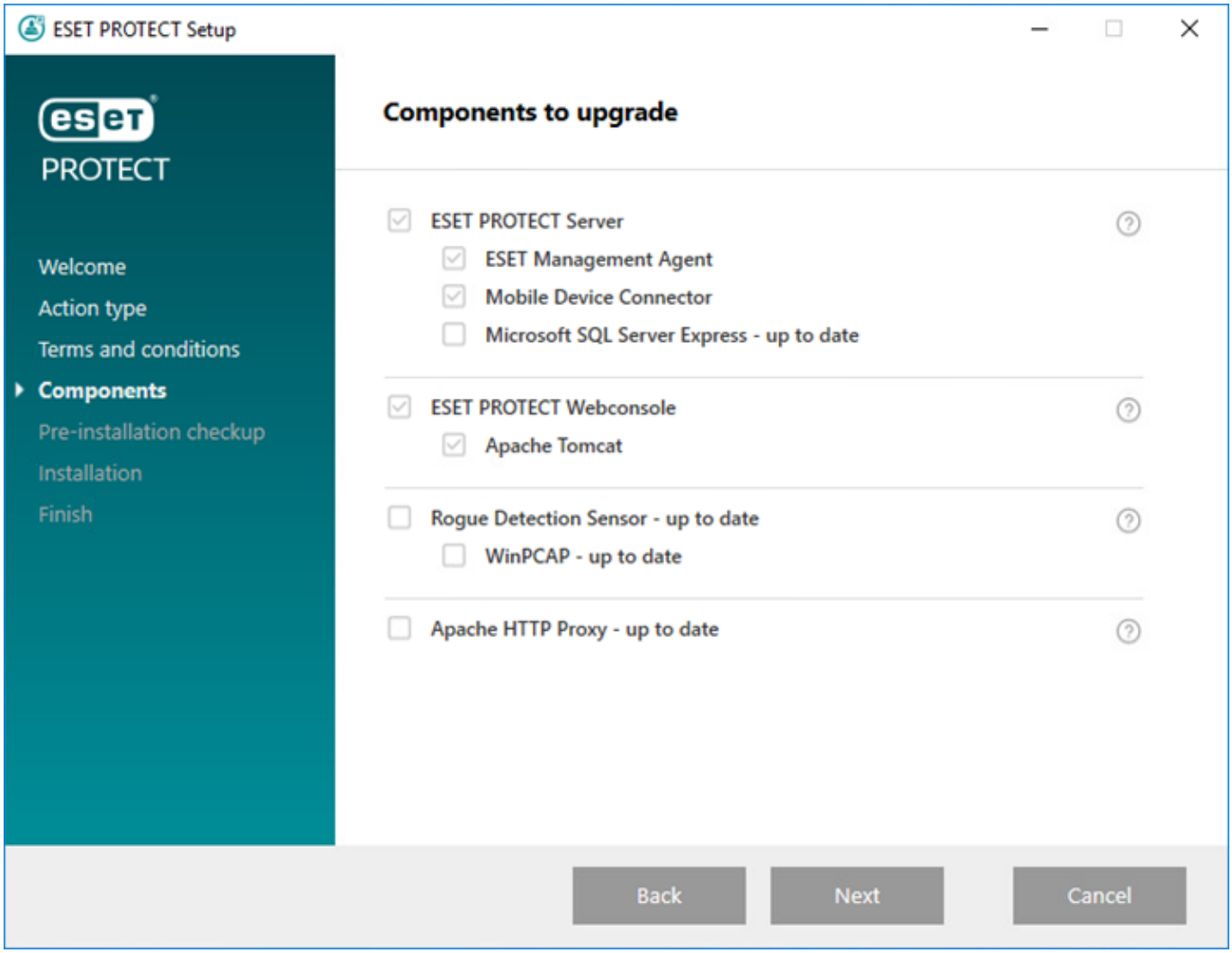
5.En **Componentes**, revise qué componentes de ESET PROTECT pueden actualizarse y haga clic en **Siguiente**.

Limitaciones de actualización de Apache Tomcat y Web Console

- Si está instalada una versión personalizada de Apache Tomcat (instalación manual del servicio Tomcat), no se admite la actualización de ESET PROTECT Web Console con el instalador todo en uno ni con la tarea de actualización de componentes.
- La actualización de Apache Tomcat eliminará la carpeta *era* ubicada en *C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\webapps*. Si usa la carpeta *era* para almacenar datos adicionales, asegúrese de realizar una copia de seguridad de los datos antes de realizar la actualización.
- Si se usa el usuario *C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\webapps* contiene datos adicionales (además de las carpetas *era* y *ROOT*), la actualización de Apache Tomcat no se llevará a cabo y solo se actualizará Web Console.
- La actualización de Web Console y Apache Tomcat borra los archivos de la Ayuda sin conexión. Si usó la ayuda sin conexión con ESMC o una versión más antigua de ESET PROTECT, vuelva a crearla para ESET PROTECT 9.1 tras la actualización para asegurarse de que tiene la ayuda sin conexión más reciente que coincide con su versión de ESET PROTECT.

Limitaciones de actualización del proxy HTTP Apache

El instalador todo en uno sobrescribe *httpd.conf* y guarda la configuración original en *httpd.conf.old*. Para mantener la configuración personalizada del proxy HTTP Apache, haga una copia de seguridad de la configuración y vuelva a utilizarla.



6.Siga la **Comprobación previa a la instalación** para asegurarse de que su sistema cumple con todos los requisitos previos.

7.Haga clic en **Actualizar** para iniciar la actualización de ESET PROTECT. La actualización puede llevar cierto

tiempo, en función del sistema y la configuración de red.

8.Cuando finalice la actualización, haga clic en **Finalizar**.

9.Tras actualizar ESET PROTECT, actualice ESET Management Agent en los ordenadores administrados utilizando la tarea Actualización de componentes. ESET PROTECT 9.1 admite la actualización automática de ESET Management Agent en ordenadores administrados.

Actualización desde ERA 6.5

No puede actualizar directamente a ESET PROTECT 9.1.

Si tiene ERA 6.5 instalado, realice estas acciones:

1.Actualice de ERA 6.5 a ESET PROTECT 8.1.

2.Actualizar ESET PROTECT 8.1 a ESET PROTECT 9.1.

Actualización/copia de seguridad del servidor de bases de datos

ESET PROTECT usa una base de datos para almacenar los datos del cliente. En las siguientes secciones se detallan la copia de seguridad y la actualización de la base de datos de ESET PROTECT Server (o ESMC):

- Si no tiene una base de datos configurada para usarla con ESET PROTECT Server, **Microsoft SQL Server Express** está incluido en el instalador. El instalador todo en uno de ESET PROTECT 9.1 instala Microsoft SQL Server Express 2019 de forma predeterminada.

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

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

> ⚠ Microsoft SQL Server Express tiene un límite de tamaño de 10 GB en cada base de datos relacional. No recomendamos el uso de Microsoft SQL Server Express:
> - En entornos empresariales o redes de gran tamaño.
> - Si desea usar ESET PROTECT con ESET Inspect.

- Si tiene una base de datos anterior no compatible instalada (MySQL 5.5 o MS SQL 2008/2012), actualice la base de datos a una versión de base de datos compatible antes de actualizar ESET PROTECT Server.

Consulte también Migración de la base de datos de ESET PROTECT.

Se deben cumplir los siguientes requisitos para Microsoft SQL Server:

• Instale una versión compatible de Microsoft SQL Server. Elija el tipo de autenticación **Modo mixto** durante la instalación.

• Si ya tiene Microsoft SQL Server instalado, configure la autenticación como **Modo mixto (autenticación de SQL Server y de Windows)**. Para ello, siga las instrucciones de este artículo de la Base de conocimiento. Si desea usar la **Autenticación de Windows** para iniciar sesión en Microsoft SQL Server, siga los pasos indicados en este artículo de la Base de conocimiento.

• Permita las conexiones TCP/IP con SQL Server. Para ello, siga las instrucciones de este artículo de la Base de conocimiento desde la parte **II. Permitir las conexiones TCP/IP con la base de datos SQL**.

• Para configurar, gestionar y administrar Microsoft SQL Server (bases de datos y usuarios), descargue SQL Server Management Studio (SSMS).
• No instale SQL Server en un controlador de dominio (por ejemplo, Windows SBS o Essentials). Le recomendamos que instale ESET PROTECT en un servidor diferente o que no seleccione el componente SQL Server Express durante la instalación (necesita utilizar su SQL o MySQL Server existente para ejecutar la base de datos de ESET PROTECT).

Copia de seguridad y restauración del servidor de bases de datos

Toda la información y los ajustes de ESET PROTECT se almacenan en la base de datos. Le recomendamos que haga una copia de su base de datos con regularidad para evitar la pérdida de datos. Puede utilizar la copia de seguridad más adelante cuando realice la migración ESET PROTECT a un servidor nuevo. Consulte la sección adecuada a continuación para su base de datos:

• El nombre de las bases de datos y los archivos de registro no cambia, ni siquiera después del cambio de nombre del producto de ESET Security Management Center a ESET PROTECT.
• Si utiliza el dispositivo virtual de ESET PROTECT, siga las instrucciones de copia de seguridad de la base de datos del dispositivo virtual.

Ejemplos de copia de seguridad de MS SQL

Para realizar una copia de seguridad de una base de datos de MS SQL en un archivo, siga los ejemplos indicados a continuación:

Estos ejemplos están pensados para utilizarlos con la configuración predeterminada (por ejemplo, los valores predeterminados de configuración de conexión de la base de datos y de nombre de la base de datos). El script tendrá que personalizarse para dar cabida a los cambios realizados en la configuración predeterminada.
Debe tener los derechos correspondientes para ejecutar los comandos que se indican a continuación. Si no usa una cuenta de usuario de administrador local, deberá cambiar la ruta de la copia de seguridad, por ejemplo, a *'C:\USERS\PUBLIC\BACKUPFILE'*.

Copia de seguridad única de la base de datos

Ejecute este comando en un símbolo del sistema de Windows para crear una copia de seguridad en el archivo denominado **BACKUPFILE**:

```
SQLCMD -S HOST\ERASQL -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'"
```

> En este ejemplo, **HOST** equivale a la dirección IP o el nombre de host, y **ERASQL** al nombre de la instancia de MS SQL Server. Puede instalar ESET PROTECT Server en una instancia SQL con nombre personalizada (al usar la base de datos MS SQL). En esta situación debe modificar los scripts de la copia de seguridad según proceda.

Copia de seguridad periódica de la base de datos con script SQL

Elija uno de los siguientes scripts SQL:

a)Crear copias de seguridad periódicas y guárdelas en función de su fecha de creación:

```
1.@ECHO OFF

2.SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'

  WITH NOFORMAT,INIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR, CHE
CKSUM, STATS=10"

3.REN BACKUPFILE BACKUPFILE-
[%DATE:~10,4%%DATE:~4,2%%DATE:~7,2%_T%TIME:~0,2%%TIME:~3,2%].bac
```

b)Añadir la copia de seguridad a un archivo:

```
1. @ECHO OFF

2. SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'

   WITH NOFORMAT, NOINIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR,
 CHECKSUM, STATS=10"
```

Restauración de MS SQL

Para restaurar una copia de seguridad de una base de datos de MS SQL desde un archivo, siga el ejemplo indicado a continuación:

```
SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "RESTORE DATABASE ERA_DB FROM DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'"
```

Copia de seguridad de MySQL

Para realizar una copia de seguridad de una base de datos de MySQL en un archivo, siga el ejemplo indicado a continuación:

```
mysqldump --host HOST --disable-keys --extended-insert --routines -u ROOTLOGIN -
p DBNAME -r BACKUPFILE
```

En este ejemplo, **HOST** equivale a la dirección IP o el nombre de host del servidor MySQL, **ROOTLOGIN** a la cuenta root de MySQL Server y **DBNAME** al nombre de la base de datos de ESET PROTECT.

Restauración de MySQL

Para restaurar una copia de seguridad de una base de datos de MySQL desde un archivo, siga el ejemplo indicado a continuación:

```
mysql --host HOST -u ROOTLOGIN -p DBNAME < BACKUPFILE
```

Para obtener más información sobre la copia de seguridad de bases de datos de Microsoft SQL Server, visite el sitio web de Microsoft TechNet. Para obtener más información sobre la copia de seguridad de bases de datos de MySQL Server, visite el sitio web de documentación de MySQL.

Actualización del servidor de la base de datos

Siga las instrucciones indicadas a continuación para actualizar una instancia de Microsoft SQL Server existente a una versión más reciente para usarla con la base de datos de ESET PROTECT Server:

1. Utilice la opción Detener para parar todos los servicios de ESMC/ESET PROTECT Server o Proxy que se encuentren en ejecución y se estén conectando al servidor de base de datos que va a actualizar. También puede detener el resto de aplicaciones que podría estar conectándose a su instancia de Microsoft SQL Server.

2. Realice una copia de seguridad de todas las bases de datos relevantes antes de continuar.

3. Realice la actualización del servidor de la base de datos:

Actualizar SQL Server (Windows):

- Siga el artículo de la base de conocimiento para actualizar la base de datos de MS SQL Express a la versión más reciente.
- También puede seguir las instrucciones del proveedor de la base de datos: https://msdn.microsoft.com/en-us/library/bb677622.aspx.
- No se admite MS SQL Server en Linux. Sin embargo, puede conectar ESET PROTECT Server en Linux a MS SQL Server en Windows.

Actualizar MySQL Server (Windows y Linux):

- Actualizar desde MySQL 5.6 a la versión 5.7
- Actualizar desde MySQL 5.7 a la versión 8

4. Utilice la opción IniciarESET PROTECT Server y revise los registros de seguimiento para asegurarse de que la conexión con la base de datos funciona correctamente.

ActualizaciónESMC/ESET PROTECTinstalación en un clúster de conmutación por error en Windows

Si tiene ESMC/ESET PROTECT Server instalado en un entorno de clúster de conmutación por error en Windows, siga los pasos indicados a continuación para actualizar a la versión más reciente de ESET PROTECT:

Asegúrese de tener un sistema operativo compatible.

1. Detenga la función del clúster de ESMC/ESET PROTECT Server en el administrador de clústeres. Asegúrese de que el servicio (**ESET Security Management Center Server** o **ESET PROTECT Server**) esté detenido en todos los nodos del clúster.

2. Conecte el disco compartido del clúster en el nodo1 y actualice el componente de Server manualmente. Para ello, ejecute el último instalador *.msi* como en el caso de la instalación de un componente.

3. Una vez finalizada la instalación (actualización), asegúrese de que el servicio **ESET PROTECT Server** se haya detenido.

4. Conecte el disco compartido del clúster en el nodo2 y actualice el componente de Server del mismo modo que en el paso n.º 2.

5. Una vez que ESET PROTECT Server esté actualizado en todos los nodos del clúster, inicie la **función de ESET PROTECT Server** en el administrador de clústeres.

6. Actualice ESET Management Agent manualmente ejecutando el último instalador *.msi* en todos los nodos del clúster.

7. En ESET PROTECT Web Console, compruebe si las versiones del agente y del servidor de todos los nodos muestran la última versión a la que ha actualizado.

Actualizar el proxy HTTP Apache

El proxy HTTP Apache es un servicio que puede usarse junto con ESET PROTECT para distribuir las actualizaciones a los ordenadores cliente y los paquetes de instalación a instancias de ESET Management Agent.

Si instaló el proxy HTTP Apache anteriormente en Windows y desea actualizarlo a la versión más reciente, puede hacerlo de dos formas diferentes, bien manualmente o a través del instalador todo en uno.

Actualizar el proxy HTTP Apache con el instalador todo en uno (Windows)

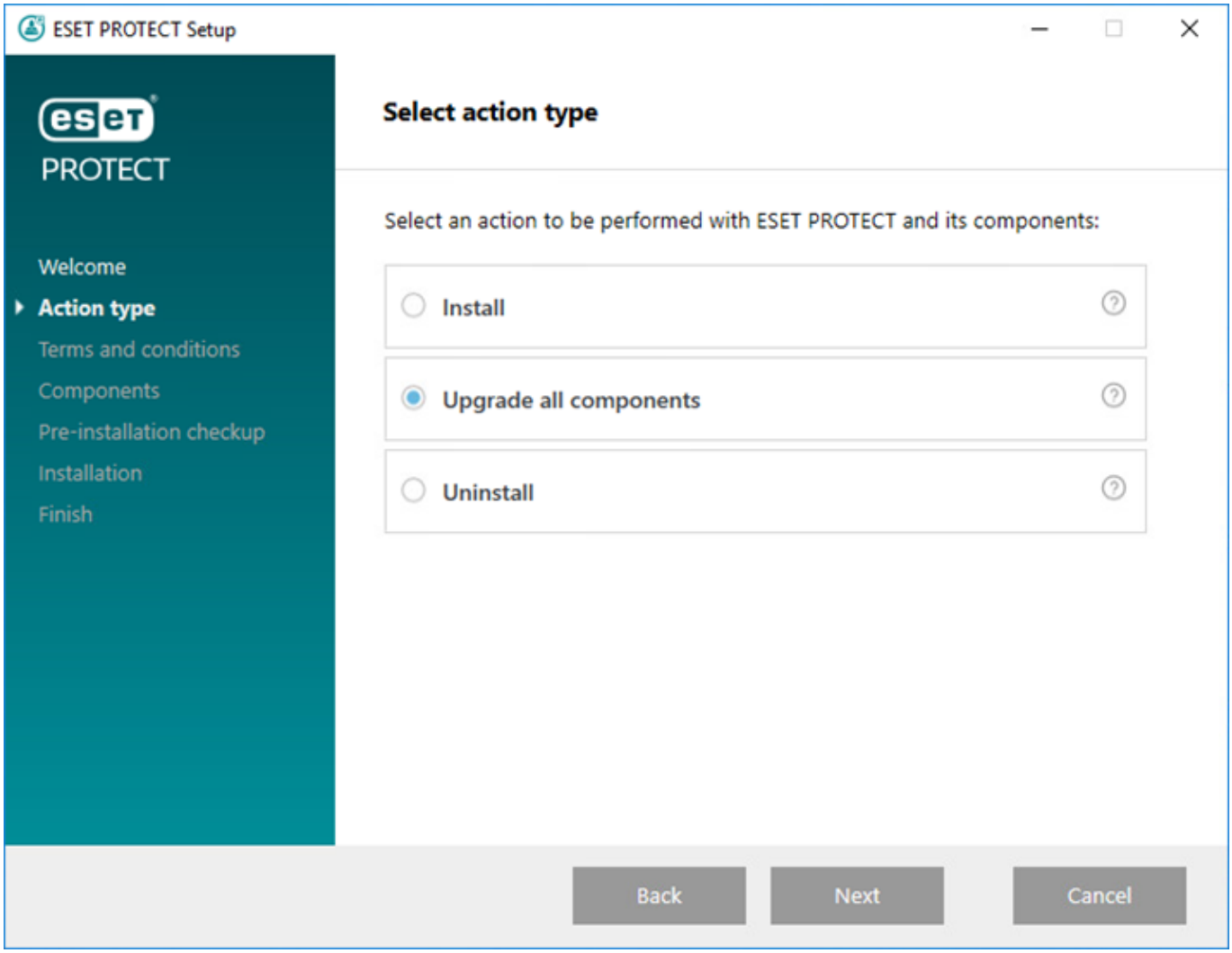
Si descargó el instalador todo en uno de ESET PROTECT más reciente, puede utilizar este método para actualizar rápidamente el proxy HTTP Apache a la versión más reciente. Si no tiene el instalador más reciente descargado, utilice el método de actualización manual del proxy HTTP Apache.

1. Realice una copia de seguridad de los siguientes archivos:

- *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf*
- *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\password.file*
- *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\group.file*

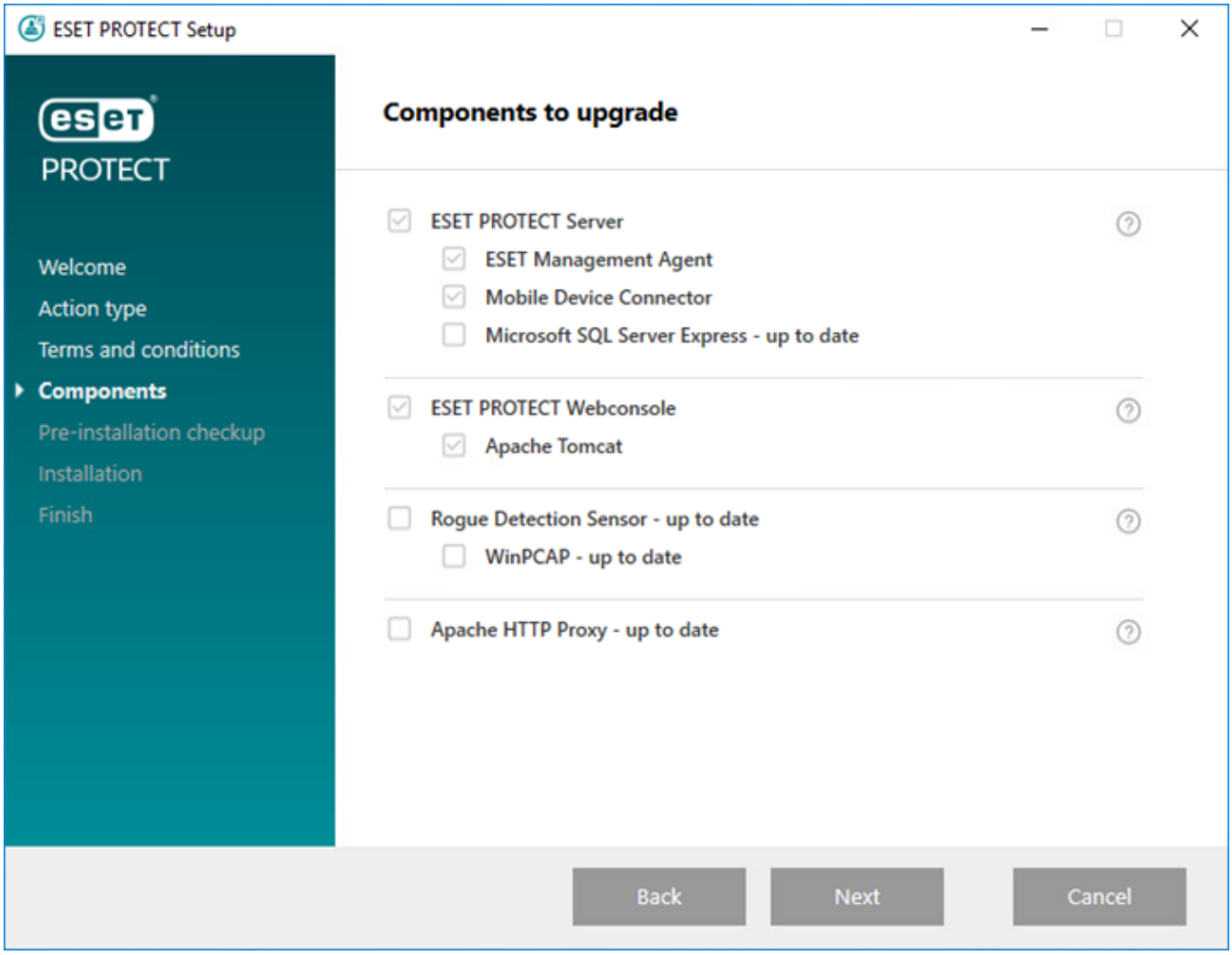
2. Inicie el instalador todo en uno; para ello, haga doble clic en el archivo *setup.exe* y haga clic en **Siguiente** en la pantalla de bienvenida.

