ESET PROTECT

Guía de instalación actualización y migración

Haga clic aquí para mostrar la versión de ayuda de este documento

Digital Security
Progress. Protected.

ESET PROTECT ha sido 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 Ayuda

Esta guía de instalación fue desarrollada para ayudar a la instalación y actualización de ESET PROTECT y proporciona instrucciones para el proceso.

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

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

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

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

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

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

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

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

- La Base de conocimiento de ESET incluye respuestas a las preguntas frecuentes, así como también a las soluciones recomendadas para varios temas. Actualizado regularmente por los especialistas técnicos de ESET, la Base de conocimiento es la herramienta más poderosa para solucionar distintos tipos de problemas.

- El Foro de ESET proporciona a los usuarios un medio sencillo para obtener ayuda y ayudar a los demás. Puede publicar cualquier problema o consulta relacionada con los productos de ESET.

Instalación, actualización o migración

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

ESET PROTECT no proporciona protección contra el código malicioso. La protección de su entorno depende de la presencia de una solución de seguridad de ESET como ESET Endpoint Security en las estaciones de trabajo y los dispositivos móviles o ESET Server Security para el servidor en las máquinas de servidor.

ESET PROTECT está diseñado en función de dos principios principales:

- **Administración centralizada**: toda la red se puede configurar, administrar y supervisar desde un solo lugar.

- **Escalabilidad:** el sistema se puede implementar en una red pequeña o en grandes entornos empresariales. ESET PROTECT está diseñado para adaptarse al crecimiento de su infraestructura.

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

ESET PROTECT Ayuda a las páginas a incluir una instalación completa y una guía de actualización:

- Arquitectura de ESET PROTECT
- Proceso de instalación
- Procedimientos de actualización
- Procedimientos de migración
- Procedimientos de desinstalación
- Administración de licencias
- Procesos de implementación e implementación de agentes mediante GPO o SCCM
- Primeros pasos después de instalar ESET PROTECT
- Guía de administración

Nuevas características en ESET PROTECT 9.1

Recorrido del producto

Hemos agregado un nuevo recorrido del producto para ayudarle a navegar rápidamente por nuestra solución y para que comience a usarla pronto. Obtener más información

Cambios en los nombres de productos

Se cambió el nombre de ESET Enterprise Inspector por ESET Inspect y de ESET Dynamic Threat Defense por ESET LiveGuard Advanced. Puede encontrar más información en este artículo.

Mejores reinicios

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. Obtener más información

Instalación más sencilla

Hemos rediseñado el asistente de creación del instalador para que sea más intuitivo. En la tarea Instalar software, ahora puede usar el parámetro especial “más reciente”, que garantiza que el instalador creado instale siempre la versión más reciente del producto cuando se haya lanzado. Obtener más información

Soporte nativo de ARM para macOS.

Con la versión más reciente de ESET Management Agent y ESET Endpoint Antivirus para macOS (v7), ofrecemos soporte nativo de ARM. Obtener 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. Obtener más información

Filtros avanzados

Presentamos un nuevo concepto de filtrado de datos que le ayudará a filtrar fácilmente los dispositivos relevantes en entornos de mayor tamaño, pero no solo aquí. Siempre tendrá una visión general estadística de la cantidad 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 Equipos. Obtener más información

Mejor comunicación de las actualizaciones automáticas

Hemos agregado una nueva sección azul al estado de la versión del componente en el dashboard de información general de estado para ayudarlo a identificar fácilmente los puntos de conexión con actualizaciones automáticas activadas que están esperando actualizarse, pero que también se pueden actualizar de forma manual por adelantado. Obtener más información

Lista de componentes desactualizados

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

Control web para MDM

Adaptamos las funciones de control web de Cloud MDM a la variante local. El administrador puede limitar el acceso de los empleados a varias categorías de contenido o enlaces a Internet específicos.

Otras mejoras y cambios de facilidad de uso

Puede ver más detalles en el registro de cambios.

Arquitectura

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

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

- Servidor ESET PROTECT
- Consola web ESET PROTECT
- Agente ESET Management

Los siguientes componentes auxiliares son opcionales, pero se recomienda su instalación para garantizar un mejor rendimiento de la aplicación en la red:

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

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

Información general de los elementos de la infraestructura

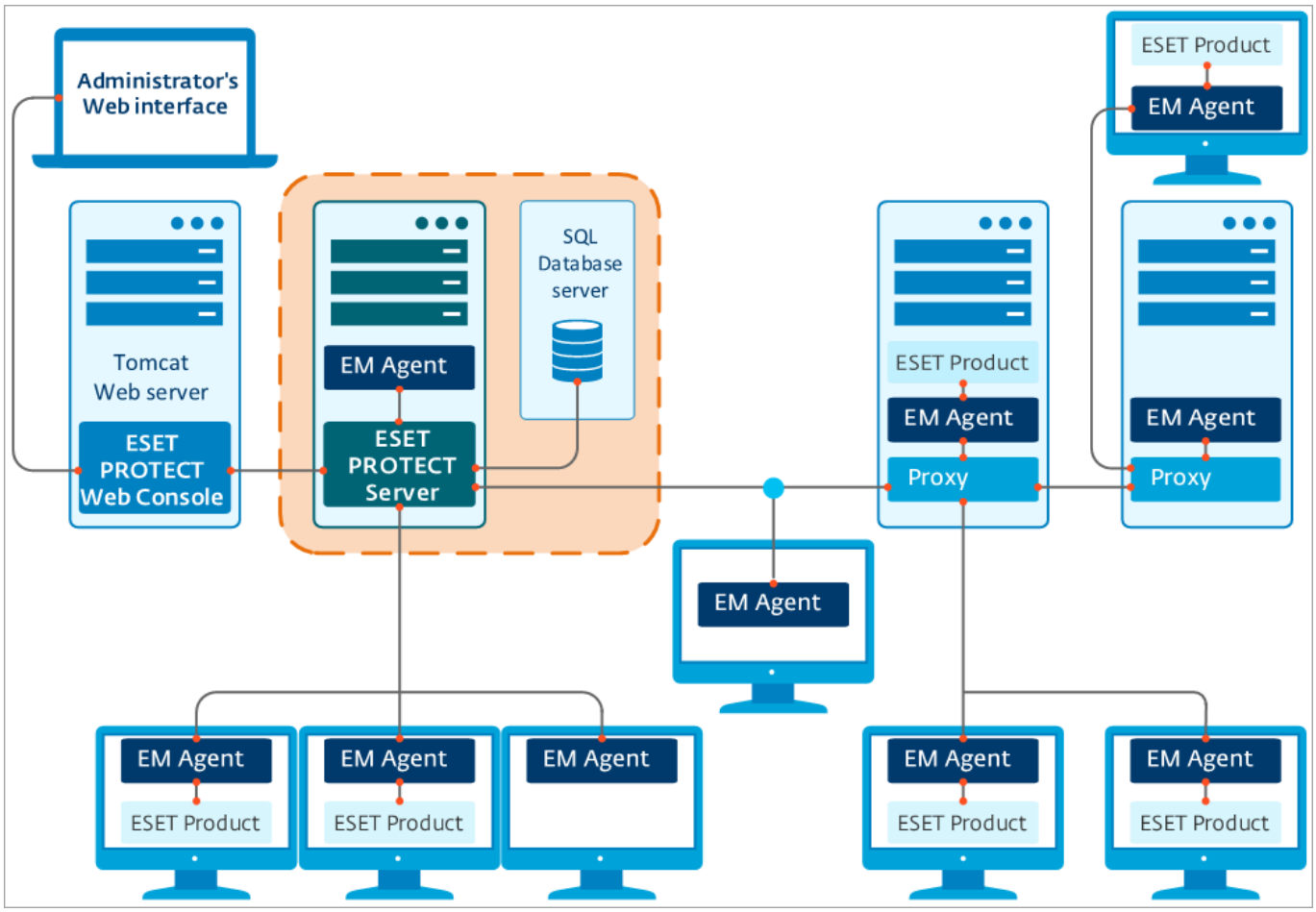
La tabla a continuación contiene información general de los elementos de la infraestructura de ESET PROTECT y sus principales funciones:

Funcionalidad	ESET PROTECTServidor	Agente ESET Management	Producto de seguridad ESET	Proxy HTTP	Servidores ESET	Conector de dispositivo móvil
Gestión remota de productos de seguridad de ESET (creación de políticas, tareas, informes, etc.)	✔	X	X	X	X	X
Comunicación con el servidor de ESET PROTECT y gestión del producto de seguridad de ESET en el dispositivo cliente	X	✔	X	X	X	✔
Provisión de actualizaciones, validación de licencia	X	X	X	X	✔	X

Funcionalidad	ESET PROTECTServidor	Agente ESET Management	Producto de seguridad ESET	Proxy HTTP	Servidores ESET	Conector de dispositivo móvil
Almacenamiento en caché y reenvío de actualizaciones (motor de detección, instaladores, módulos)	X	X	✔	✔	X	X
Reenvío del tráfico de red entre el agente de ESET Management y el servidor de ESET PROTECT	X	X	X	✔	X	X
Asegurar el dispositivo cliente	X	X	✔	X	X	X
Gestión remota de dispositivos móviles	X	X	X	X	X	✔

Servidor

ESET PROTECT El Servidor es la aplicación ejecutiva que procesa todos los datos recibidos de los clientes que se conectan al Servidor (a través del Agente ESET Management o el HTTP Proxy). Para procesar los datos correctamente, el servidor requiere una conexión estable a un servidor de la base de datos donde se almacenan los datos de la red. Se recomienda que instale el servidor de la base de datos en un equipo diferente para lograr un mejor rendimiento.