3. Seleccione **Actualizar todos los componentes** y haga clic en **Siguiente**.



4. Lea el **Acuerdo de licencia para el usuario final**, acéptelo y haga clic en **Siguiente**.

5. En **Componentes**, revise qué componentes de ESET PROTECT pueden actualizarse y haga clic en **Siguiente**.



6. Siga la **Comprobación previa a la instalación** para asegurarse de que su sistema cumple con todos los requisitos previos.

7. Haga clic en **Actualizar** para iniciar la actualización de ESET PROTECT. La actualización puede llevar cierto tiempo, en función del sistema y la configuración de red.

8. Cuando finalice la actualización, haga clic en **Finalizar**.

El instalador todo en uno sobrescribe *httpd.conf* y guarda la configuración original en *httpd.conf.old*. Para mantener la configuración personalizada del proxy HTTP Apache, haga una copia de seguridad de la configuración y vuelva a utilizarla.

9. Pruebe la conexión con el proxy HTTP Apache; para ello, acceda a la siguiente URL desde su navegador:

http://[IP address]:3128/index.html

Resolución de problemas

Para resolver un problema, consulte los archivos de registro del proxy HTTP Apache.

Si se realizó una configuración personalizada en el archivo *httpd.conf* en la instalación anterior del proxy HTTP Apache, siga estos pasos:

1. Detenga el servicio **ApacheHttpProxy** abriendo un símbolo del sistema de administración y ejecutando el

siguiente comando:

```
sc stop ApacheHttpProxy
```

2.Si utiliza un nombre de usuario o contraseña para acceder al proxy HTTP Apache (tema Instalación del proxy HTTP Apache), sustituya el siguiente bloque de código:

```
<Proxy *>
 Deny from all
</Proxy>
```

por el siguiente bloque de código (está en la copia de seguridad de *httpd.conf*):

```
<Proxy *>
 AuthType Basic
 AuthName "Password Required"
 AuthUserFile password.file
 AuthGroupFile group.file
 Require group usergroup
 Order deny,allow
 Deny from all
 Allow from all
</Proxy>
```

3.Si personalizó de algún otro modo el archivo *httpd.conf* en la instalación anterior del proxy HTTP Apache, podrá copiar manualmente esas modificaciones desde *httpd.conf.old* (o desde la copia de seguridad de *httpd.conf* realizada en el paso 1) hasta el archivo *httpd.conf* nuevo (actualizado).

4.Guarde los cambios e inicie el servicio **ApacheHttpProxy** ejecutando el siguiente comando en un símbolo del sistema elevado:

```
sc start ApacheHttpProxy
```

Actualizar el proxy HTTP Apache de forma manual (Windows)

Para actualizar Apache HTTP Proxy a la versión más reciente, siga los pasos que se indican a continuación.

1. Realice una copia de seguridad de los siguientes archivos:

   • *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf*

   • *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\password.file*

   • *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\group.file*

2. Detenga el servicio **ApacheHttpProxy** abriendo un símbolo del sistema de administración y ejecutando el siguiente comando:

```
sc stop ApacheHttpProxy
```

3. Descargue el archivo de instalación del Apache HTTP Proxy del sitio de descargas de ESET y extraiga su contenido en *C:\Program Files\Apache HTTP Proxy 2.[x.xx]*\. Durante la extracción sobrescriba los archivos

existentes.

4. Vaya a *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf*, haga clic con el botón derecho del ratón en *httpd.conf*, en el menú contextual, y seleccione **Abrir con** > **Bloc de notas**.

5. Añada el siguiente código al final de *httpd.conf*:

```
ServerRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]"
DocumentRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs">
 Options Indexes FollowSymLinks
 AllowOverride None
 Require all granted
</Directory>
CacheRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\cache"
```

6. Si configura un nombre de usuario o contraseña para acceder al proxy HTTP Apache (tema Instalación del proxy HTTP Apache), sustituya el siguiente bloque de código:

```
<Proxy *>
 Deny from all
</Proxy>
```

por este otro (se encuentra en el archivo *httpd.conf* de la copia de seguridad que realizó en el paso 1):

```
<Proxy *>
 AuthType Basic
 AuthName "Password Required"
 AuthUserFile password.file
 AuthGroupFile group.file
 Require group usergroup
 Order deny,allow
 Deny from all
 Allow from all
</Proxy>
```

Si se realizaron otras personalizaciones del archivo *httpd.conf* en la instalación anterior del proxy HTTP Apache, copie las modificaciones de la configuración desde el archivo *httpd.conf* de copia de seguridad en el archivo *httpd.conf* nuevo (actualizado).

7. Guarde los cambios e inicie el servicio **ApacheHttpProxy** ejecutando el siguiente comando en un símbolo del sistema de administración:

```
sc start ApacheHttpProxy
```

8. Actualice la versión en la descripción del servicio.

```
sc description ApacheHttpProxy "Apache/2.4.43"
```

9. Pruebe la conexión con el proxy HTTP Apache; para ello acceda a la siguiente URL desde su navegador:

http:///[IP address]:3128/index.html

Consulte los archivos de registro del proxy HTTP Apache si debe solucionar algún problema.

Actualizar Apache Tomcat

Apache Tomcat es un componente obligatorio necesario para ejecutar ESET PROTECT Web Console.

Si está actualizando a una versión más reciente de ESET PROTECT, o si no ha actualizado Apache Tomcat durante un periodo de tiempo prolongado, debería plantearse actualizar Apache Tomcat a la última versión. Si mantiene servicios de orientación pública, como Apache Tomcat y sus dependencias, actualizados se reducirán los riesgos de seguridad en su entorno.

Para actualizar Apache Tomcat, siga las instrucciones:

- Instrucciones para Windows (el instalador todo en uno de ESET PROTECT más reciente) - Esta es la opción de actualización recomendada si la instalación de Apache Tomcat se realizó con el instalador todo en uno.
- Instrucciones para Windows (instalación manual) – Actualice Apache Tomcat manualmente si realizó la instalación de Apache Tomcat existente manualmente o no tiene el instalador todo en uno de ESET PROTECT más reciente.
- Instrucciones para Linux

Actualizar Apache Tomcat con el instalador todo en uno (Windows)

Apache Tomcat es un componente obligatorio necesario para ejecutar ESET PROTECT Web Console. Use este método para actualizar Apache Tomcat con la versión más reciente del instalador todo en uno de ESET PROTECT 9.1. Esta es la opción de actualización recomendada si la instalación de Apache Tomcat se realizó con el instalador todo en uno. También puede actualizar Apache Tomcat manualmente.

Antes de actualizar

Realice una copia de seguridad de los siguientes archivos:

C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\.keystore
C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\conf\server.xml
C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties

Si utiliza un almacén de certificados SSL personalizado en la carpeta *Tomcat*, realice también una copia de seguridad de ese certificado.

Limitaciones de actualización de Apache Tomcat y Web Console

- Si está instalada una versión personalizada de Apache Tomcat (instalación manual del servicio Tomcat), no se admite la actualización de ESET PROTECT Web Console con el instalador todo en uno ni con la tarea de actualización de componentes.
- La actualización de Apache Tomcat eliminará la carpeta *era* ubicada en *C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\webapps*. Si usa la carpeta *era* para almacenar datos adicionales, asegúrese de realizar una copia de seguridad de los datos antes de realizar la actualización.
- Si se usa el usuario *C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\webapps* contiene datos adicionales (además de las carpetas *era* y *ROOT*), la actualización de Apache Tomcat no se llevará a cabo y solo se actualizará Web Console.
- La actualización de Web Console y Apache Tomcat borra los archivos de la Ayuda sin conexión. Si usó la ayuda sin conexión con ESMC o una versión más antigua de ESET PROTECT, vuelva a crearla para ESET PROTECT 9.1 tras la actualización para asegurarse de que tiene la ayuda sin conexión más reciente que coincide con su versión de ESET PROTECT.

Procedimientos de actualización

1. Descargue el instalador todo en uno de ESET PROTECT del sitio web de ESET y descomprima el archivo descargado.

2. Si desea instalar la versión más reciente de Apache Tomcat y el instalador todo en uno contiene una versión más antigua de Apache Tomcat (este paso es opcional, vaya al paso 4 si no necesita la versión más reciente de Apache Tomcat):

   a. Abra la carpeta *x64* y diríjase a la carpeta *installers*.

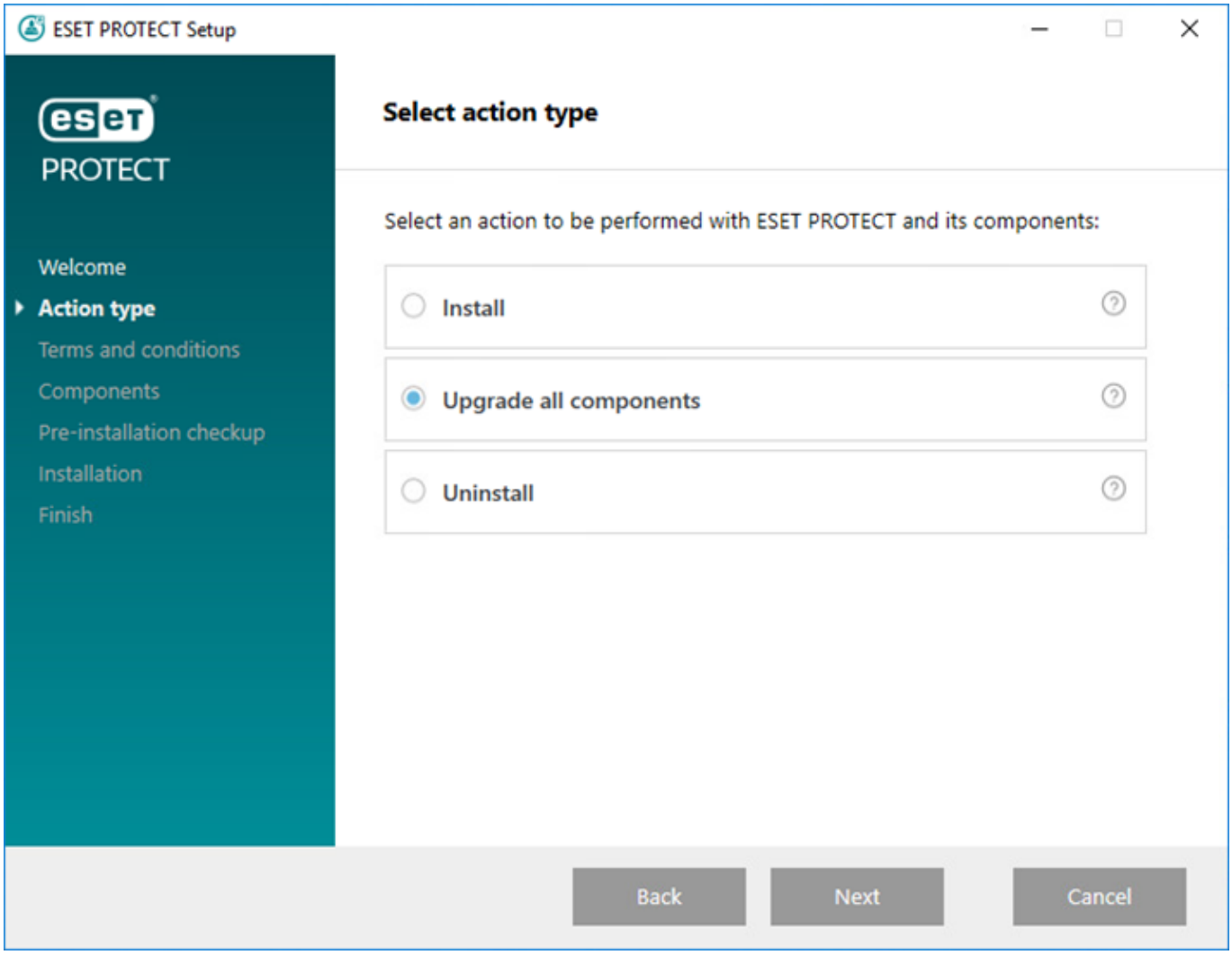
   b. Elimine el archivo *apache-tomcat-9.0.x-windows-x64.zip* situado en la carpeta *installers*.

   c. Descargue el paquete zip para Windows de 64 bits de Apache Tomcat 9.

   d. Mueva el paquete zip descargado a la carpeta *installers*.

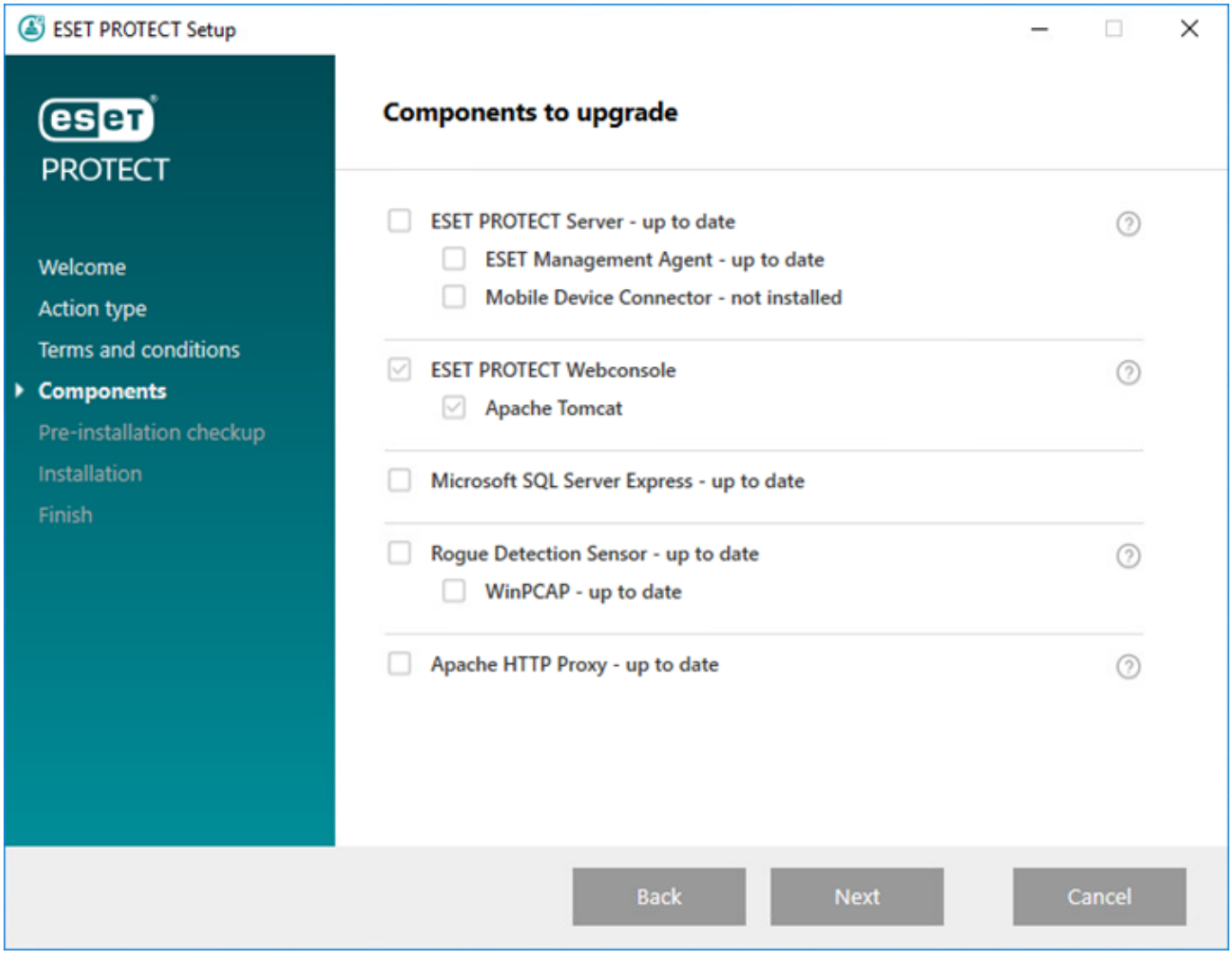
3. Para iniciar el instalador todo en uno, haga doble clic en el archivo *Setup.exe* y haga clic en **Siguiente** en la pantalla **Bienvenido**.

5. Seleccione **Actualizar todos los componentes** y haga clic en **Siguiente**.



6. Tras aceptar el EULA, haga clic en **Siguiente**.

7. El instalador todo en uno detecta automáticamente si la actualización está disponible: hay casillas de verificación junto a los componentes de ESET PROTECT que se pueden actualizar. Haga clic en **Siguiente**.



8. Seleccione una instalación de Java en el ordenador. Apache Tomcat requiere Java/OpenJDK de 64 bits. Si tiene instaladas en su sistema varias versiones de Java, le recomendamos que desinstale las versiones de Java anteriores y mantenga únicamente la versión de Java compatible.

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

9. Haga clic en **Actualizar** para completar la actualización y, a continuación, haga clic en **Finalizar**.

10. Si ha instalado Web Console en un ordenador distinto de ESET PROTECT Server:

a. Detenga el servicio Apache Tomcat: Diríjase a **Inicio** > **Servicios** > haga clic con el botón derecho del ratón en el servicio Apache Tomcat y seleccione **Detener**.

b.Restaure el archivo *EraWebServerConfig.properties* (desde el paso 1) en su ubicación original.

c. Reinicie el servicio Apache Tomcat: Diríjase a **Inicio** > **Servicios** > haga clic con el botón derecho del ratón en el servicio Apache Tomcat y seleccione **Iniciar**.

11. Conéctese a ESET PROTECT Web Console y asegúrese de que Web Console se carga correctamente.

ℹ Consulte también la configuración de Web Console adicional para soluciones empresariales o sistemas de bajo rendimiento.

Resolución de problemas

Si se produce un error al actualizar Apache Tomcat, instale la versión anterior y aplique la configuración desde el paso 1.

Actualizar Apache Tomcat de forma manual (Windows)

Apache Tomcat es un componente obligatorio necesario para ejecutar ESET PROTECT Web Console. Actualice Apache Tomcat manualmente si realizó la instalación de Apache Tomcat existente manualmente o no tiene el instalador todo en uno de ESET PROTECT más reciente.

Si está instalada una versión personalizada de Apache Tomcat (instalación manual del servicio Tomcat), no se admite la actualización de ESET PROTECT Web Console con el instalador todo en uno ni con la tarea de actualización de componentes.

Antes de actualizar

- Apache Tomcat requiere Java/OpenJDK de 64 bits. Si tiene instaladas en su sistema varias versiones de Java, le recomendamos que desinstale las versiones de Java anteriores y mantenga únicamente la versión de Java compatible.

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

- Compruebe qué versión de Apache Tomcat se está utilizando actualmente.

  a.Diríjase a la carpeta de instalación de Apache Tomcat:
  C:\Program Files\Apache Software Foundation\[Tomcat carpeta]

  b.Abra el archivo RELEASE-NOTES en un editor de texto y consulte el número de versión (por ejemplo, 9.0.34).

  c.Si hay una versión compatible más reciente disponible, realice la actualización.

Procedimientos de actualización

1. Detenga el servicio Apache Tomcat: Diríjase a **Inicio** > **Servicios** > haga clic con el botón derecho del ratón en el servicio Apache Tomcat y seleccione **Detener**.

Cierre *Tomcat7w.exe* si se está ejecutando en la bandeja del sistema.

2. Realice una copia de seguridad de los siguientes archivos:

   C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\.keystore
   C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\conf\server.xml
   C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties

Si utiliza un almacén de certificados SSL personalizado en la carpeta *Tomcat*, realice también una copia de

seguridad de ese certificado.

3. Desinstale la versión actual de Apache Tomcat.

4. Elimine la siguiente carpeta si aún está presente en el sistema:

C:\Program Files\Apache Software Foundation\[Tomcat carpeta]

5. Descargue la versión compatible más reciente del archivo del instalador de Apache Tomcat (instalador del servicio de Windows de 32/64 bits) `apache-tomcat-[versión].exe` de https://tomcat.apache.org.

6. Instale la versión más reciente de Apache Tomcat que ha descargado:

- Si tiene más versiones de Java instaladas, seleccione la ruta de acceso a la versión más reciente de Java durante la instalación.

- Una vez completada la instalación, desmarque la casilla de verificación situada junto a **Ejecutar Apache Tomcat**.

7. Restaure *.keystore*, *server.xml* y los certificados personalizados en sus ubicaciones originales.

8. Abra el archivo *server.xml* y asegúrese de que la ruta de acceso *keystoreFile* sea correcta (actualice la ruta de acceso si ha actualizado a una versión principal de Apache Tomcat más reciente):

keystoreFile="C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\.keystore"

9. Asegúrese de que la conexión HTTPS para Apache Tomcat de ESET PROTECT Web Console esté correctamente configurada.

10. Implemente ESET PROTECT Web Console (Instalación de Web Console: Windows).

11. Restaure *EraWebServerConfig.properties* a su ubicación original.

12. Ejecute Apache Tomcat y establezca una VM Java correcta:

a.Vaya a la carpeta *C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\bin* y ejecute *Tomcat9w.exe*.

b.En la pestaña **General**, establezca el **Tipo de inicio** en **Automático** y pulse **Iniciar**.

c.Haga clic en la ficha **Java**, desmarque la opción **Utilizar valores predeterminados** y asegúrese de que **Máquina virtual de Java** incluya la ruta de acceso al archivo *jvm.dll* (consulte las instrucciones ilustradas de la Base de conocimiento) y, a continuación, haga clic en **Aceptar**.

13. Conéctese a ESET PROTECT Web Console y asegúrese de que Web Console se carga correctamente.

> Consulte también la configuración de Web Console adicional para soluciones empresariales o sistemas de bajo rendimiento.

Resolución de problemas

- Si no es capaz de configurar correctamente una conexión HTTPS para Apache Tomcat, puede omitir este paso y utilizar una conexión HTTP de forma temporal.

- Si se produce un error al actualizar Apache Tomcat, instale la versión original y aplique la configuración desde el paso 2.

- La actualización de Web Console y Apache Tomcat borra los archivos de la Ayuda sin conexión. Si usó la ayuda sin conexión con ESMC o una versión más antigua de ESET PROTECT, vuelva a crearla para ESET PROTECT 9.1 tras la actualización para asegurarse de que tiene la ayuda sin conexión más reciente que coincide con su versión de ESET PROTECT.

Actualizar Apache Tomcat (Linux)

Apache Tomcat es un componente obligatorio necesario para ejecutar ESET PROTECT Web Console.

Antes de actualizar

1. Ejecute el siguiente comando para ver la versión instalada de Apache Tomcat (en algunos casos, el nombre de la carpeta es `tomcat7` o `tomcat8`):

```
cd /usr/share/tomcat/bin && ./version.sh
```

2. Si hay una versión más reciente disponible:

   a.Asegúrese de que la versión más reciente es compatible.

   b.Realice una copia de seguridad del archivo de configuración de Tomcat */etc/tomcat7/server.xml*.

Procedimientos de actualización

1. Ejecute el siguiente comando para detener el servicio Apache Tomcat (en algunos casos, el nombre del servicio es `tomcat7`):

```
sudo systemctl stop tomcat
```

2. Actualice Apache Tomcat y Java. Los ejemplos de nombres de paquetes que se indican a continuación pueden ser distintos de los paquetes del repositorio de su distribución Linux.

Distribución Linux	Comandos de terminal
Distribuciones Debian y Ubuntu	`sudo apt-get update` `sudo apt-get install openjdk-17-jdk tomcat9`
Distribuciones CentOS y Red Hat	`yum update` `yum install java-17-openjdk tomcat`
OpenSUSE	`zypper refresh` `sudo zypper install java-17-openjdk tomcat9`

3. Sustituya el archivo */etc/tomcat9/server.xml* por el archivo *server.xml* de su copia de seguridad.

4. Abra el archivo *server.xml* y asegúrese de que la ruta de acceso *keystoreFile* sea correcta.

5. Asegúrese de que la conexión HTTPS para Apache Tomcat esté correctamente configurada.

Consulte también la configuración de Web Console adicional para soluciones empresariales o sistemas de bajo rendimiento.

Después de actualizar Apache Tomcat a una versión principal posterior (por ejemplo, de Apache Tomcat versión 7.x a 9.x):
1.Implemente de nuevo la Consola web de ESET PROTECT (consulte Instalación de la Consola web de ESET PROTECT: Linux)
2.Vuelva a usar *%TOMCAT_HOME%/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties* para conservar los ajustes personalizados de la Consola web de ESET PROTECT.
La actualización de Web Console y Apache Tomcat borra los archivos de la Ayuda sin conexión. Si usó la ayuda sin conexión con ESMC o una versión más antigua de ESET PROTECT, vuelva a crearla para ESET PROTECT 9.1 tras la actualización para asegurarse de que tiene la ayuda sin conexión más reciente que coincide con su versión de ESET PROTECT.

Procedimientos de migración y reinstalación

Existen diferentes formas de migrar y reinstalar su ESET PROTECT Server y otros componentes de ESET PROTECT:

- Migrar o reinstalar ESET PROTECT 9 de un servidor a otro.

Para migrar de un ESET PROTECT Server a un nuevo equipo servidor, exporte/realice una copia de seguridad de todas las autoridades certificadoras y del certificado de ESET PROTECT Server. De lo contrario, ningún componente de ESET PROTECT podrá comunicarse con su nuevo ESET PROTECT Server.

- migración de la base de datos de ESET PROTECT
- Migración de MDM
- Cambie una dirección IP o un nombre de host en una instancia de ESET PROTECT Server.
- Migración desde ERA 5.x

Consulte procedimientos de actualización.

Migración de un servidor a otro

Existen diversos modos de migrar ESET PROTECT de un servidor a otro (estas situaciones pueden utilizarse durante la reinstalación de su ESET PROTECT Server):

- Instalación limpia: misma dirección IP: la nueva instalación no utiliza la base de datos anterior del antiguo ESET PROTECT Server y mantiene la dirección IP original.

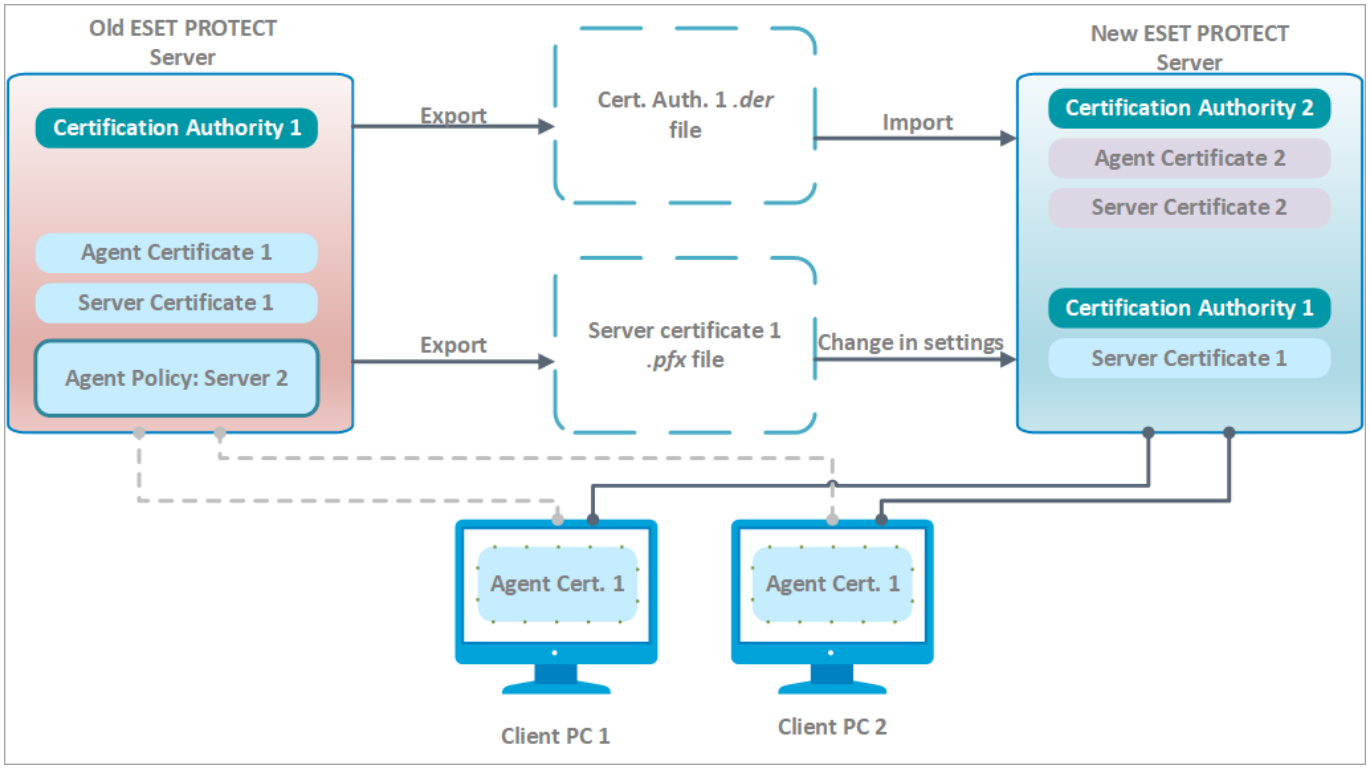
- Instalación limpia: direcciónes IP diferente (artículo de la Base de conocimiento): la nueva instalación no utiliza la base de datos anterior del antiguo ESET PROTECT Server y tiene una dirección IP diferente.

- Base de datos migrada: dirección IP igual/diferente: la migración de la base de datos solo puede realizarse entre dos tipos de base de datos similares (de MySQL a MySQL o de MS SQL a MS SQL) y dos versiones similares de ESET PROTECT.

Instalación limpia: misma dirección IP

El objetivo de este procedimiento es instalar una instancia completamente nueva de ESET PROTECT Server que no utilice la base de datos anterior. Este nuevo ESET PROTECT Server tendrá la **misma dirección IP** que el servidor anterior, pero no utilizará la base de datos del antiguo ESET PROTECT Server.

En las instrucciones indicadas a continuación se indica que el antiguo ESET PROTECT Servidor se está ejecutando con una Web Console accesible. Si no puede acceder a su antiguo ESET PROTECT Server:
1. Instale ESET PROTECT Server/MDM con el instalador de paquetes todo en uno (Windows) o elija otro método de instalación (instalación manual en Windows, Linux o dispositivo virtual).
2. Conéctese a ESET PROTECT Web Console.
3. Agregue ordenadores cliente a la infraestructura de ESET PROTECT e implemente ESET Management Agent de forma local o remota.



Ver la imagen más grande

❑ **En su ESET PROTECT Server actual (antiguo):**

Si administra dispositivos cifrados con ESET Full Disk Encryption, siga estos pasos para evitar la pérdida de datos de recuperación.
1.Antes de la migración: vaya a **Resumen del estado** > **Cifrado**. Aquí puede **exportar** los **datos de recuperación deESET Full Disk Encryption** actuales.
2.Después de la migración: **importe** los **datos de recuperación de ESET Full Disk Encryption** en la nueva consola de administración.
Si no puede realizar estos pasos, tendrá que descifrar los dispositivos administrados antes de la migración. Tras la migración, puede cifrar los dispositivos administrados desde ESET PROTECT Web Console.

1. Exporte un certificado de servidor del ESET PROTECT Server actual y guárdelo en el almacenamiento externo.

   • Exporte todos los certificados de autoridades certificadoras de su ESET PROTECT Server y guarde cada certificado de la autoridad certificadora como un archivo *.der*.

   • Exporte el certificado del servidor de su ESET PROTECT Server en un archivo *.pfx*. El archivo *.pfx* exportado también incluirá una clave privada.

2. Detenga el servicio ESET PROTECT Server.

3. Apague su equipo ESET PROTECT Server.

No desinstale ni quite aún su antiguo ESET PROTECT Server.

❑ **En su nuevo ESET PROTECT Server:**

Para usar un nuevo ESET PROTECT Server con la misma dirección IP, asegúrese de que la configuración de red de su nuevo ESET PROTECT Server (**dirección IP, FQDN, nombre del ordenador, registro SRV de DNS**) coincida con la de su antiguo ESET PROTECT Server.

1. Instale ESET PROTECT Server/MDM con el instalador de paquetes todo en uno (Windows) o elija otro método de instalación (instalación manual en Windows, Linux o dispositivo virtual).

2. Conéctese a ESET PROTECT Web Console.

3. Importe todas las autoridades certificadoras que haya exportado de su antiguo ESET PROTECT Server. Para ello, siga las instrucciones sobre cómo importar una clave pública.

4. Cambie el certificado de ESET PROTECT Server en la **Más** > Configuración para utilizar el certificado del servidor de su antiguo ESET PROTECT Server.

5. Importe todas las licencias de ESET necesarias en ESET PROTECT.

6. Reinicie el servicio ESET PROTECT Server, consulte nuestro artículo de la Base de conocimiento para obtener más información.

Tras uno o dos intervalos de conexión del agente, los ordenadores cliente deben conectarse a su nuevo ESET PROTECT Server utilizando el certificado de ESET Management Agent original, que está siendo autenticado por la autoridad certificadora importada del antiguo ESET PROTECT Server. Si los clientes no se conectan, consulte Problemas después de la actualización o migración de ESET PROTECT Server.

cuando añada nuevos ordenadores cliente, utilice una nueva autoridad certificadora para firmar los certificados del agente. Esto se debe a que una autoridad certificadora importada no puede utilizarse para firmar nuevos certificados de igual, sino que solo puede autenticar instancias de ESET Management Agent de ordenadores cliente que se hayan migrado.

❑ **Desinstalación del antiguo ESET PROTECT Server/MDM:**

Cuando todo se esté ejecutando correctamente en su nuevo ESET PROTECT Server, quite su antiguo ESET PROTECT Server/MDM con cuidado utilizando nuestras instrucciones paso a paso.

Base de datos migrada: dirección IP igual/diferente

El objetivo de este procedimiento es instalar una instancia completamente nueva de ESET PROTECT Server y **mantener su base de datos de ESET PROTECT existente**, incluidos los ordenadores cliente actuales. El nuevo ESET PROTECT Server tendrá **la misma dirección IP o una dirección IP diferente**, y la base de datos del antiguo ESET PROTECT Server se importará en el nuevo equipo servidor antes de la instalación.

- La migración de bases de datos solo es compatible entre tipos de base de datos idénticos (de MySQL a MySQL o de MS SQL a MS SQL).
- cuando migre una base de datos, deberá realizar la migración entre instancias de la misma versión de ESET PROTECT. Consulte nuestro artículo de la Base de conocimiento para obtener instrucciones sobre cómo conocer las versiones de sus componentes de ESET PROTECT. Una vez realizada la migración de la base de datos, podrá realizar una actualización, si fuera necesario, para obtener la última versión de ESET PROTECT.

❑ **En su ESET PROTECT Server actual (antiguo):**

Recomendamos la migración a una dirección IP diferente solo para usuarios avanzados. Si su nuevo ESET PROTECT Server tiene una **dirección IP diferente**, realice estos pasos adicionales en su ESET PROTECT Server actual (antiguo):
a)Genere un nuevo certificado de ESET PROTECT Server con información de conexión para el nuevo ESET PROTECT Server. Deje el valor predeterminado (un asterisco) en el campo **Host** para permitir la distribución de este certificado sin asociación a un nombre DNS o dirección IP específicos.
b)Cree una política para definir una nueva dirección IP de ESET PROTECT Server y asígnela a todos los ordenadores. Espere a que la política se distribuya a todos los ordenadores cliente (los ordenadores dejarán de informar cuando reciban la nueva información del servidor).

1. Detenga el servicio ESET PROTECT Server.

2. Exporte o realice una copia de seguridad de la base de datos de ESET PROTECT.

3. Apague el equipo ESET PROTECT Server actual (opcional si el nuevo servidor tiene una dirección IP diferente).

No desinstale ni quite aún su antiguo ESET PROTECT Server.

❑ **En su nuevo ESET PROTECT Server:**

Para usar un nuevo ESET PROTECT Server con la misma dirección IP, asegúrese de que la configuración de red de su nuevo ESET PROTECT Server (**dirección IP, FQDN, nombre del ordenador, registro SRV de DNS**) coincida con la de su antiguo ESET PROTECT Server.

1. Instale o inicie una base de datos de ESET PROTECT compatible.

2. Importe o restaure la base de datos de ESET PROTECT desde su antiguo ESET PROTECT Server.

3. Instale ESET PROTECT Server/MDM con el instalador de paquetes todo en uno (Windows) o elija otro método de instalación (instalación manual en Windows, Linux o dispositivo virtual). Especifique la configuración de la conexión de la base de datos durante la instalación de ESET PROTECT Server.

4. Conéctese a ESET PROTECT Web Console.

5. Diríjase a **Más** > **Configuración** > **Conexión**. Haga clic en **Cambiar certificado** > **Abrir lista de certificados** y seleccione el **Certificado del servidor** del antiguo ESET PROTECT Server y haga clic en **OK** dos veces.

6. Reinicie el servicio ESET PROTECT Server.

7. Inicie sesión en ESET PROTECT Web Console y haga clic en **Ordenadores**.

Después de uno o dos intervalos de conexión del agente, los ordenadores cliente deben conectarse a su nuevo ESET PROTECT Server utilizando el certificado de ESET Management Agent original. Si los clientes no se conectan, consulte Problemas después de la actualización o migración de ESET PROTECT Server.

❑ **Desinstalación del antiguo ESET PROTECT Server/MDM:**

Cuando todo se esté ejecutando correctamente en su nuevo ESET PROTECT Server, quite su antiguo ESET PROTECT Server/MDM con cuidado utilizando nuestras instrucciones paso a paso.

migración de la base de datos de ESET PROTECT

Estas instrucciones se aplican a la migración de la base de datos de ESET PROTECT entre instancias de SQL Server distintas (esto también se aplica al migrar a una versión de SQL Server distinta o al migrar a una instancia de SQL Server alojada en un equipo distinto):

- Proceso de migración de MS SQL Server
- Proceso de migración de MySQL Server

Proceso de migración de MS SQL Server

Este proceso de migración es igual para **Microsof SQL Server** y para **Microsoft SQL Server Express**.

Si desea obtener más información, consulte el siguiente artículo de la Knowledge Base de Microsoft: https://msdn.microsoft.com/en-us/library/ms189624.aspx.

Requisitos previos

- Las instancias de SQL Server de origen y de destino deben estar instaladas. Pueden estar alojadas en máquinas distintas.
- La instancia de SQL Server de destino debe tener, como mínimo, la misma versión que la instancia de origen. **No es posible realizar una reversión a una versión anterior.**
- **SQL Server Management Studio** debe estar instalado. Si las instancias de SQL Server se encuentran en máquinas distintas, debe estar instalado en ambas.

Migración con SQL Server Management Studio

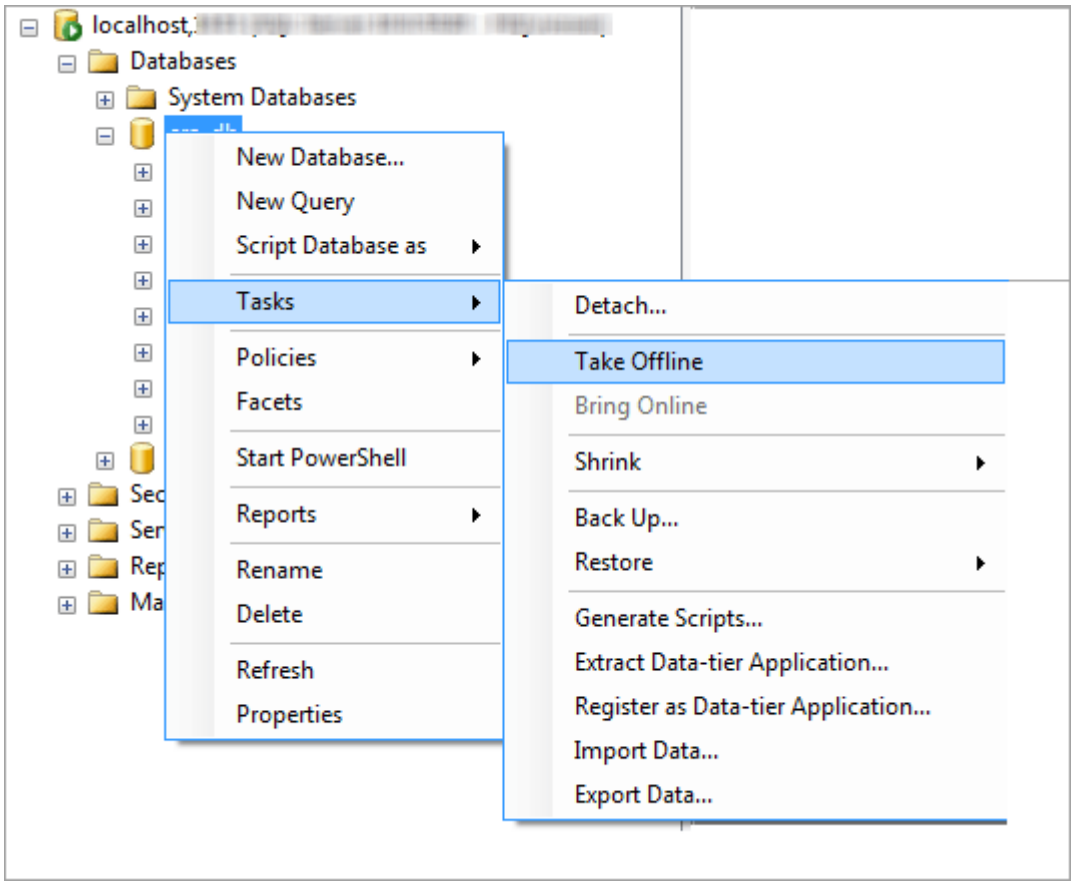
1. Detenga el servicio ESET PROTECT Server (o el servicio ESMC Server) o el servicio ESET PROTECT MDM.

⚠ No inicie ESET PROTECT Server o ESET PROTECT MDM antes de completar todos los pasos siguientes.

2. Inicie sesión en la instancia de SQL Server de origen desde SQL Server Management Studio.

3. Cree una copia de seguridad de la base de datos completa de la base de datos que va a migrar. Le recomendamos que especifique un nuevo nombre de conjunto de copia de seguridad. De lo contrario, si el conjunto de copia de seguridad ya se ha utilizado, la nueva copia de seguridad se anexará y el archivo de copia de seguridad resultante será innecesariamente grande.

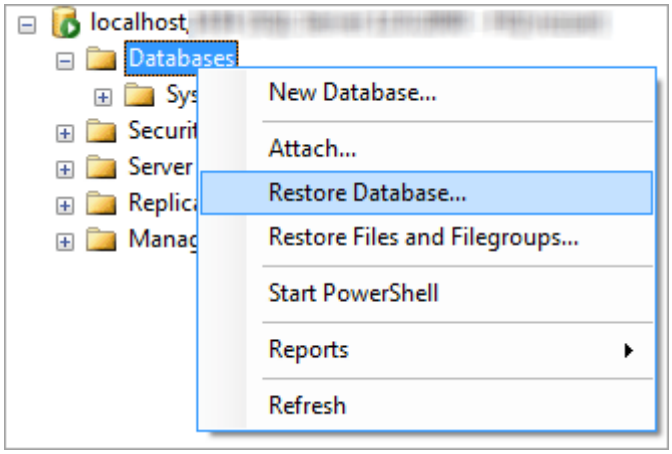
4. Establezca la base de datos de origen sin conexión; seleccione **Tareas** > **Establecer sin conexión**.



5. Copie el archivo de copia de seguridad (*.bak*) que ha creado en el paso tres en una ubicación a la que pueda acceder la instancia de SQL Server de destino. Puede que tenga que editar los derechos de acceso del archivo de copia de seguridad de la base de datos.

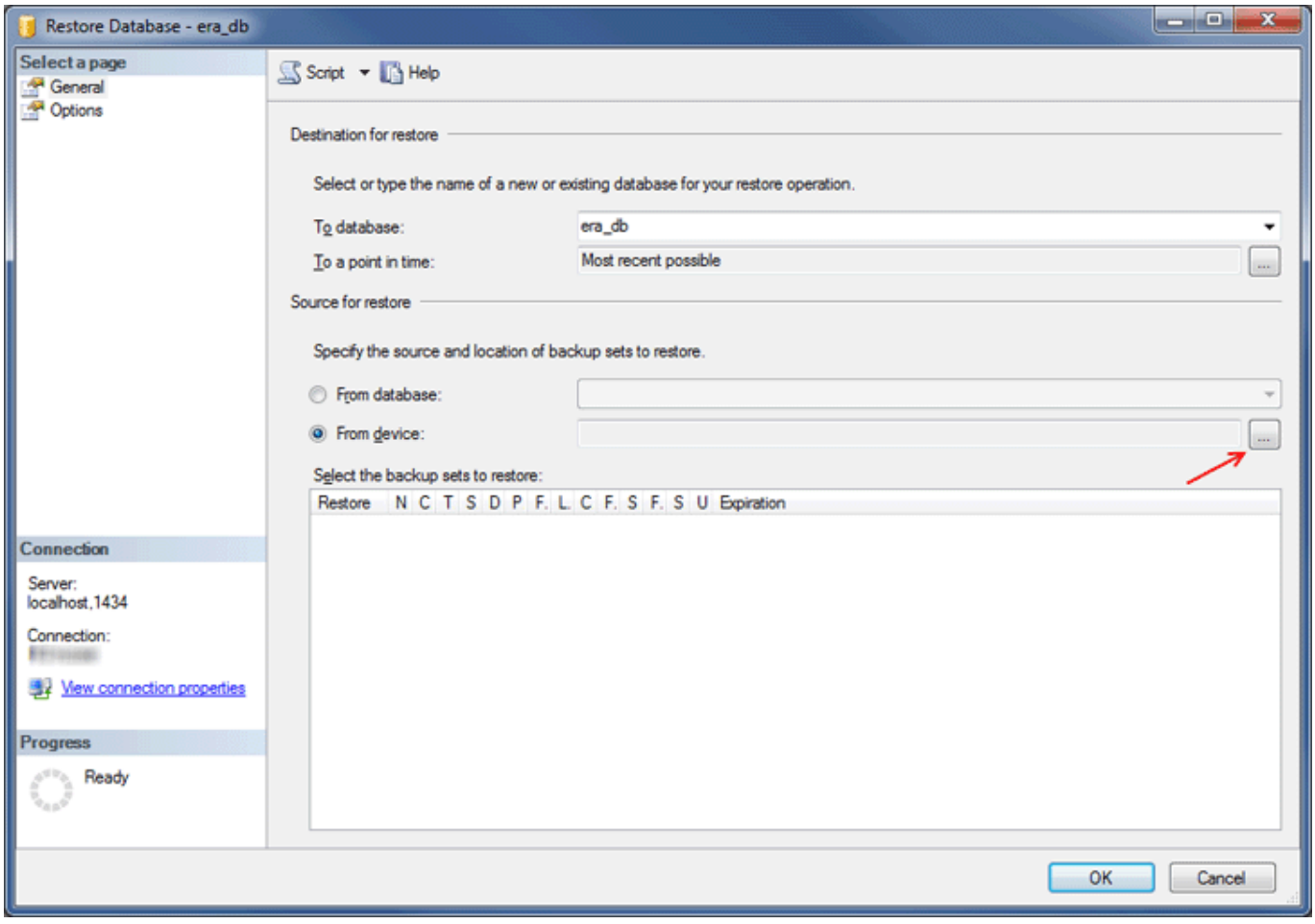
6. Inicie sesión en la instancia de SQL Server de destino desde SQL Server Management Studio.

7. Restaure su base de datos en la instancia de SQL Server de destino.



8. Escriba el nombre de la nueva base de datos en el campo **A base de datos**. Si lo prefiere, puede usar el mismo nombre que tenía su antigua base de datos.

9. Elija la opción Desde dispositivo en **Especifique el origen y la ubicación de los conjuntos de copia de seguridad que desea restaurar** y, a continuación, haga clic en … .



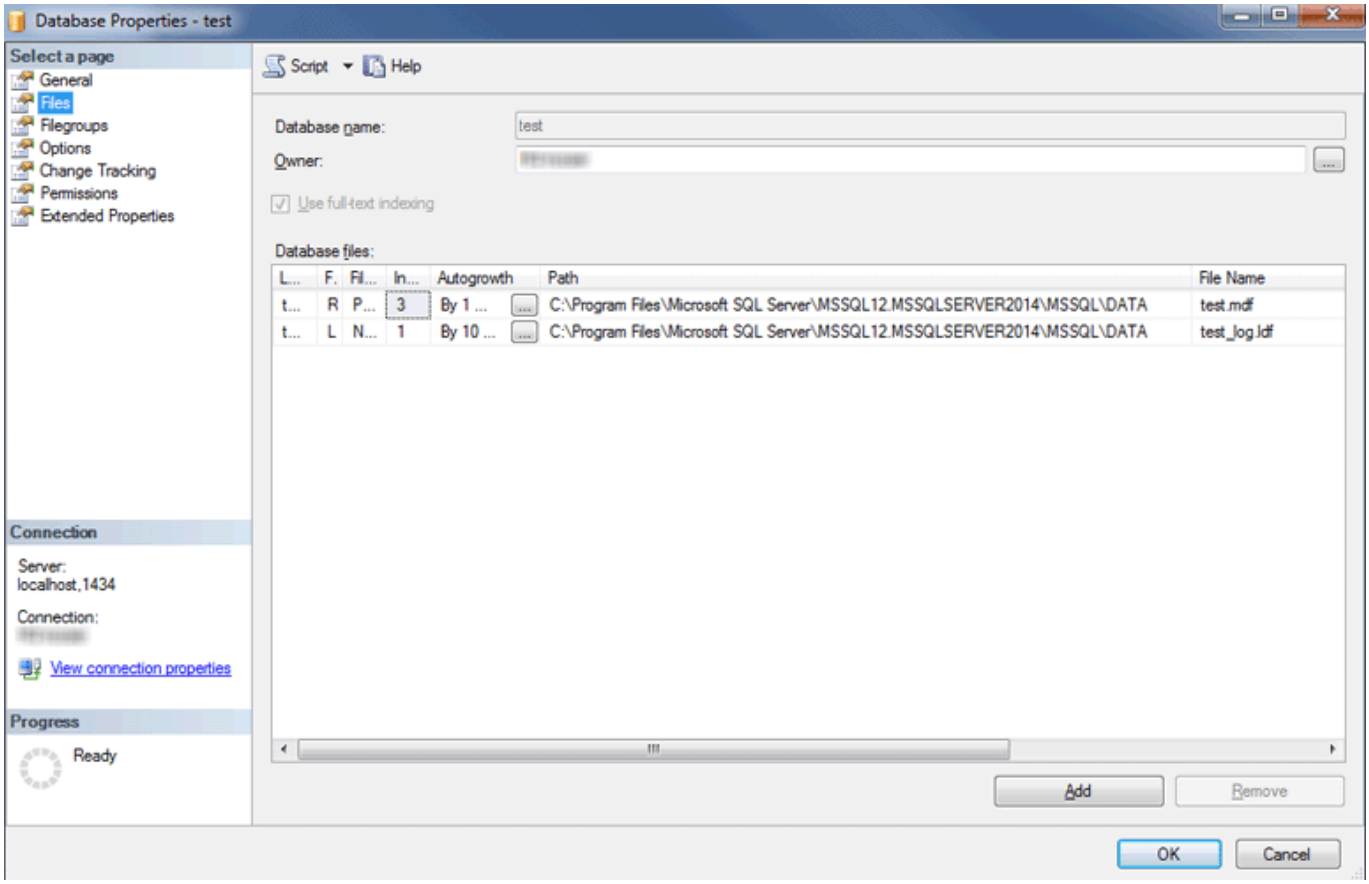
10. Haga clic en **Agregar, diríjase a su archivo de copia de seguridad y ábralo**.

11. Seleccione la copia de seguridad más reciente posible que desee restaurar (el conjunto de copia de seguridad puede contener varias copias de seguridad).

12. Haga clic en la página **Opciones** del asistente de restauración. Si lo desea, seleccione **Sobrescribir base de datos existente** y asegúrese de que las ubicaciones de restauración de la base de datos (*.mdf*) y del archivo de registro (*.ldf*) son correctas. Mantener los valores predeterminados sin cambios utilizará las rutas de la

instancia de SQL Server de origen, por lo que deberá revisar estos valores.

- Si no está seguro de dónde están guardados los archivos de la base de datos en la instancia de SQL Server de destino, haga clic con el botón derecho en una base de datos existente, seleccione **propiedades** y haga clic en la pestaña **Archivos**. El directorio en el que la base de datos está almacenada se muestra en la columna **Ruta** de la tabla que aparece a continuación.

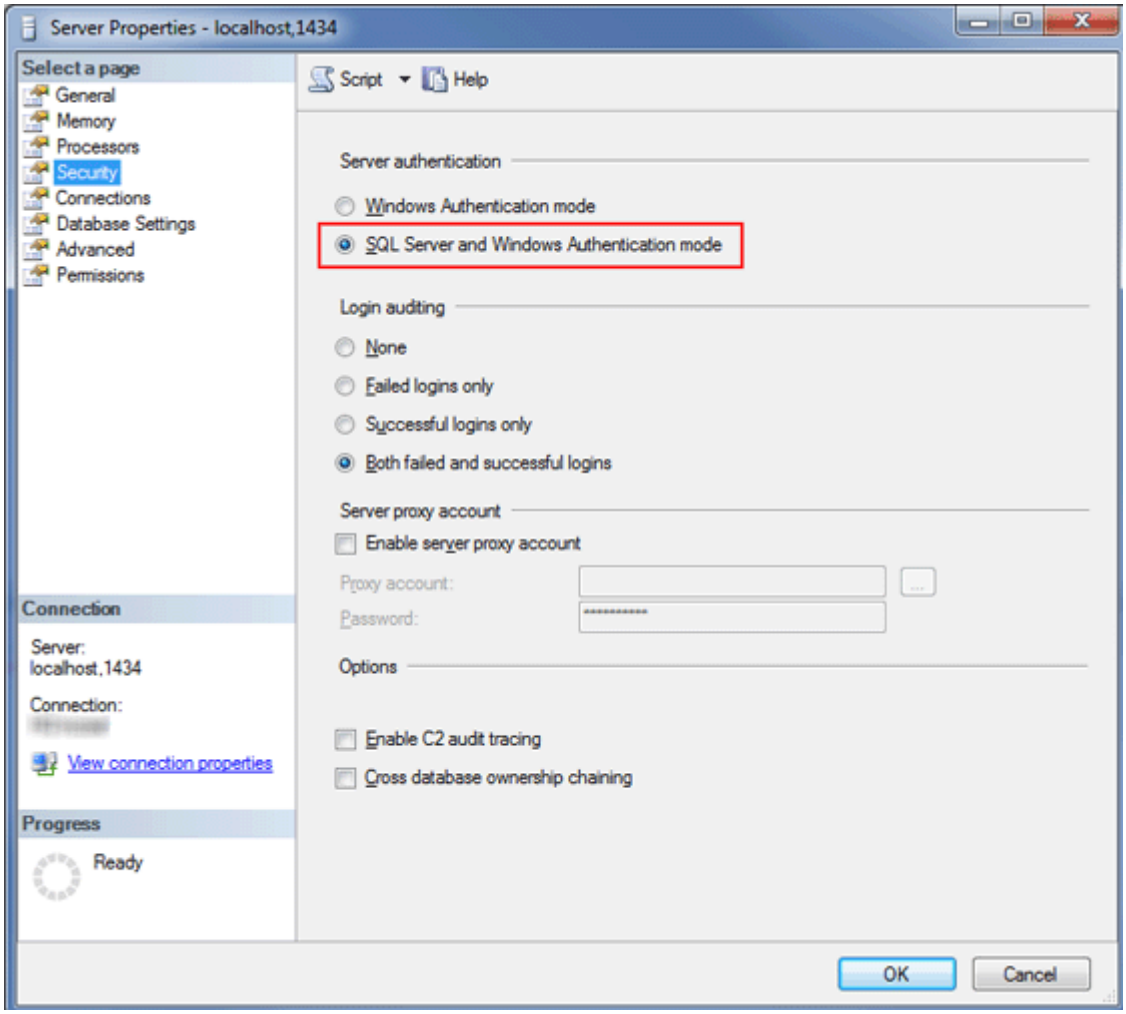


13. Haga clic en **Aceptar** en la ventana del asistente de restauración.

14. Haga clic con el botón derecho del ratón en la base de datos **era_db**, seleccione **Nueva consulta** y ejecute la siguiente consulta para eliminar el contenido de la tabla **tbl_authentication_certificate** (de lo contrario, los agentes podrían no conectarse con el nuevo servidor):

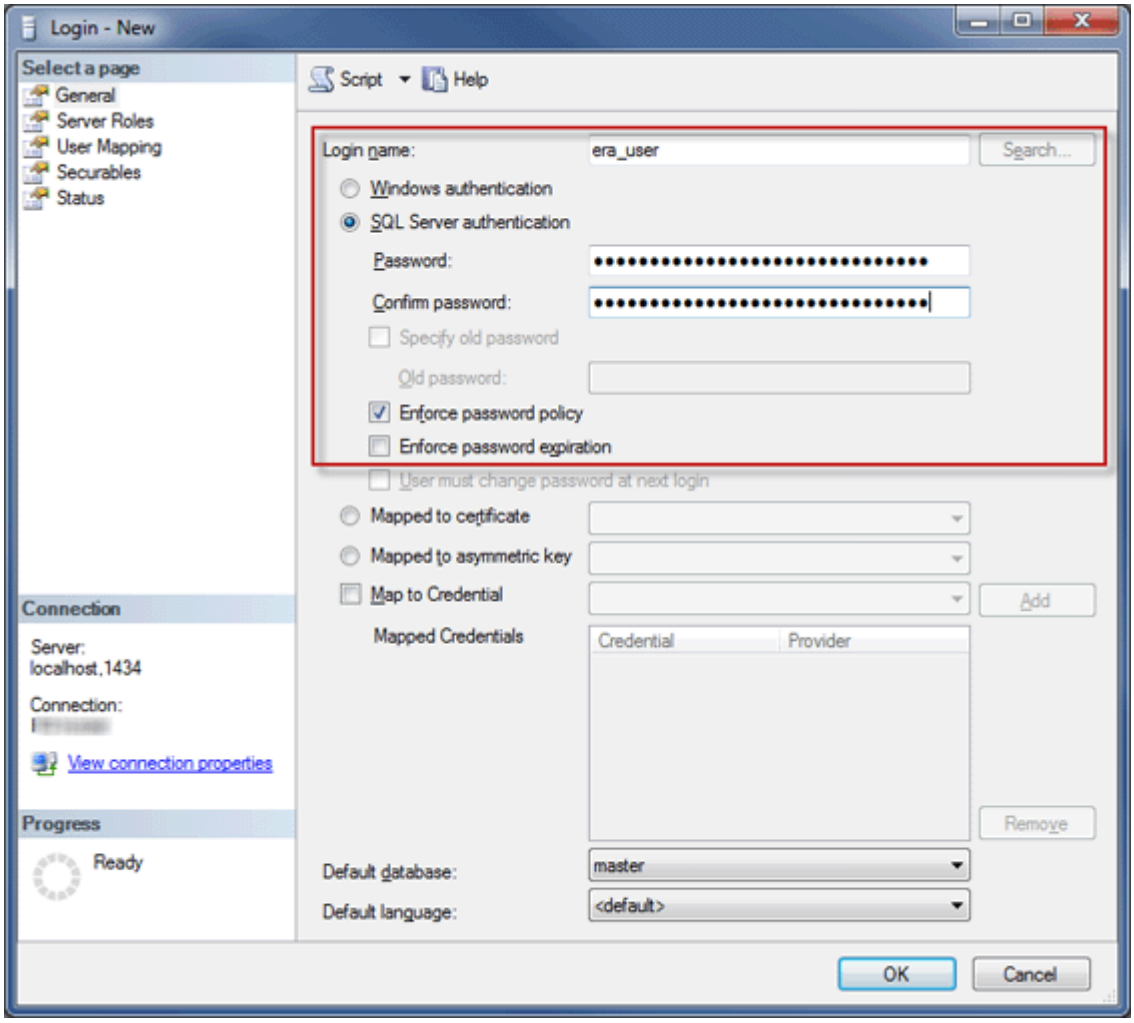
```
delete from era_db.dbo.tbl_authentication_certificate where certificate_id = 1;
```

15. Asegúrese de que el nuevo servidor de la base de datos tenga activada la opción **Autenticación SQL Server**. Haga clic con el botón derecho en el servidor y, a continuación, en **Propiedades**. Diríjase a **Seguridad** y asegúrese de que esté seleccionado el **modo Autenticación SQL Server y Windows**.

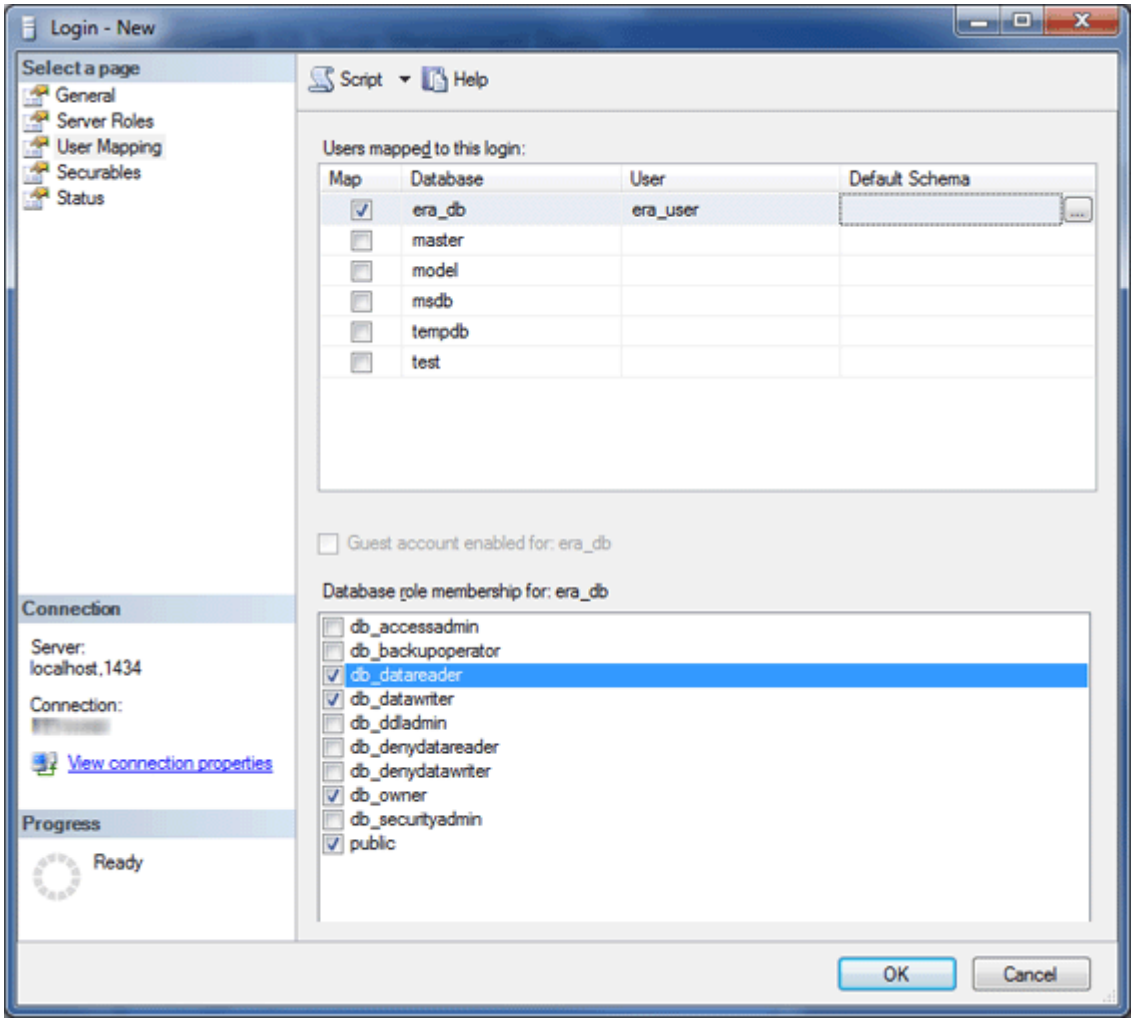


16. Cree un nuevo inicio de sesión en SQL Server (para ESET PROTECT Server/ESET PROTECT MDM) en la instancia de SQL Server de destino con **Autenticación SQL Server** y asigne el inicio de sesión a un usuario de la base de datos restaurada.

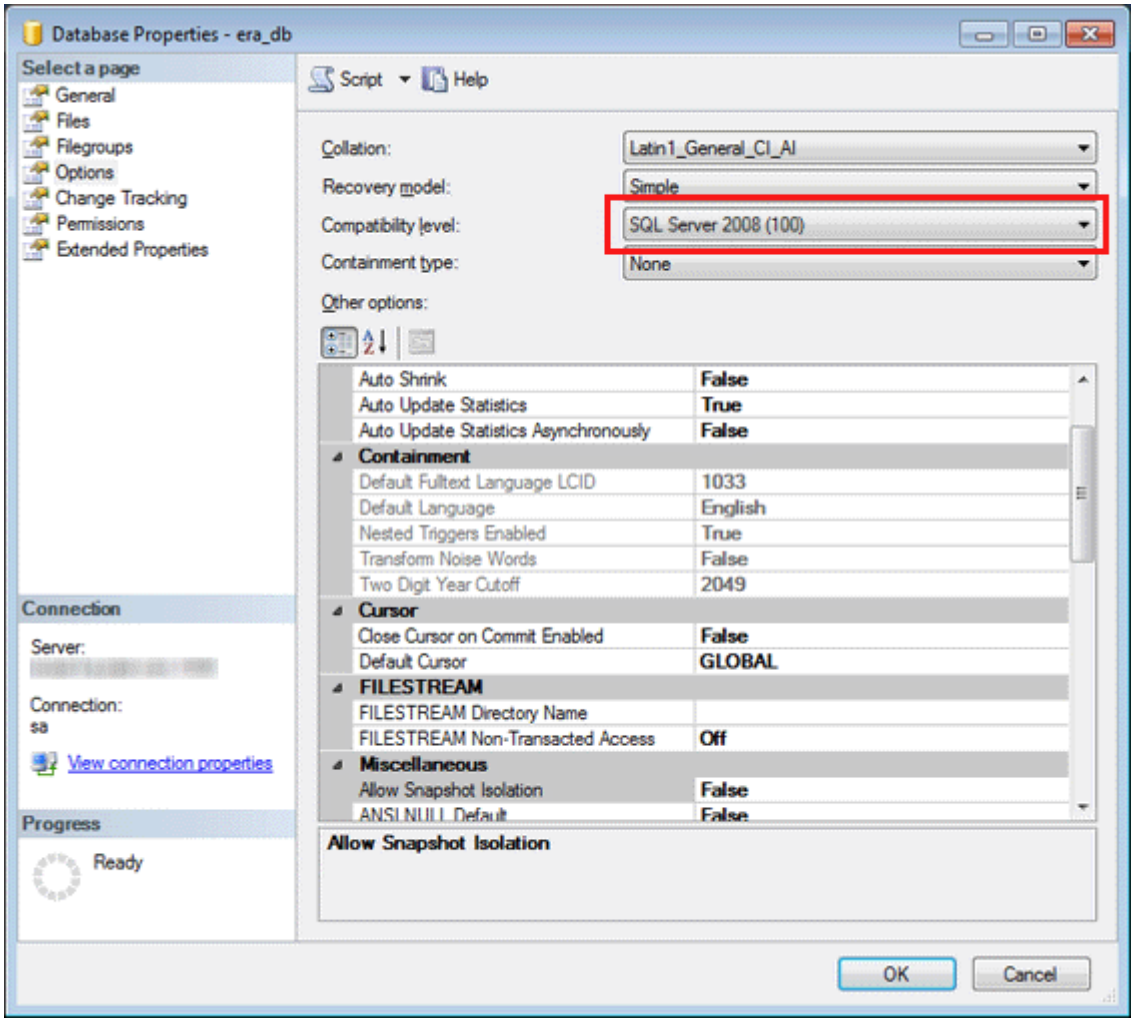
- No aplique la función de caducidad de contraseña.
- Caracteres recomendados para nombres de usuario:
  - Letras ASCII en minúscula, números y guion bajo "_"
- Caracteres recomendados para contraseñas:
  - Caracteres ASCII ÚNICAMENTE, incluidas letras ASCII en minúscula y en mayúscula, números, espacios, caracteres especiales
- No utilice caracteres que no sean ASCII, como corchetes {} y @
- Tenga en cuenta que, si no sigue las recomendaciones relativas a caracteres anteriormente indicadas, puede tener problemas de conectividad con la base de datos o tendrá que aplicar carácter de escape a los caracteres especiales en pasos posteriores, durante la modificación de la cadena de conexión de la base de datos. Las reglas referentes a los caracteres de escape no están incluidas en este documento.



17. Asigne el inicio de sesión a un usuario de la base de datos de destino. En la pestaña de **asignaciones de usuarios**, asegúrese de que el usuario de la base de datos tenga las siguientes funciones: **db_datareader**, **db_datawriter**, **db_owner**.

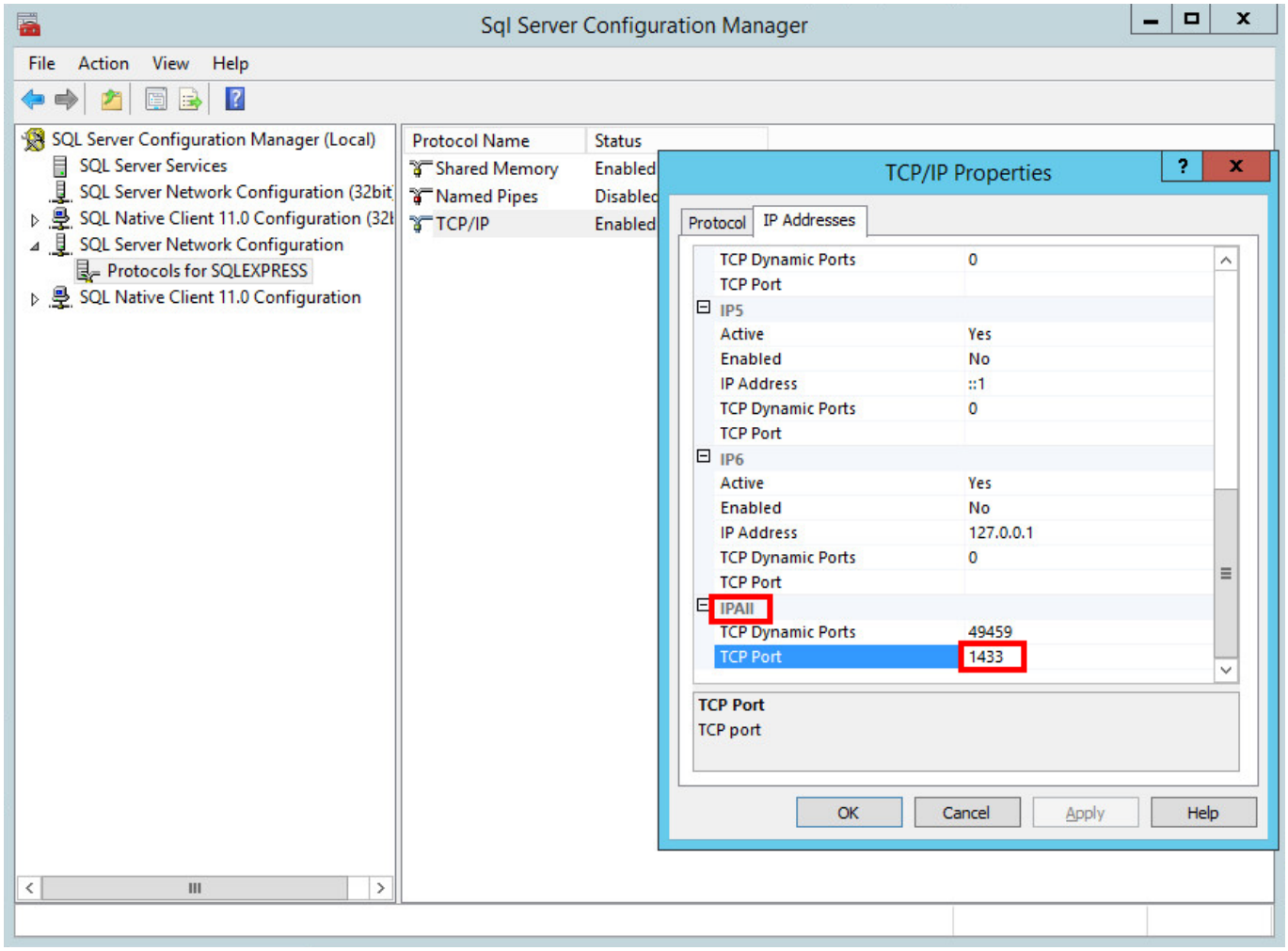


18. Para activar las funciones del servidor de la base de datos más reciente, cambie la opción **Nivel de compatibilidad** de la base de datos restaurada a la más reciente. Haga clic con el botón derecho en la nueva base de datos, y abra las **Propiedades** de la base de datos.



> SQL Server Management Studio no puede definir los niveles de compatibilidad posteriores a los de la versión en uso. Por ejemplo, SQL Server Management Studio 2014 no puede definir el nivel de compatibilidad de SQL Server 2019.

19. Asegúrese de que el protocolo de conexión **TCP/IP** esté **activado** para "db_instance_name" (por ejemplo, SQLEXPRESS o MSSQLSERVER) y de que el **puerto** TCP/IP esté establecido en **1433**. Para ello, abra el **Administrador de configuración de SQL Server**, diríjase a **Configuración de red de SQL Server** > **Protocolos para db_instance_name**, haga clic con el botón derecho del ratón en **TCP/IP** y seleccione **Activado**. Haga doble clic en **TCP/IP**, cambie a la pestaña **Protocolos**, desplácese hacia abajo **IPAll** y, en el campo **Puerto TCP**, escriba 1433. Haga clic en **Aceptar** y reinicie el servicio **SQL Server**.



20. Conecte ESET PROTECT Server o MDM a la base de datos.

Proceso de migración de MySQL Server

Requisitos previos

• Las instancias de SQL Server de origen y de destino deben estar instaladas. Pueden estar alojadas en máquinas distintas.

• Las herramientas de MySQL deben estar disponibles al menos en uno de los ordenadores (cliente de mysql y `mysqldump`).

Enlaces útiles

- https://dev.mysql.com/doc/refman/5.6/en/copying-databases.html
- https://dev.mysql.com/doc/refman/5.6/en/mysqldump.html
- https://dev.mysql.com/doc/refman/5.6/en/mysql.html

Proceso de migración

En los comandos, archivos de configuración o instrucciones SQL expuestos a continuación, cambie siempre:
- **SRCHOST** por la dirección del servidor de la base de datos de origen
- **SRCROOTLOGIN** por el inicio de sesión del usuario root del servidor MySQL de origen
- **SRCDBNAME** por el nombre de la base de datos ESET PROTECT de origen de la que se desea realizar la copia de seguridad
- **BACKUPFILE** por la ruta del archivo en la que se almacenará la copia de seguridad
- **TARGETROOTLOGIN** por el inicio de sesión del usuario root del servidor MySQL de destino
- **TARGETHOST** por la dirección del servidor de la base de datos de destino
- **TARGETDBNAME** por el nombre de la base de datos ESET PROTECT de destino (tras la migración)
- **TARGETLOGIN** por el nombre de inicio de sesión del nuevo usuario de la base de datos de ESET PROTECT en el servidor de bases de datos de destino
- **TARGETPASSWD** por la contraseña del nuevo usuario de la base de datos de ESET PROTECT en el servidor de bases de datos de destino

No es necesario ejecutar las instrucciones SQL indicadas a continuación desde la línea de comandos. Si hay una interfaz gráfica de usuario disponible, puede usar una aplicación que ya conoce.

1. Detenga los servicios ESET PROTECT Server/MDM.

2. Utilice la opción Crear para crear una copia de seguridad completa de la base de datos de ESET PROTECT de origen (la base de datos que tiene previsto migrar):

```
mysqldump --host SRCHOST --disable-keys --extended-insert --routines -
u SRCROOTLOGIN -p SRCDBNAME > BACKUPFILE
```

3. Utilice la opción Preparar para preparar una base de datos vacía en el servidor MySQL de destino:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=CREATE DATABASE TARGETDBNAME /*!40100 DEFAULT CHARACTER SET utf8 */;"
```

en sistemas Linux, use el apóstrofe ' en lugar de las comillas ".

4. Utilice la opción Restaurar para restaurar la base de datos del servidor MySQL de destino en la base de datos vacía que ha preparado anteriormente:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p TARGETDBNAME < BACKUPFILE
```

5. Utilice la opción Crear para crear un usuario de base de datos de ESET PROTECT en el servidor MySQL de destino:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=CREATE USER TARGETLOGIN@'%' IDENTIFIED BY 'TARGETPASSWD';"
```

Caracteres recomendados para **TARGETLOGIN:**

- Letras ASCII en minúscula, números y guion bajo "_"

Caracteres recomendados para **TARGETPASSWD:**

- Caracteres ASCII únicamente, incluidas letras ASCII en minúscula y en mayúscula, números, espacios y caracteres especiales
- No utilice caracteres que no sean ASCII, como corchetes {} y @

Tenga en cuenta que, si no sigue las recomendaciones relativas a caracteres anteriormente indicadas, puede tener problemas de conectividad con la base de datos o tendrá que aplicar carácter de escape a los caracteres especiales en pasos posteriores, durante la modificación de la cadena de conexión de la base de datos. Las reglas referentes a los caracteres de escape no están incluidas en este documento.

6. Utilice la opción Conceder para otorgar los derechos de acceso al usuario de la base de datos de ESET PROTECT en el servidor MySQL de destino:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=GRANT ALL ON TARGETDBNAME.* TO TARGETLOGIN;"
```

en sistemas Linux, use el apóstrofe ' en lugar de las comillas ".

7. Elimine el contenido de la tabla **tbl_authentication_certificate** (de lo contrario, los agentes podrían no conectarse con el nuevo servidor):

```
 mysql --host TARGETHOST -u root -p "--
execute=DELETE FROM era_db.tbl_authentication_certificate where certificate_id = 1;"
```

8. Conecte ESET PROTECT Server o MDM a la base de datos.

Conectar ESET PROTECT Server o MDM a una base de datos

Siga los pasos que se indican a continuación en el equipo en el que estén instalados ESET PROTECT Server o ESET PROTECT MDM para conectarlos a una base de datos.

1. Detenga el servicio de ESET PROTECT Server/MDM.
2. Busque *startupconfiguration.ini*
   - Windows:

Servidor:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configurati
on\startupconfiguration.ini
```

MDMCore:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\MDMCore\EraServerApplicationData\Configurat
ion\startupconfiguration.ini
```

- Linux:

Servidor:

/etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini

MDMCore:

/etc/opt/eset/RemoteAdministrator/MDMCore/startupconfiguration.ini

3. Cambie la cadena de conexión de la base de datos en ESET PROTECT Server/MDM *startupconfiguration.ini*
    - Defina la dirección y el puerto del nuevo servidor de la base de datos.
    - Defina el nuevo nombre de usuario y la contraseña de ESET PROTECT en la cadena de conexión.

El resultado final debe ser similar al siguiente:

- MS SQL:

```
DatabaseType=MSSQLOdbc

DatabaseConnectionString=Driver=SQL Server;Server=TARGETHOST,1433;Uid=TARGETLOGIN;Pw
d={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

- MySQL:

```
DatabaseType=MySqlOdbc
DatabaseConnectionString=Driver=MySQL ODBC 5.3 Unicode Driver;Server=TARGETHOST;Port
=3306;User=TARGETLOGIN;
Password={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

En la configuración anterior, sustituya siempre:
- **TARGETHOST** por la dirección del servidor de la base de datos de destino
- **TARGETDBNAME** por el nombre de la base de datos ESET PROTECT de destino (tras la migración)
- **TARGETLOGIN** por el nombre de inicio de sesión del nuevo usuario de la base de datos de ESET PROTECT en el servidor de bases de datos de destino
- **TARGETPASSWD** por la contraseña del nuevo usuario de la base de datos de ESET PROTECT en el servidor de bases de datos de destino

4. Inicie ESET PROTECT Server o ESET PROTECT MDM y asegúrese de que el servicio se ejecute correctamente.

Migración de MDM

Este procedimiento es migrar una instancia existente de ESET PROTECT MDM y **mantener su base de datos de ESET PROTECT MDM existente**, incluidos los dispositivos móviles inscritos. El ESET PROTECT MDM migrado tendrá **la misma dirección IP/nombre de host** que el antiguo ESET PROTECT MDM, y la base de datos del antiguo ESET PROTECT MDM se importará al nuevo host MDM antes de realizar la instalación.

- La migración de bases de datos solo es compatible entre tipos de base de datos idénticos (de MySQL a MySQL o de MS SQL a MS SQL).
- cuando migre una base de datos, deberá realizar la migración entre instancias de la misma versión de ESET PROTECT. Consulte nuestro artículo de la Base de conocimiento para obtener instrucciones sobre cómo conocer las versiones de sus componentes de ESET PROTECT. Una vez realizada la migración de la base de datos, podrá realizar una actualización, si fuera necesario, para obtener la última versión de ESET PROTECT.

❑ **En su ESET PROTECT MDM Server actual (antiguo):**

1. Cree una copia de seguridad de la configuración de MDM.

   a)En **Ordenadores**, haga clic en el servidor de MDM y seleccione **Detalles**.

   b)Haga clic en **Configuración** > **Solicitar configuración**. Es posible que deba esperar algún tiempo (en función del intervalo de conexión del agente) hasta que se cree la configuración solicitada.

   c)Haga clic en **ESET PROTECT Mobile Device Connector** y seleccione **Abrir configuración**.

   d)Exporte los siguientes elementos de la configuración al almacenamiento externo:

   - El nombre de host exacto del MDM Server.
   - Certificados de iguales: el archivo *.pfx* exportado tendrá la clave privada incluida.

   Si está ejecutando el servidor de MDM de ESET PROTECT en Linux, tendrá que exportar el certificado HTTPS de la política de configuración de MDM:
   I.Haga clic en **Ver** junto a **Certificado HTTPS**.
   II.Haga clic en **Descargar** y descargue el certificado HTTPS en formato PFX.

   e)Exporte también los siguientes certificados y tokens, si están presentes:

   - El certificado de firma de perfil de inscripción.
   - Un certificado APNS (exportar el certificado APNS y la clave privada APNS).
   - Token de autorización del Programa de inscripción de dispositivos (DEP) de Apple.

2. Detenga el servicio de ESET PROTECT MDM.

3. Exporte la base de datos de ESET PROTECT MDM o realice una copia de seguridad de dicha base de datos.

4. Apague la máquina de ESET PROTECT MDM actual.

No desinstale ni quite aún el antiguo ESET PROTECT MDM.

❑ **En su nuevo ESET PROTECT MDM Server:**

Asegúrese de que la configuración de red de su nuevo ESET PROTECT MDM Server (el nombre del host que exportó de la configuración de su MDM Server "antiguo") coincida con la de su antiguo ESET PROTECT MDM.

1. Instale/inicie una base de datos de ESET PROTECT MDM compatible.

2. Importe/restaure la base de datos de ESET PROTECT MDM desde su ESET PROTECT MDM anterior.

3. Instale ESET PROTECT Server/MDM con el instalador de paquetes todo en uno (Windows) o elija otro método de instalación (instalación manual en Windows, Linux o dispositivo virtual). Especifique la configuración de la conexión de la base de datos durante la instalación de ESET PROTECT MDM.

Al instalar ESET PROTECT MDM en Linux, utilice el certificado HTTPS de la copia de seguridad.

4. Conéctese a ESET PROTECT Web Console.

5. Reinicie el servicio ESET PROTECT MDM.

Los dispositivos móviles administrados deben ahora conectarse al nuevo ESET PROTECT MDM Server con su certificado original.

❑ **Desinstalación del antiguo ESET PROTECT Server/MDM:**

Cuando todo se esté ejecutando correctamente en su nuevo ESET PROTECT Server, quite su antiguo ESET PROTECT Server/MDM con cuidado utilizando nuestras instrucciones paso a paso.

Cambio de la dirección IP o el nombre de host de ESET PROTECT Server tras la migración

Para cambiar una dirección IP o un nombre de host en ESET PROTECT Server, siga los pasos que se indican a continuación:

1. Si el certificado de ESET PROTECT Server contiene una dirección IP o un nombre de host específicos, cree un nuevo certificado del servidor e incluya la nueva dirección IP o el nuevo nombre de host a los que desea cambiar. Sin embargo, si tiene un comodín * en el campo Host del certificado del servidor, **avance al paso 2**. De lo contrario, cree el nuevo certificado del servidor añadiendo la nueva dirección IP y el nuevo nombre de host separados con una coma e incluya la dirección IP y el nombre de host anteriores.

2. Firme el nuevo certificado del servidor utilizando la autoridad certificadora de ESET PROTECT Server.

3. Cree una política cambiando las conexiones del cliente a la nueva dirección IP o al nuevo nombre de host (preferiblemente a la nueva dirección IP), pero incluya una segunda conexión (alternativa) a la dirección IP o al nombre de host anteriores para ofrecer a ESET Management Agent la posibilidad de conectarse a ambos servidores. Si desea obtener más información, consulte Crear una política para que ESET Management Agent

se conecte al nuevo ESET PROTECT Server.

4. Aplique esta política a sus ordenadores cliente y permita que las instancias de ESET Management Agent se repliquen. Aunque la política redirigirá a los clientes al nuevo servidor (que no está funcionando), las instancias de ESET Management Agent utilizarán la información del servidor alternativo para conectarse a la dirección IP original.

5. Configure el nuevo Certificado del servidor en Más > Configuración.

6. Reinicie el servicio de ESET PROTECT Server y cambie la dirección IP o el nombre de host.

Consulte nuestro artículo de la Base de conocimiento para acceder a instrucciones ilustradas de cómo cambiar la dirección del ESET PROTECT Server.

Migración desde ERA 5.x

No puede actualizar o migrar directamente ERA de 5. x a ESET PROTECT 9.1.

Si tiene ERA 5. x instalado, realice estas acciones:

1. Migrar de ERA 5. x a ESMC 7.2
2. Actualizar ESMC 7.2 a ESET PROTECT 9.1

Desinstalar ESET PROTECT Server y sus componentes

Seleccione uno de los capítulos que se indican a continuación para desinstalar ESET PROTECT Server y sus componentes:

- Desinstalar ESET Management Agent
- Windows: desinstalar ESET PROTECT Server y sus componentes
- Linux: actualizar, reinstalar o desinstalar componentes de ESET PROTECT
- macOS: desinstalar ESET Management Agent y el producto ESET Endpoint
- Retirar del servicio el antiguo ESMC/ESET PROTECT/MDM Server después de la migración a otro servidor

Desinstalar ESET Management Agent

ESET Management Agent puede desinstalarse de varias formas.

Desinstalación remota con ESET PROTECT Web Console

1. Inicio de sesión en ESET PROTECT Web Console.

2. En el panel **Ordenadores**, seleccione el ordenador en el que desee quitar ESET Management Agent y haga clic en **Nueva tarea**.

También puede seleccionar varios ordenadores a la vez. Para ello, marque las casillas de verificación correspondientes y, a continuación, haga clic en **Ordenador** > **Tareas** > **Nueva tarea**.

3. Introduzca un **Nombre** para la tarea.

4. En el menú desplegable **Categoría de la tarea**, seleccione **ESET PROTECT**.

5. En el menú desplegable **Tarea**, seleccione Detener administración (desinstalar ESET Management Agent).

Cuando desinstale el agente de ESET Management del ordenador cliente, ESET PROTECT dejará de administrar el dispositivo:
- El producto de seguridad de ESET puede conservar algunos ajustes después de la desinstalación del agente de ESET Management.
- Si el agente está protegido por contraseña, no podrá desinstalarlo. Se recomienda restablecer algunos ajustes que no se deseen mantener (por ejemplo, la protección con contraseña) a los valores predeterminados mediante una política antes de quitar el dispositivo de la administración.
- Asimismo se abandonarán todas las tareas que se estén ejecutando en el agente. Es posible que los estados de ejecución **En ejecución**, **Finalizado** o **Con error** de esta tarea no se muestren con precisión en ESET PROTECT Web Console en función de la replicación de los datos.
- Tras la desinstalación del agente puede gestionar el producto de seguridad mediante eShell o la EGUI integrada.

6. Revise la tarea **Resumen** y haga clic en **Finalizar**.

7. Hacer clic en Crear desencadenador para especificar cuándo debe ejecutarse esta tarea del cliente y en qué **destinos** debe hacerse.

Desinstalación local: Windows

Consulte también las instrucciones de desinstalación local de ESET Management Agent en Linux o macOS. Para resolver problemas de desinstalación del agente, consulte Resolución de problemas de desinstalación de ESET Management Agent.

1. Conéctese al ordenador de punto final en el que desee quitar ESET Management Agent (por ejemplo, a través de RDP).

2. Vaya a **Panel de control** > **Programas y características** y haga doble clic en **ESET Management Agent**.

3. Haga clic en **Siguiente** > **Quitar** y siga las instrucciones de desinstalación.

Si ha configurado una contraseña utilizando una política para sus instancias de ESET Management Agent, tiene estas opciones:
- Tendrá que escribir la contraseña durante la desinstalación.
- Cancele la asignación de la política antes de desinstalar ESET Management Agent.
- Volver a implementar ESET Management Agent sobre un agente protegido por contraseña existente (un artículo de la Base de conocimiento).

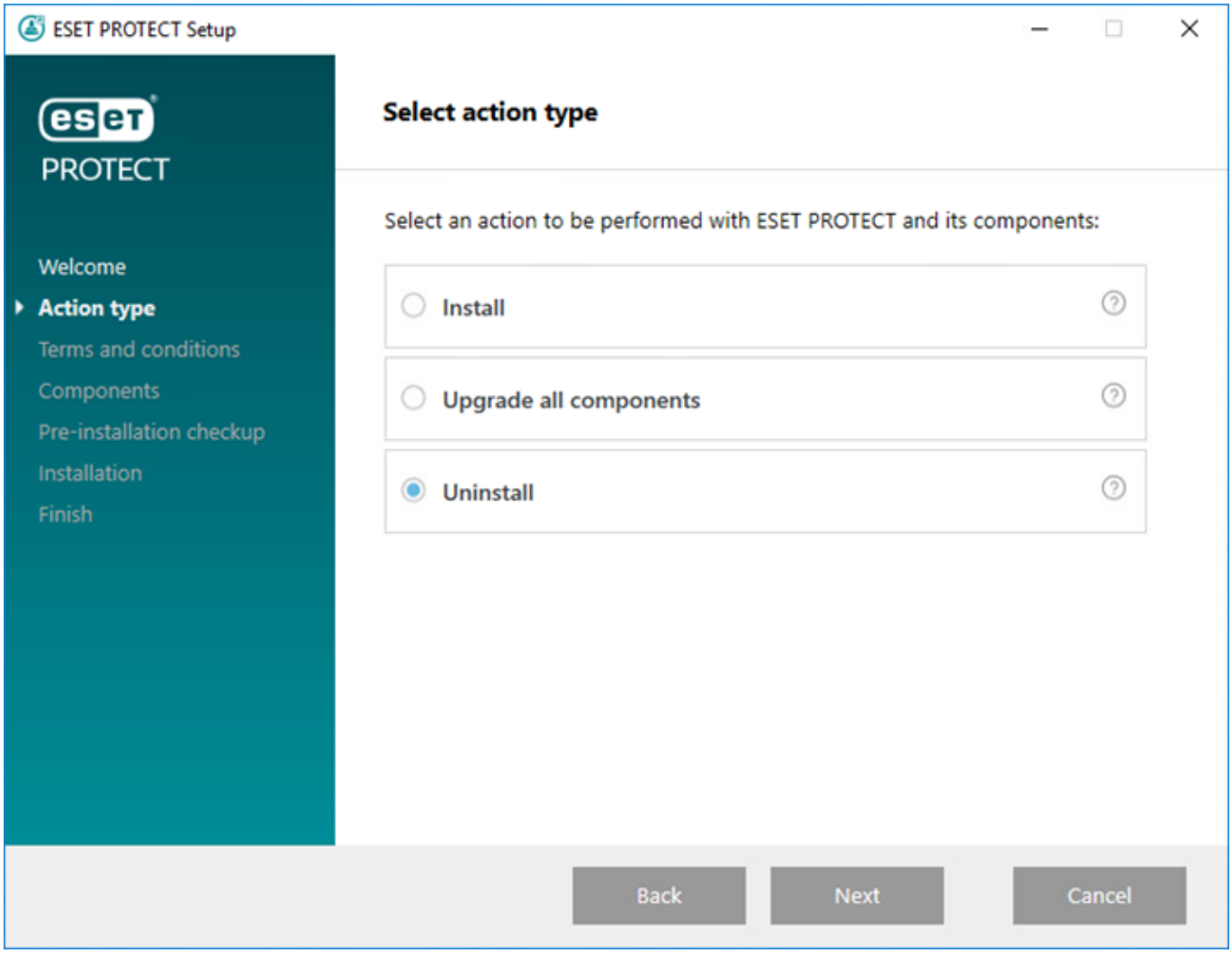
Windows: desinstalar ESET PROTECT Server y sus

componentes

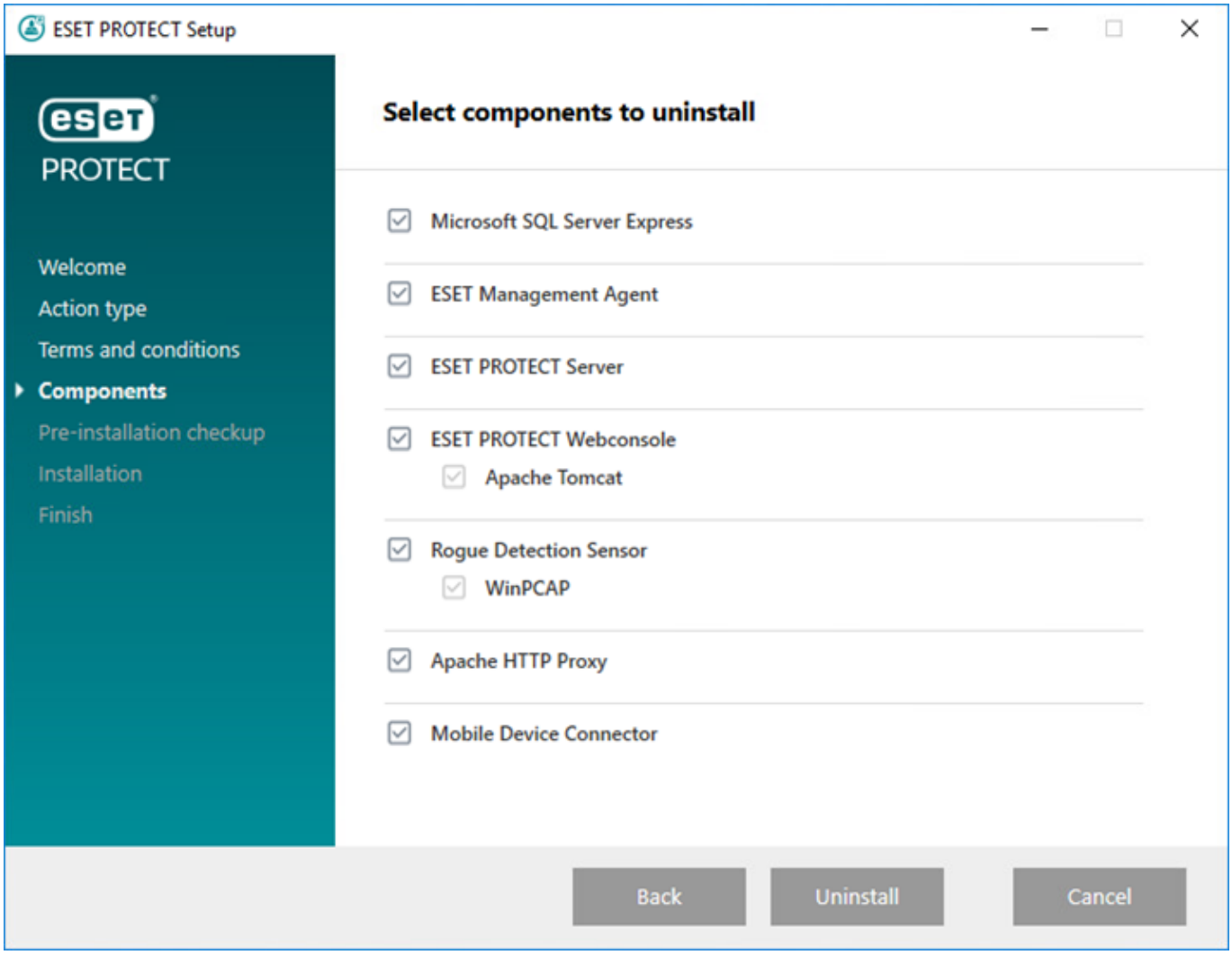
Antes de desinstalar ESET PROTECT, desinstale los agentes de los ordenadores administrados.
Antes de desinstalar el Conector del dispositivo móvil, lea Función de concesión de licencias de MDM para iOS.

Siga estos pasos para desinstalar ESET PROTECT Server y sus componentes en Windows:

1. Descargue el instalador todo en uno de ESET PROTECT y descomprima el paquete.
2. Ejecute el archivo *Setup.exe*. Puede seleccionar el **Idioma** en el menú desplegable. Haga clic en **Siguiente**.
3. Seleccione **Desinstalar** y haga clic en **Siguiente**.



4. Acepte el EULA y haga clic en **Siguiente**.
5. Seleccione los componentes que desee desinstalar y haga clic en **Desinstalar**.



6. Es posible que deba reiniciar el ordenador para completar la eliminación de determinados componentes.

Consulte también Retirar del servicio el antiguo ESMC/ESET PROTECT/MDM Server después de la migración a otro servidor.

Linux: actualizar, reinstalar o desinstalar componentes de ESET PROTECT

Si desea volver a instalar o actualizar a una versión más reciente, solo tiene que ejecutar el script de instalación de nuevo.

Para desinstalar un componente (en este caso ESET PROTECT Server), ejecute el instalador con el parámetro `--uninstall` como se muestra a continuación:

```
sudo ./server-linux-x86_64.sh --uninstall --keep-database
```

Si desea desinstalar otro componente, utilice el nombre del paquete correspondiente en el comando. Por ejemplo, ESET Management Agent:

```
sudo ./agent-linux-x86_64.sh --uninstall
```

los archivos de configuración y de la base de datos se eliminarán durante la desinstalación. Para conservar los archivos de la base de datos, cree un volcado SQL de la base de datos o utilice el parámetro `--keep-database`.

Tras la desinstalación, compruebe si

- el servicio `eraserver` se ha eliminado.
- la carpeta `/etc/opt/eset/RemoteAdministrator/Server/` se ha eliminado.

Le recomendamos que cree una copia de seguridad de volcado de la base de datos antes de realizar la desinstalación en caso de que necesite restaurar los datos.
Para obtener más información sobre la reinstalación del agente, consulte el capítulo relacionado.
Para resolver problemas de desinstalación del agente, consulte Resolución de problemas de desinstalación de ESET Management Agent.

macOS: desinstalar ESET Management Agent y el producto ESET Endpoint

Desinstale ESET Management Agent y el producto ESET Endpoint de forma local o remota mediante ESET PROTECT.

Encontrará instrucciones más detalladas sobre la desinstalación local de ESET Management Agent y el producto ESET Endpoint en el artículo de la base de conocimiento.

Si desea desinstalar de forma remota el producto ESET Endpoint, asegúrese de hacerlo antes de desinstalar ESET Management Agent.

Desinstalar ESET Management Agent localmente

1. Haga clic en **Finder** para abrir una nueva ventana de **Finder**.
2. Haga clic en **Aplicaciones** > mantenga pulsada la tecla **CTRL** > haga clic en **ESET Management Agent** > seleccione **Mostrar contenido del paquete** en el menú contextual.
3. Vaya a **Contenido** > **Scripts** y haga doble clic en **Uninstaller.command** para ejecutar el desinstalador.
4. Escriba la contraseña de administrador y pulse **Entrar** si se le pide que introduzca una contraseña.
5. Verá el mensaje **Proceso completado** cuando se haya desinstalado ESET Management Agent.

Desinstalar ESET Management Agent localmente mediante Terminal

1. Abra el **Finder** > **Aplicaciones** > **Utilidades** > **Terminal**.
2. Escriba el siguiente código y pulse **Entrar**:

```
sudo /Applications/ESET\ Management\ Agent.app/Contents/Scripts/Uninstall.command ;
 exit;
```

3. Escriba la contraseña de administrador y pulse **Entrar** si se le pide que introduzca una contraseña.

4. Verá el mensaje **Proceso completado** cuando se haya desinstalado ESET Management Agent.

Desinstalar ESET Management Agent de forma remota con ESET PROTECT

En **Ordenadores**, haga clic en el ordenador macOS cliente y seleccione **Quitar** para desinstalar ESET Management Agent y quitar el ordenador de la administración.

Para resolver problemas de desinstalación del agente, consulte Resolución de problemas de desinstalación de ESET Management Agent.

Desinstalar el producto ESET Endpoint localmente

1. Haga clic en **Finder** para abrir una nueva ventana de **Finder**.

2. Haga clic en **Aplicaciones** > mantenga pulsada la tecla **CTRL** > haga clic en **ESET Endpoint Security** o **ESET Endpoint Antivirus** > seleccione **Mostrar contenido del paquete** en el menú contextual.

3. Vaya a **Contenido** > **Aplicaciones auxiliares** y haga doble clic en **Uninstaller.app** para ejecutar el desinstalador.

4. Haga clic en **Desinstalar**.

5. Escriba la contraseña de administrador y haga clic en **Aceptar** si se le pide que introduzca una contraseña.

6. Verá el mensaje **Desinstalación realizada correctamente** cuando ESET Endpoint Security o ESET Endpoint Antivirus se hayan desinstalado correctamente. Haga clic en **Cerrar**.

Desinstalar el producto ESET Endpoint localmente mediante Terminal

1. Abra el **Finder** > **Aplicaciones** > **Utilidades** > **Terminal**.

2. Escriba el siguiente código y pulse **Entrar**:

- Desinstalar ESET Endpoint Antivirus:

```
sudo /Applications/ESET\ Endpoint\ Antivirus.app/Contents/Helpers/Uninstaller.app
/Contents/Scripts/uninstall.sh
```

- Desinstalar ESET Endpoint Security:

```
sudo /Applications/ESET\ Endpoint\ Security.app/Contents/Helpers/Uninstaller.app/
Contents/Scripts/uninstall.sh
```

3. Escriba la contraseña de administrador y pulse **Entrar** si se le pide que introduzca una contraseña.

4. Verá el mensaje **Proceso completado** cuando se haya desinstalado el producto ESET Endpoint.

Desinstalar el producto ESET Endpoint de forma remota con ESET PROTECT

Para desinstalar ESET Management Agent de forma remota con ESET PROTECT, puede utilizar una de las siguientes opciones:

- En **Ordenadores**, haga clic en el ordenador macOS cliente, seleccione **Detalles** > **Aplicaciones instaladas** > seleccione **ESET Endpoint Security** o **ESET Endpoint Antivirus** y haga clic en el botón **Desinstalar**.
- Utilice la **tarea** Desinstalación de software.

Retirar del servicio el antiguo ESMC/ESET PROTECT/MDM Server después de la migración a otro servidor

Asegúrese de que su nuevo ESET PROTECT Server/MDM se esté ejecutando y que los ordenadores cliente y los dispositivos móviles estén correctamente conectados a su nuevo ESET PROTECT.

Existen varias opciones a la hora de retirar del servicio su antiguo ESMC/ESET PROTECT Server/MDM tras la migración a otro servidor:

I.**Conservar el sistema operativo del equipo servidor y reutilizarlo**

1. Detenga el servicio ESMC/ESET PROTECT Server antiguo.
2. Elimine (`DROP DATABASE`) la antigua instancia de la base de datos de ESMC/ESET PROTECT Server (MS SQL o MySQL).

Si migró la base de datos al nuevo ESET PROTECT Server, asegúrese de eliminar la base de datos del antiguo ESMC/ESET PROTECT Server antes de su desinstalación para evitar que las licencias se disocien (eliminen) de la nueva base de datos de ESET PROTECT Server.

3. Desinstale el antiguo ESMC/ESET PROTECT/MDM Server y todos sus componentes (incluidos ESET Management Agent, Rogue Detection Sensor, MDM, etc.):
    - Desinstalar ESMC 7.2: Windows
    - Desinstalar ESET PROTECT 8.x - Windows
    - Desinstalación de ESET PROTECT 9.x - Windows
    - Desinstalar ESET PROTECT: Linux

No desinstale su base de datos si hay otro software que dependa de su base de datos.

4. Planifique el reinicio del sistema operativo de su servidor después de la desinstalación.

II.**Mantener el equipo servidor**

La forma más sencilla de quitar ESMC/ESET PROTECT/MDM es formatear el disco en el que está instalado.

⚠ Esto acción borrará todo el contenido del disco, incluido el sistema operativo.

Resolución de problemas

Dado que ESET PROTECT es un producto complejo que utiliza varias herramientas de terceros y admite diversas plataformas de SO, es posible que tenga problemas que deban solucionarse.

La documentación de ESET incluye varios métodos para solucionar los problemas con ESET PROTECT. Consulte Respuestas a problemas de instalación comunes para resolver algunos problemas comunes relacionados con ESET PROTECT. Consulte también los problemas conocidos de los productos empresariales de ESET.

¿No puede solucionar el problema?

- Cada componente de ESET PROTECT tiene un archivo de registro que puede configurar para que contenga más o menos nivel de detalle. Consulte los registros para identificar errores que podrían explicar su problema.

- El nivel de detalle del registro de cada componente se establece en su política > **Configuración avanzada** > **Registro** > **Nivel de detalle de seguimiento de registros**: establezca el nivel de detalle del registro para determinar la cantidad de información que se recogerá y registrará de **Trazar** (datos meramente informativos) a **Fatal** (la información más importante).

  - Política de ESET Management Agent: para que surta efecto, la política se debe aplicar al dispositivo. Para habilitar el registro completo del ESET Management Agent en el archivo *trace.log*, cree un archivo ficticio llamado *traceAll* sin extensión en la misma carpeta que un *trace.log* y, a continuación, reinicie el ordenador (para reiniciar el servicio ESET Management Agent).

  - ESET PROTECT Configuración del servidor

  - Política de ESET Mobile Device Connector: para que surta efecto, la política se debe aplicar al dispositivo. Consulte también Resolución de problemas de MDM.

- Si no puede solucionar el problema, puede visitar el Foro de ESET Security y ponerse en contacto con la comunidad de ESET para obtener información sobre posibles problemas.

- Cuando se ponga en contacto con el Servicio de soporte técnico de ESET, es posible que le pidamos que recopile archivos de registro con ESET Log Collector o la Herramienta de diagnóstico. Le recomendamos encarecidamente que incluya registros cuando se ponga en contacto con el equipo de soporte técnico para acelerar la solicitud enviada al servicio de atención al cliente.

Actualización de los componentes de ESET PROTECT en un entorno sin conexión

Siga estos pasos para actualizar los componentes de ESET PROTECT y los productos ESET Endpoint sin disponer de acceso a Internet:

Es posible utilizar la tarea Actualización de componentes en un entorno sin conexión cuando se cumplen las siguientes condiciones:
- Hay un repositorio sin conexión disponible.
- La ubicación del repositorio de ESET Management Agent se ha configurado mediante una política en una ubicación accesible.

Actualice ESET PROTECT Server y Web Console:

1. Compruebe qué versión de la consola de administración de ESET se está ejecutando en el servidor.

2. Descargue el instalador todo en uno más reciente para Windows o los instaladores de componentes independientes más recientes de ESET PROTECT para Linux del sitio de descargas de ESET.

3. Actualice ESET PROTECT Server y ESET PROTECT Web Console:

   - Windows: Actualización con el instalador todo en uno

   - Linux: Actualización manual basada en componentes

La actualización de Web Console y Apache Tomcat borra los archivos de la Ayuda sin conexión. Si usó la ayuda sin conexión con ESMC o una versión más antigua de ESET PROTECT, vuelva a crearla para ESET PROTECT 9.1 tras la actualización para asegurarse de que tiene la ayuda sin conexión más reciente que coincide con su versión de ESET PROTECT.

Continúe con la actualización sin conexión de los productos ESET Endpoint

1. Vea qué productos de ESET están instalados en los clientes: Abra ESET PROTECT Web Console y diríjase a **Consola** > **Aplicaciones de ESET**.

2. Asegúrese de tener las versiones más recientes de los productos ESET Endpoint.

3. Descargue los instaladores del sitio de descargas de ESET en el repositorio local configurado durante la instalación sin conexión.

4. Ejecute una tarea Instalación del software desde ESET PROTECT Web Console.

Respuestas a problemas de instalación comunes

Expanda la sección del mensaje de error que desee resolver:

ESET PROTECT Server

El servicio ESET PROTECT Server no se inicia:

Instalación dañada

- Este podría ser el resultado de claves de registro que faltan, archivos que faltan o permisos de archivo no válidos.

- El instalador todo en uno de ESET tiene su propio archivo de registro. Cuando instale un componente

manualmente, utilice el método Registro de MSI.

Puerto de escucha ya utilizado (principalmente 2222 y 2223)

Utilice el comando correspondiente para su SO:

- Windows:

```
netstat -an | find "2222"
netstat -an | find "2223"
```

- Linux:

```
netstat | grep 2222
netstat | grep 2223
```

La base de datos no se está ejecutando o no está accesible

- MS SQL Server: Compruebe que el puerto 1433 está disponible en el servidor de base de datos o intente iniciar sesión en SQL Server Management Studio
- MySQL: Compruebe que el puerto 3306 está disponible en el servidor de base de datos o intente iniciar sesión en la interfaz de su base de datos (por ejemplo, utilizando la interfaz de línea de comandos de MySQL o `phpmyadmin`)

Base de datos dañada

Aparecerán varios errores de SQL en el archivo de registro de ESET PROTECT Server. Le recomendamos que restaure la base de datos a partir de una copia de seguridad. Si no existe una copia de seguridad, reinstale ESET PROTECT.

Recursos del sistema insuficientes (espacio en disco, RAM)

Compruebe los procesos en ejecución y el rendimiento del sistema:

- Usuarios de Windows: Ejecute y revise la información en el Administrador de tareas o en el Visor de eventos
- Usuarios de Linux: Ejecute uno de los siguientes comandos:
`df -h` (para consultar la información sobre el espacio en disco)
`cat /proc/meminfo` (para consultar la información sobre el espacio en memoria)
`dmesg` (para consultar el estado del sistema Linux)

Error con el conector ODBC durante la conexión con ESET PROTECT

```
Error: (Error 65533) ODBC connector compatibility check failed.
Please install ODBC driver with support for multi-threading.
```

Vuelva a instalar la versión del controlador de ODBC compatible con multi-threading o vuelva a configurar *odbcinst.ini* como se muestra en la sección Configuración de ODBC.

Error de conexión de base de datos durante la instalación de ESET

PROTECT Server

La instalación de ESET PROTECT Server finaliza con el mensaje de error genérico:

```
The database server is not configured correctly.
Please check the documentation and reconfigure the database server as needed.
```

Mensaje de error del registro de instalación:

```
Error: Execution test of long statement failed with exception:
CMysqlCodeTokenExecutor: CheckVariableInnodbLogFileSize:
Server variables innodb_log_file_size*innodb_log_files_in_group

value 100663296 is too low.
```

Compruebe que la configuración del controlador de la base de datos coincide con la que se muestra en la sección Configuración de ODBC.

ESET Management Agent

Desinstalación y resolución de problemas del agente ESET Management

- Consulte archivos de registro para ESET Management Agent.

- Puede desinstalar ESET Management Agent utilizando ESET Uninstaller o de una forma no convencional (por ejemplo, quitando archivos o quitando el servicio de ESET Management Agent y las entradas de registro). Si hay un producto ESET Endpoint en el mismo ordenador, no será posible debido a la autodefensa activada.

- El mensaje "La base de datos no se ha podido actualizar. Quite el producto o elija volver a instalar." aparece durante la desinstalación del agente - Repare ESET Management Agent:

    1. Haga clic en **Panel de control** > **Programas y características** y haga doble clic en **ESET Management Agent**.

    2. Haga clic en **Siguiente** > **Reparar** y siga las instrucciones.

Todas las formas posibles de desinstalar ESET Management Agent se describen en la sección Desinstalación.

Se produce el código de error 1603 durante la instalación del agente

Este error puede aparecer cuando los archivos del instalador no están disponibles en el disco local. Para resolver este problema, copie los archivos del instalador en el directorio local y ejecute la instalación de nuevo. Si los archivos ya están presentes o el error sigue apareciendo, siga las instrucciones de la Base de conocimiento.

Aparece un mensaje de error durante la instalación del agente en Linux

Mensaje de error:

```
Checking certificate ... failed
Error checking peer certificate: NOT_REGULAR_FILE
```

Este error puede estar provocado por el uso de un nombre de archivo incorrecto en el comando de instalación. La consola distingue entre mayúsculas y minúsculas. Por ejemplo, `Agent.pfx` no es lo mismo que `agent.pfx`.

La implementación remota desde Linux en Windows 8.1 (32 bits) ha fallado

Se trata de un problema de autenticación provocado por la actualización KB3161949 de Microsoft. Esto se puede resolver al suprimir dicha actualización de los hosts en los que la implementación falla.

El ESET Management Agent no se puede conectar al ESET PROTECT Server

Consulte Resolución de problemas de conexión con el agente y nuestro artículo de la base de conocimiento.

El script instalador del agente se cerró con el código 30

Utiliza el script instalador del agente con una ubicación de instalador personalizada y no ha editado el script correctamente. Revise la página de ayuda e inténtelo de nuevo.

Web Console

Proxy HTTP Apache

El tamaño de la caché del proxy HTTP Apache es de varios GB y sigue aumentando

Si ha instalado el proxy HTTP Apache utilizando el instalador todo en uno, las limpiezas se activarán de forma automática. Si las limpiezas no funcionan correctamente, realice una limpieza manual o programe una tarea de limpieza.

Las actualizaciones del motor de detección no funcionan tras la instalación del proxy HTTP Apache

Si las estaciones de trabajo cliente no pueden actualizarse, consulte las instrucciones de la base de conocimiento para desactivar el proxy HTTP Apache en las estaciones de trabajo de punto final durante un tiempo. Una vez solucionados los problemas de conexión, piense en volver a activar el proxy HTTP Apache.

La actualización remota de ESET Management Agent falla con el código de

error 20008

Si la actualización remota de ESET Management Agent falla con el siguiente mensaje:
GetFile: Failed to process the HTTP request (error code 20008, url: 'http://repository.eset.com/v1//info.meta')

Siga los pasos del I al III de este artículo para resolver el problema de conexión. Si la máquina en la que se supone que el ESET Management Agent debe actualizarse se encuentra fuera de su red corporativa, configure una política para que ESET Management Agent no utilice un proxy para conectarse al repositorio cuando esté fuera de la red corporativa.

ESET Rogue Detector Sensor

¿Por qué el siguiente mensaje de error se registra continuamente en el archivo trace.log de ESET Rogue Detector?

```
Information: CPCAPDeviceSniffer [Thread 764]:
CPCAPDeviceSniffer on rpcap://\Device\NPF_

{2BDB8A61-FFDA-42FC-A883-CDAF6D129C6B} throwed error:
Device open failed with error:Error opening adapter:

The system cannot find the device specified. (20)
```

Este problema radica en WinPcap. Detenga el servicio ESET Rogue Detector Sensor, vuelva a instalar la versión más reciente de WinPcap (como mínimo la versión 4.1.0) y reinicie el servicio ESET Rogue Detector Sensor.

Linux

Falta la dependencia libQtWebKit en CentOS Linux

Si aparece el siguiente error:

```
Error: CReportPrinterModule [Thread 7f5f4c7b8700]:
ReportPrinter: ReportPrinterTool exited with:
/opt/eset/RemoteAdministrator/Server//ReportPrinterTool:
error while loading shared libraries: libQtWebKit.so.4:
cannot open shared object file: No such file or directory [code:127]
```

Siga las instrucciones del artículo de la base de conocimiento.

La instalación de ESET PROTECT Server en CentOS 7 ha fallado

Si aparece el siguiente error:

```
Error: DbCheckConnection: locale::facet::_S_create_c_locale name not valid
```

La causa probable del problema es la configuración del entorno/regional. La ejecución del siguiente comando antes del script del instalador del servidor debería ayudar:

```
export LC_ALL="en_US.UTF-8"
```

Microsoft SQL Server

Aparece el código de error -2068052081 durante la instalación de Microsoft SQL Server.

Reinicie el ordenador y vuelva a realizar la instalación. Si el problema no desaparece, desinstale el cliente nativo de SQL Server y realice la instalación de nuevo. Si esto no resuelve el problema, desinstale todos los productos de Microsoft SQL Server, reinicie el ordenador y realice la instalación de nuevo.

Aparece el código de error -2067922943 durante la instalación de Microsoft SQL Server.

Compruebe que su sistema cumpla con los requisitos de la base de datos de ESET PROTECT.

Aparece el código de error -2067922934 durante la instalación de Microsoft SQL Server.

Asegúrese de que tiene los privilegios de la cuenta de usuario correctos.

Se muestra "No se pudieron cargar los datos" en Web Console.

MS SQL Server intenta utilizar todo el espacio posible para los registros de transacciones. Si desea liberar espacio, visite el sitio web oficial de Microsoft.

Aparece el código de error -2067919934 durante la instalación de Microsoft SQL Server.

Asegúrese de que todos los pasos anteriores se hayan realizado correctamente. Este error está provocado por un fallo en la configuración de los archivos del sistema. Reinicie el ordenador y vuelva a realizar la instalación.

Archivos de registro

Cada componente de ESET PROTECT realiza el proceso de registro. Los componentes de ESET PROTECT escriben información sobre determinados eventos en archivos de registro. La ubicación de los archivos de registro varía en función del componente. A continuación se muestra una lista de ubicaciones de los archivos de registro:

Windows

ESET PROTECT componente	Ubicación de los archivos de registro
ESET PROTECT Server	*C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs*

ESET PROTECT componente	Ubicación de los archivos de registro
ESET Management Agent	*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs* Consulte también resolución de problemas de conexión del agente.
ESET PROTECT Web Console y Apache Tomcat	*C:\ProgramData\ESET\RemoteAdministrator\Tomcat\Logs* Consulte también https://tomcat.apache.org/tomcat-9.0-doc/logging.html
Conector del dispositivo móvil	*C:\ProgramData\ESET\RemoteAdministrator\MDMCore\Logs* Consulte también Resolución de problemas de MDM.
Rogue Detection Sensor	*C:\ProgramData\ESET\Rogue Detection Sensor\Logs*
Proxy HTTP Apache	*C:\Program Files\Apache HTTP Proxy 2.[x.xx]\logs* *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\logs\errorlog*

C:\ProgramData se oculta de forma predeterminada. Para mostrar la carpeta:
1.Vaya a **Inicio** > **Panel de control** > **Opciones de carpeta** > **Ver**.
2.Seleccione **Mostrar archivos, carpetas y unidades ocultos** y haga clic en **Aceptar**.

Linux

ESET PROTECT componente	Ubicación de los archivos de registro
ESET PROTECT Server	*/var/log/eset/RemoteAdministrator/Server/* */var/log/eset/RemoteAdministrator/EraServerInstaller.log*
ESET Management Agent	*/var/log/eset/RemoteAdministrator/Agent/* */var/log/eset/RemoteAdministrator/EraAgentInstaller.log*
Conector del dispositivo móvil	*/var/log/eset/RemoteAdministrator/MDMCore/* */var/log/eset/RemoteAdministrator/MDMCore/Proxy/* Consulte también Resolución de problemas de MDM.
Proxy HTTP Apache	*/var/log/httpd/*
ESET PROTECT Web Console y Apache Tomcat	*/var/log/tomcat/* Consulte también https://tomcat.apache.org/tomcat-9.0-doc/logging.html
ESET RD Sensor	*/var/log/eset/RogueDetectionSensor/*

Dispositivo virtual de ESET PROTECT

ESET PROTECT componente	Ubicación de los archivos de registro
Configuración del dispositivo virtual de ESET PROTECT	*/root/appliance-configuration-log.txt*
ESET PROTECT Server	*/var/log/eset/RemoteAdministrator/EraServerInstaller.log*
Proxy HTTP Apache	*/var/log/httpd*

macOS

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/

/Users/%user%/Library/Logs/EraAgentInstaller.log

Herramienta de diagnóstico

La herramienta de diagnóstico es una parte de los componentes de ESET PROTECT. Se utiliza para recopilar y empaquetar los registros que pueden utilizar los desarrolladores y agentes del servicio de soporte técnico para resolver problemas con los componentes del producto.

Ubicación de la herramienta de diagnóstico

Windows

Carpeta: *C:\Program Files\ESET\RemoteAdministrator\<product>***Diagnostic.exe**.

Linux

En el siguiente directorio del servidor: */opt/eset/RemoteAdministrator/<product>/*, hay un ejecutable de **Diagnostic<product>** (una palabra, por ejemplo, **DiagnosticServer**, **DiagnosticAgent**)

Uso (Linux)

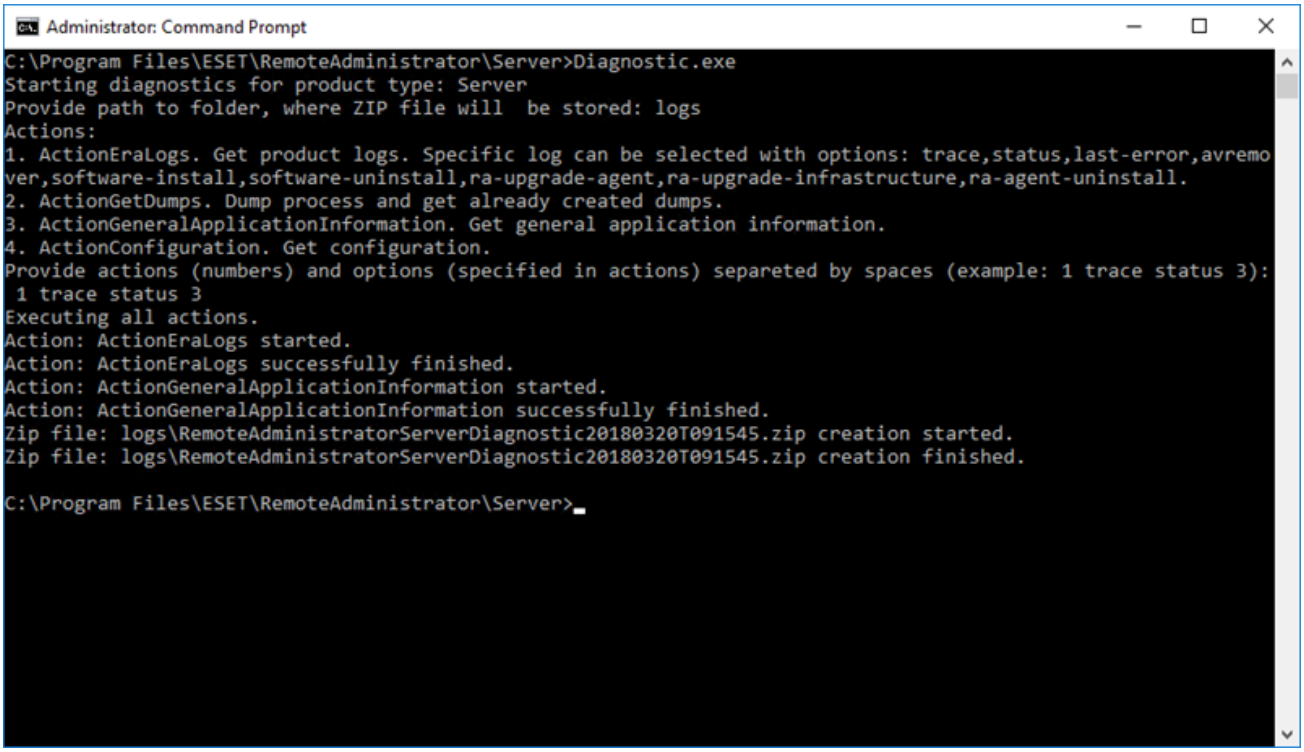
Ejecute el ejecutable de diagnóstico en el terminal como usuario raíz y siga las instrucciones mostradas en la pantalla.

Uso (Windows)

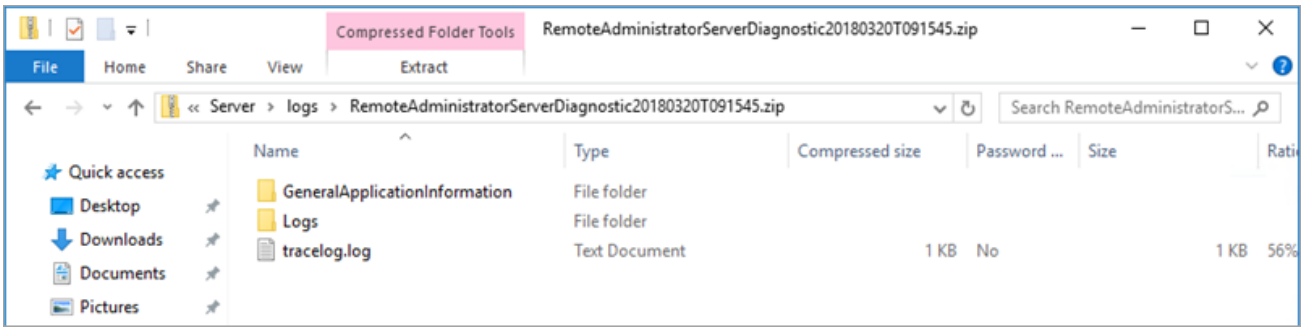
1. Ejecute la herramienta con el símbolo del sistema.

2. Introduzca la ubicación de los archivos de registro que desea guardar (en nuestro ejemplo, "logs") y pulse **Intro**.

3. Introduzca la información que desee recopilar (en nuestro ejemplo, `1 trace status 3`). Consulte **Acciones** a continuación para obtener más información.



4. Cuando finalice, podrá encontrar los archivos de registro comprimidos en un archivo *.zip* en el directorio "**logs**" de la ubicación de la herramienta de diagnóstico.



Acciones

- **ActionEraLogs**: se crea una carpeta de registros donde se guardan todos los registros. Para especificar solo determinados registros, utilice un espacio para separar cada registro.

- **ActionGetDumps**: se crea una carpeta nueva. Generalmente se crea un archivo de proceso de volcado si se detecta un problema. Cuando se detecta un problema grave el sistema crea un archivo de volcado. Para revisarlo manualmente, vaya a la carpeta %temp% (en Windows) o a la carpeta /tmp/ (en Linux) e inserte un archivo dmp.

> El servicio del componente (Agent, , Server, RD Sensor,) debe estar en ejecución.

- **ActionGeneralApplicationInformation**: se crea la carpeta GeneralApplicationInformation y dentro de ella el archivo *GeneralApplicationInformation.txt*. Este archivo contiene información de texto que incluye el nombre y la versión del producto instalado actualmente.

- **ActionConfiguration**: se crea una carpeta de configuración donde se guarda el archivo storage.lua.

Problemas después de la actualización o migración de ESET PROTECT Server

Si no puede iniciar el servicio ESET PROTECT Server debido a daños en la instalación y a mensajes de error de los archivos de registro desconocidos, realice una reparación siguiendo los pasos que se indican a continuación:

le recomendamos que realice una Copia de seguridad del servidor de base de datos antes de iniciar la reparación.

1. Vaya a **Inicio** > **Panel de control** > **Programa y características** y haga doble clic en **ESET PROTECT Server**.

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

3. Vuelva a utilizar los ajustes de conexión de la base de datos existentes y haga clic en **Siguiente**. Haga clic en **Sí si se le solicita una confirmación**. Encontrará la información de conexión de la base de datos en *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*

4. Seleccione **Usar contraseña de administrador ya almacenada en la base de datos** y haga clic en **Siguiente**.

5. Seleccione **Mantener certificados existentes actualmente** y haga clic en **Siguiente**.

6. Active ESET PROTECT Server con una clave de licencia válida o seleccione **Activar más tarde** (consulte Administración de licencias para obtener instrucciones adicionales) y haga clic en **Siguiente**.

7. Haga clic en **Reparar**.

8. Conéctese a Web Console de nuevo y compruebe si todo está correcto.

Otros casos de resolución de problemas:

ESET PROTECT Server no se está ejecutando pero hay una copia de seguridad de la base de datos:

1. Restaure la copia de seguridad de la base de datos.

2. Compruebe que el nuevo equipo utiliza la misma dirección IP o el mismo nombre de host que la instalación anterior para garantizar la conexión de los agentes.

3. Repare ESET PROTECT Server y utilice la base de datos restaurada.

ESET PROTECT Server no se está ejecutando pero tiene el certificado del servidor exportado y la autoridad certificadora del mismo:

1. Compruebe que el nuevo equipo utiliza la misma dirección IP o el mismo nombre de host que la instalación anterior para garantizar la conexión de los agentes.

2. Repare ESET PROTECT Server utilizando los certificados de copia de seguridad (cuando realice la reparación, seleccione **Cargar certificados desde archivo** y siga las instrucciones).

ESET PROTECT Server no se está ejecutando y no tiene una copia de seguridad de la base de datos o el certificado de ESET PROTECT Server y la autoridad certificadora:

1. Repare ESET PROTECT Server.

2. Repare las instancias de ESET Management Agent utilizando uno de los siguientes métodos:

   - Script instalador del agente
   - Implementación remota (para ello deberá desactivar el cortafuegos en los equipos de destino)
   - Instalador de componentes del agente manual

Registro de MSI

Esto resulta útil si no puede instalar correctamente un componente de ESET PROTECT en Windows, por ejemplo, ESET Management Agent:

```
msiexec /i C:\Users\Administrator\Downloads\Agent_x64.msi /L*v log.txt
```

ESET PROTECT API

La ESET PROTECT ServerApi (*ServerApi.dll*) es una interfaz de programación de aplicaciones, un conjunto de funciones y herramientas para crear aplicaciones de software personalizadas que cumplen sus necesidades y especificaciones. Mediante el uso de ServerApi, su aplicación puede proporcionar una interfaz personalizada, funcionalidades y operaciones que normalmente realizarían a través de ESET PROTECT Web Console, como administración de ESET PROTECT, generar y recibir informes, etc.

Si desea obtener más información y ejemplos en lenguaje C y una lista de mensajes JSON disponibles, consulte la siguiente ayuda en línea:

ESET PROTECT 9 API

Preguntas frecuentes

¿Por qué debo instalar Java en un servidor? ¿Acaso esto no crea un riesgo de seguridad? La mayoría de las empresas de seguridad y marcos de seguridad recomiendan desinstalar Java de los ordenadores, especialmente de los servidores.

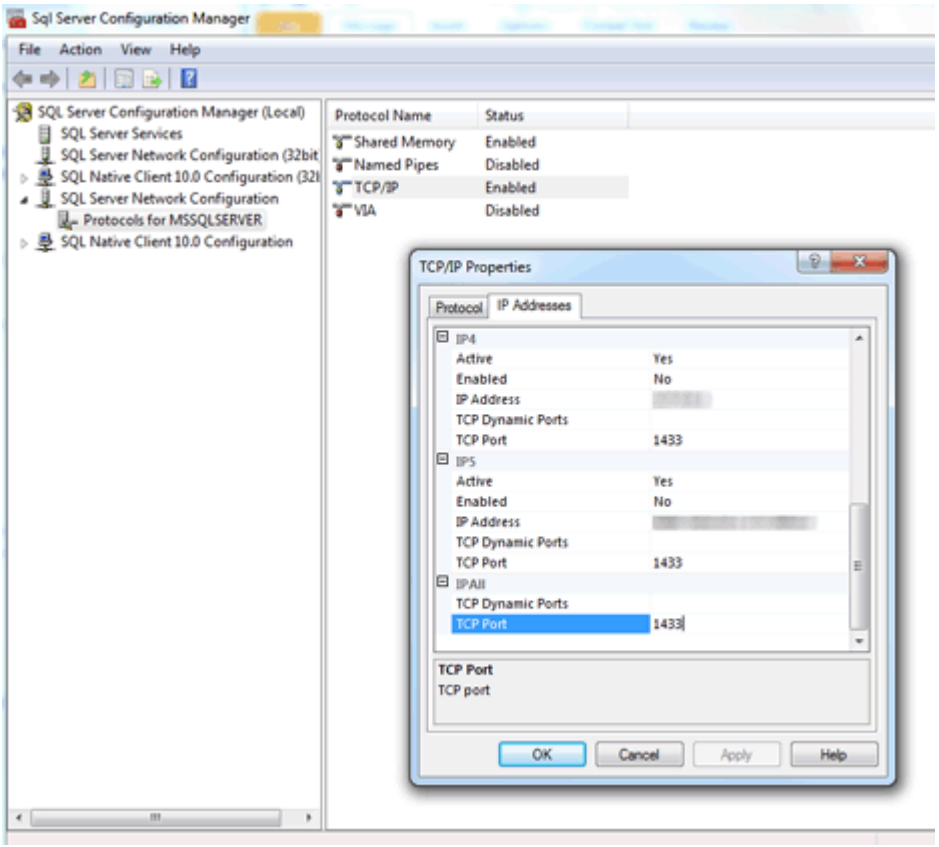
ESET PROTECT Web Console requiere Java/OpenJDK para funcionar. Java es un estándar del sector para consolas

web, y las principales consolas web utilizan Java y un servidor web (Apache Tomcat) para funcionar. Java es necesario para ofrecer soporte al servidor web multiplataforma. Es posible instalar un servidor web en un equipo dedicado por motivos de seguridad.

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

¿Cómo puedo saber qué puerto utiliza SQL Server?

Existen diversas formas de determinar el puerto que está usando SQL Server. El resultado más preciso se obtiene a través del administrador de configuración de SQL Server. Consulte la figura siguiente para ver un ejemplo de dónde encontrar esta información en el administrador de configuración de SQL:



Después de instalar SQL Server Express (incluido en mi paquete de ESET PROTECT) en mi Windows Server 2012 no parece estar escuchando en un puerto de SQL estándar. Lo más probable es que esté escuchando un puerto distinto al predeterminado, el puerto 1433.

¿Cómo puedo configurar MySQL para aceptar un paquete de gran

tamaño?

Consulte las instrucciones de instalación y configuración de MySQL para Windows o Linux.

Si instalo SQL por mí mismo, ¿cómo creo una base de datos ESET PROTECT

No tiene que hacerlo. El instalador de *Server.msi*, no el instalador de ESET PROTECT, crea una base de datos. El instalador de ESET PROTECT se incluye para simplificar los pasos: instala SQL Server y, a continuación, el instalador *Server.msi* crea la base de datos.

¿El ESET PROTECT instalador crea una nueva base de datos para mí en una instalación de MS SQL Server existente, si le proporciono las credencias y detalles de conexión adecuados de MS SQL Server? Resultaría práctico si el instalador admitiera diferentes versiones de SQL Server (2014, 2019, etc.).

La base de datos se crea mediante *Server.msi*. Sí, puede crear una base de datos de ESET PROTECT para usted en instancias de SQL Server instaladas individualmente. Las versiones compatibles de MS SQL Server son 2014 y posteriores.

El instalador todo en uno de ESET PROTECT 9.1 instala Microsoft SQL Server Express 2019 de forma predeterminada.

- Si utiliza una versión anterior de Windows (Server 2012 o SBS 2011), Microsoft SQL Server Express 2014 se instalará de forma predeterminada.
- El instalador genera automáticamente una contraseña aleatoria para la autenticación de la base de datos (almacenada en *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

⚠ Microsoft SQL Server Express tiene un límite de tamaño de 10 GB en cada base de datos relacional. No recomendamos el uso de Microsoft SQL Server Express:
- En entornos empresariales o redes de gran tamaño.
- Si desea usar ESET PROTECT con ESET Inspect.

Si va a realizar la instalación en un SQL Server existente, ¿SQL Server debe usar el modo de autenticación de Windows integrado de forma predeterminada?

No, porque el modo de autenticación de Windows se puede desactivar en SQL Server y la única forma de iniciar sesión es utilizar la autenticación de SQL Server (con nombre de usuario y contraseña). Durante la instalación de ESET PROTECT Server, se requiere la autenticación de modo mixto (autenticación de SQL Server y autenticación de Windows). Al instalar manualmente SQL Server, se recomienda que cree una contraseña raíz (el usuario raíz se llama "sa", por las siglas en inglés de administrador de seguridad) y la guarde para el futuro en un lugar seguro. La contraseña raíz puede ser necesaria cuando se actualiza ESET PROTECT Server. Puede configurar la Autenticación de Windows después de instalar ESET PROTECT Server.

¿Puedo utilizar MariaDB en lugar de MySQL?

No, MariaDB no es compatible. Asegúrese de instalar una versión compatible de MySQL Server y el conector ODBC. Consulte Instalación y configuración de MySQL.

He instalado Microsoft .NET Framework 4 como me ha indicado el instalador de ESET PROTECT (http://www.microsoft.com/en-us/download/details.aspx?id=17851), pero no ha funcionado en una instalación nueva de Windows Server 2012 R2 con SP1.

Este instalador no se puede utilizar en Windows Server 2012 debido a la política de seguridad en Windows Server 2012. Microsoft .NET Framework debe instalarse mediante el **Asistente para agregar roles y características**.

Es muy difícil saber si la instalación de SQL Server está en ejecución. ¿Cómo puedo saber lo que está sucediendo si la instalación tarda más de 10 minutos?

La instalación de SQL Server puede, en casos raros, tardar hasta 1 hora. Los tiempos de instalación dependen del rendimiento del sistema.

¿Cómo puedo restablecer la contraseña de administrador de Web Console (introducida durante la configuración)?

Es posible restablecer la contraseña mediante la ejecución del instalador del servidor y, después, eligiendo **Reparar**. Tenga en cuenta que la contraseña podría ser necesaria para acceder a la base de datos de ESET PROTECT si no utilizó la autenticación de Windows durante la creación de la base de datos.

- Tenga cuidado, porque algunas opciones de reparación pueden eliminar datos almacenados.
- El restablecimiento de la contraseña desactiva la autenticación de doble factor.

¿Cuál es el formato de archivo requerido al importar un archivo con una lista de ordenadores para añadirlos a ESET PROTECT?

Tiene el formato de las siguientes líneas:

All\Grupo1\GrupoN\Ordenador1
All\Grupo1\GrupoM\OrdenadorX
All es el nombre necesario del grupo raíz.

¿Puede utilizarse IIS en lugar de Apache? ¿Y otro servidor HTTP?

IIS es un servidor HTTP. La consola web necesita un contenedor de servlet Java (como Tomcat) para ejecutarse, y el servidor HTTP no es suficiente. Se han propuesto soluciones acerca de cómo cambiar IIS en un contenedor de servlet Java aunque, en general, esto no se admite.

No utilizamos un servidor HTTP Apache, utilizamos Apache Tomcat, que es un producto diferente.

¿Dispone ESET PROTECT de una interfaz de línea de comandos?

Sí, disponemos de ESET PROTECT ServerApi.

¿Puede instalar ESET PROTECT en un controlador de dominio?

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

¿Detectará la instalación de ESET PROTECT Server si SQL ya está instalado en el sistema? ¿Qué ocurre si ya está instalado? ¿Cómo afecta a MySQL?

ESET PROTECT comprobará la ejecución de SQL en un sistema si se utiliza el asistente de instalación y se ha seleccionado la instalación de SQL Express. Si SQL ya se está ejecutando en un sistema, el asistente mostrará una notificación para desinstalar la instancia de SQL existente y, a continuación, ejecutar la instalación de nuevo o instalar ESET PROTECT sin SQL Express. Consulte los requisitos de la base de datos para ESET PROTECT.

¿Dónde puedo encontrar un componente de ESET PROTECT asignado según la versión publicada?

Consulte nuestro artículo de la base de conocimiento.

¿Cómo puedo realizar una actualización de ESET PROTECT a la versión más reciente?

Consulte procedimientos de actualización.

¿Cómo puedo actualizar un sistema sin una conexión a Internet?

Mediante el uso del proxy HTTP instalado en un equipo que pueda conectarse a los servidores de actualización de ESET (en los que se almacenan los archivos de actualización en memoria caché) y dirigiendo los puntos finales a dicho proxy HTTP en una red local. Si su servidor no tiene una conexión a Internet, puede activar la función Mirror

del producto del punto final en un equipo, utilizar una unidad USB para proporcionar archivos de actualización a este ordenador y configurar el resto de ordenadores sin conexión para que lo utilicen como servidor de actualizaciones.

Para obtener más información sobre cómo realizar una instalación sin conexión, siga estas instrucciones.

¿Cómo puedo reinstalar ESET PROTECT Server y conectarlo a un SQL Server existente si el SQL Server lo configuró automáticamente la instalación inicial de ESET PROTECT?

Si instala la nueva instancia de ESET PROTECT Server con la misma cuenta de usuario (por ejemplo, una cuenta de administrador de dominio) bajo la que ha instalado el ESET PROTECT Serveroriginal, puede utilizar **MS SQL Server mediante autenticación de Windows**.

¿Cómo se solucionan problemas con la sincronización de Active Directory en Linux?

Compruebe que el nombre de dominio esté escrito en mayúsculas (`administrator@TEST.LOCAL`, en lugar de `administrator@test.local`).

¿Existe alguna forma de usar mi propio recurso de red (como el recurso compartido de SMB) en lugar del repositorio?

Puede optar por proporcionar la URL directa de la ubicación de un paquete. Si utiliza un recurso compartido de archivo, especifíquelo en el siguiente formato: file:// seguido de la ruta de acceso de red completa hasta el archivo, por ejemplo:

file://\\eraserver\install\ees_nt64_ENU.msi

¿Cómo puedo restablecer o cambiar mi contraseña?

Lo ideal sería que la cuenta de administrador solo se utilizara para crear cuentas para los administradores individuales. Una vez que se hayan creado las cuentas de administrador, la contraseña del administrador se debe guardar y la cuenta de administrador no se debe utilizar. Esta práctica permite que la cuenta de administrador se utilice únicamente para restablecer las contraseñas o ver los datos de la cuenta.

Cómo restablecer la contraseña de una cuenta de administrador de ESET PROTECT integrada:

1.Abra **Programas y características** (ejecute appwiz.cpl), localice ESET PROTECT Server y haga clic con el botón derecho.

2.Seleccione **Cambiar** en el menú contextual.

3.Elija **Reparar**.

4.Especifique los detalles de conexión a la base de datos.

5.Seleccione **Usar base de datos existente y aplicar la actualización**.

6.Cancele la selección de **Usar contraseña ya almacenada en la base de datos** y escriba una nueva contraseña.

7.Inicie sesión en ESET PROTECT Web Console con su nueva contraseña.

Se recomienda encarecidamente crear cuentas adicionales con derechos de acceso específicos según las competencias que desee que tenga la cuenta.

¿Cómo puedo cambiar los puertos de ESET PROTECT Server y ESET PROTECT Web Console?

Se requiere cambiar el puerto en la configuración de su servidor web para permitir las conexiones del servidor web con el nuevo puerto. Para hacerlo, siga estos pasos:

1.Apague el servidor web.
2.Modifique el puerto en la configuración del servidor web.
*a)*Abra el archivo *webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties*
*b)*Establezca el nuevo número de puerto (por ejemplo, `server_port=44591`)

3.Inicie el servidor web de nuevo.

¿Puedo actualizar de ERA 5 o 6 a ESET PROTECT 9 directamente mediante el instalador todo en uno?

La actualización directa no es compatible; consulte Migración desde ERA 5.x o Actualización desde ERA 6.x.

Recibo mensajes de error o tengo problemas con ESET PROTECT, ¿qué debo hacer?

Consulte Preguntas frecuentes sobre la resolución de problemas.

Acuerdo de licencia para el usuario final

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

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

Acuerdo de licencia para el usuario final

En virtud de los términos de este Acuerdo de licencia para el usuario final ("Acuerdo"), firmado por ESET, spol. s r. o., con domicilio social en Einsteinova 24, 85101 Bratislava, Slovak Republic, empresa inscrita en el Registro Mercantil administrado por el tribunal de distrito de Bratislava I, sección Sro, número de entrada 3586/B, número de registro comercial 31333532 ("ESET" o "el Proveedor") y usted, una persona física o jurídica ("Usted" o el "Usuario final"), tiene derecho a utilizar el Software definido en el artículo 1 del presente Acuerdo. El Software definido en el artículo 1 del presente Acuerdo puede almacenarse en un soporte de datos, enviarse por correo electrónico, descargarse de Internet, descargarse de los servidores del Proveedor u obtenerse de otras fuentes en virtud de los términos y condiciones especificados a continuación.

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

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

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

1. **Software**. En este acuerdo, el término "Software" se refiere a: (i) el programa informático que acompaña a este Acuerdo y todos sus componentes; (ii) todo el contenido de los discos, CD-ROM, DVD, mensajes de correo electrónico y documentos adjuntos, o cualquier otro soporte que esté vinculado a este Acuerdo, incluido el

código objeto del Software proporcionado en un soporte de datos, por correo electrónico o descargado de Internet; (iii) todas las instrucciones escritas y toda la documentación relacionada con el Software, especialmente todas las descripciones del mismo, sus especificaciones, todas las descripciones de las propiedades o el funcionamiento del Software, todas las descripciones del entorno operativo donde se utiliza, las instrucciones de uso o instalación del software o todas las descripciones de uso del mismo ("Documentación"); (iv) copias, reparaciones de posibles errores, adiciones, extensiones y versiones modificadas del software, así como actualizaciones de sus componentes, si las hay, para las que el Proveedor le haya concedido una licencia en virtud del artículo 3 de este Acuerdo. El Software se proporciona únicamente en forma de código objeto ejecutable.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6. **Restricciones de los derechos.** No puede copiar, distribuir, extraer componentes ni crear versiones derivadas

del software. El uso del software está sujeto a las siguientes restricciones:

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

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

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

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

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

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

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

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

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

9. **Versiones en varios idiomas, software en soporte dual, varias copias**. Si el software es compatible con varias plataformas o idiomas, o si recibe varias copias del software, solo puede utilizar el software para el número de sistemas informáticos y para las versiones para los que haya obtenido una licencia. No puede vender, arrendar,

alquilar, sublicenciar, prestar o transferir ninguna versión o copias del Software no utilizado por Usted.

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

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

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

13. **LIMITACIÓN DE RESPONSABILIDAD**. HASTA EL ALCANCE MÁXIMO PERMITIDO POR LA LEGISLACIÓN APLICABLE, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O SUS PROVEEDORES DE LICENCIAS SERÁN RESPONSABLES DE PÉRDIDAS DE BENEFICIOS, DE INGRESOS, DE VENTAS O DE DATOS NI DE COSTES DERIVADOS DE LA OBTENCIÓN DE PRODUCTOS O SERVICIOS DE SUSTITUCIÓN, DE DAÑOS A LA PROPIEDAD, DE DAÑOS PERSONALES, DE LA INTERRUPCIÓN DEL NEGOCIO, DE LA PÉRDIDA DE INFORMACIÓN COMERCIAL O DE DAÑOS ESPECIALES, DIRECTOS, INDIRECTOS, ACCIDENTALES, ECONÓMICOS, DE COBERTURA, CRIMINALES O SUCESIVOS, CAUSADOS DE CUALQUIER MODO, YA SEA A CAUSA DE UN CONTRATO, UNA CONDUCTA INADECUADA INTENCIONADA, UNA NEGLIGENCIA U OTRO HECHO QUE ESTABLEZCA RESPONSABILIDAD, DERIVADOS DE LA INSTALACIÓN, EL USO O LA INCAPACIDAD DE USO DEL SOFTWARE, INCLUSO EN EL CASO DE QUE AL PROVEEDOR O A SUS PROVEEDORES DE LICENCIAS O FILIALES SE LES HAYA NOTIFICADO LA POSIBILIDAD DE DICHOS DAÑOS. DADO QUE DETERMINADOS PAÍSES Y JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE RESPONSABILIDAD, PERO PUEDEN PERMITIR LA LIMITACIÓN DE RESPONSABILIDAD, EN DICHOS CASOS, LA RESPONSABILIDAD DEL PROVEEDOR, SUS EMPLEADOS, LICENCIATARIOS O AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR LA LICENCIA.

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

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

soporte técnico. ESET se reserva el derecho de rechazar, anular o terminar, a su discreción, la disposición de servicio técnico. Pueden ser necesarios los datos de Licencia, la Información y otros datos de acuerdo con la Política de Privacidad para prestar soporte técnico.

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

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

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

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

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

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

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

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

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

i. con una base razonable para fundamentar su opinión, ESET determine que el Usuario ha incumplido o es

probable que incumpla lo dispuesto en el Artículo 19 a) del Acuerdo; o

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

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

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

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

22. **Disposiciones generales**. El hecho de que alguna de las disposiciones de este acuerdo no sea válida o aplicable no afectará a la validez de las demás disposiciones del acuerdo, que seguirán siendo válidas y aplicables de conformidad con las condiciones aquí estipuladas. Este Acuerdo se ha formalizado en inglés. Si se realiza una traducción del Acuerdo por motivos de comodidad o por cualquier otro motivo, o en caso de discrepancia entre las versiones de este Acuerdo en diferentes idiomas, prevalecerá la versión en inglés.

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

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

ANEXO AL ACUERDO

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

adicionales:

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

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

EULAID: EULA-PRODUCT-PROTECT; 3537.0

Política de privacidad

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

- Procesamiento de datos personales
- Confidencialidad de los datos
- Derechos del titular de los datos

Procesamiento de datos personales

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

- La administración de los productos de seguridad de ESET requiere y almacena de manera local información como el ID y el nombre del puesto, el nombre del producto, información sobre la licencia, información de activación y caducidad, información de hardware y software relativa al ordenador administrado con el producto de seguridad de ESET instalado. Se recopilan registros relacionados con las actividades de los productos y de seguridad de ESET y los dispositivos administrados, y están disponibles para facilitar las funciones y los servicios de administración sin envío automatizado a ESET.
- Información relativa al proceso de instalación, incluida la plataforma en la que se instala nuestro producto e información sobre las operaciones y la funcionalidad de nuestros productos, como la huella digital de hardware,

los ID de instalación, los volcados de bloqueo, los ID de licencia, la dirección IP, la dirección MAC, los ajustes de configuración del producto, lo que también podría incluir los dispositivos administrados.

• La información sobre licencias, como el ID de licencia, y datos personales como el nombre, los apellidos, la dirección y la dirección de correo electrónico son necesarios para la facturación, la verificación de la autenticidad de las licencias y la prestación de nuestros servicios.

• La información de contacto y los datos contenidos en sus solicitudes de soporte pueden ser necesarios para el servicio de soporte. Según el canal que elija para ponerse en contacto con nosotros, podemos recopilar datos como su dirección de correo electrónico, su número de teléfono, información sobre licencias, datos del producto y descripción de su caso de asistencia. Es posible que le pidamos que nos facilite otra información para prestar el servicio de asistencia técnica, como los archivos de registro generados.

• Los datos relativos al uso de nuestros servicios son totalmente anónimos al finalizar la sesión. Una vez concluida la sesión, no se guarda ningún tipo de información personal.

Confidencialidad de los datos

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

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

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

Derechos del titular de los datos.

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

• derecho a solicitar a ESET acceso a sus datos personales;

• derecho de rectificación de sus datos personales en caso de que sean incorrectos (también tiene derecho a completarlos en caso de que estén incompletos);

• derecho a solicitar la eliminación de sus datos personales;

• derecho a solicitar la restricción del procesamiento de sus datos personales;

• derecho a oponerse al procesamiento;

- derecho a presentar una reclamación y
- derecho a la portabilidad de datos.

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

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