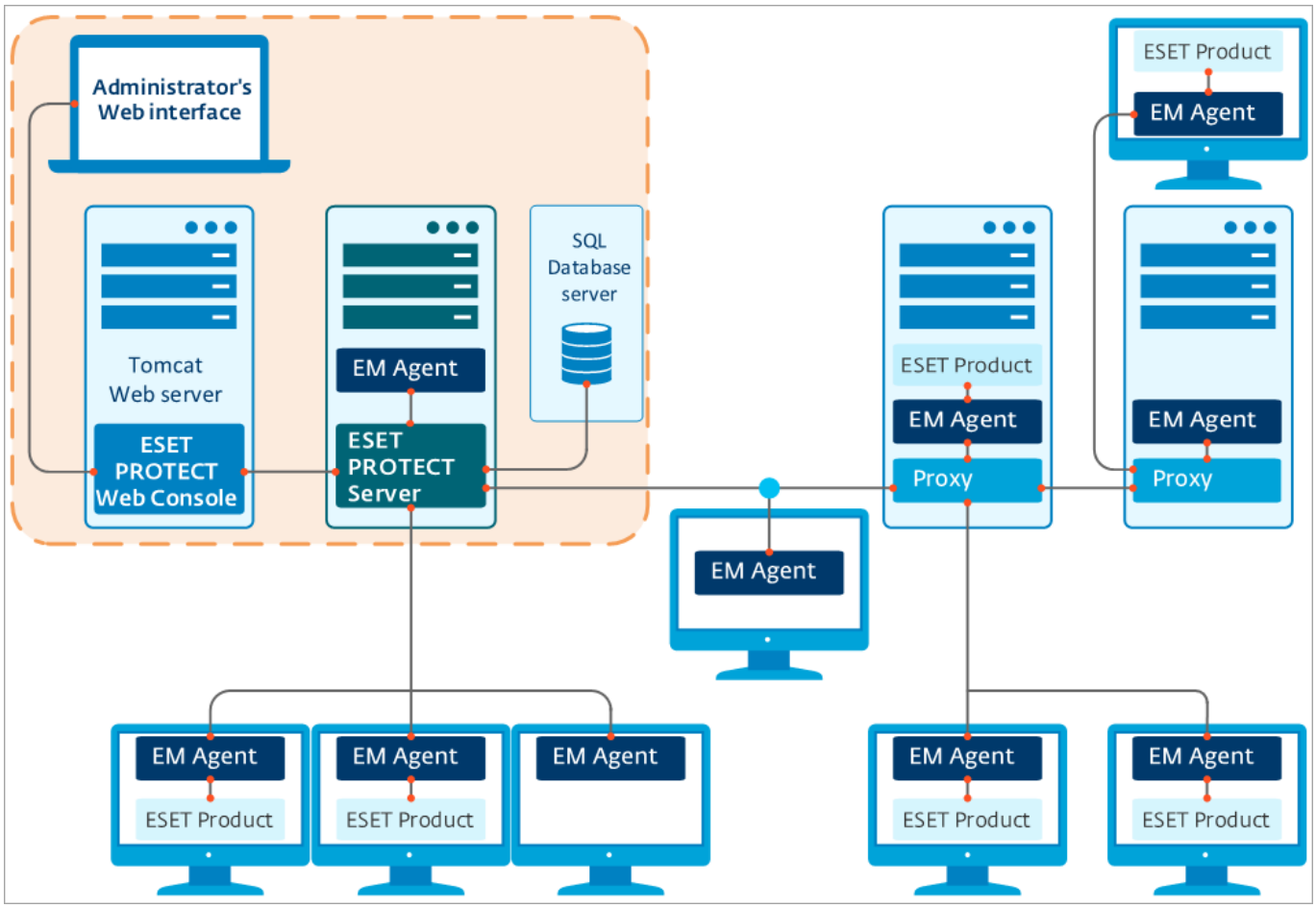
Consola web

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

dispositivo.

La consola web usa Apache Tomcat como servidor web HTTP. Al usar Tomcat en paquete en el instalador de ESET o en el dispositivo virtual, solo se permiten conexiones TLS 1.2 y 1.3 con Web Console.

> Puede instalar la consola web de ESET PROTECT en un equipo diferente a donde se ejecuta el servidor de ESET PROTECT.



Proxy HTTP

¿Qué es HTTP Proxy y cómo es útil?

HTTP Proxy reenvía la comunicación de los Agentes al Servidor ESET PROTECT en los entornos donde las máquinas del Agente no puedan alcanzar el Servidor.

¿Cómo funciona el Proxy en ESET PROTECT?

ESET PROTECT 9 utiliza una versión personalizada de Apache HTTP Proxy como componente del Proxy. Luego de una configuración correcta, el Apache HTTP Proxy puede funcionar como Proxy para los Agentes ESET Management. El Proxy no almacena o abre la comunicación, solo la envía.

¿Puedo usar otro Proxy que no sea Apache HTTP Proxy?

Puede usar cualquier solución proxy que cumpla con las siguientes condiciones con el Agente ESET Management:

- puede enviar SSL communicación
- es compatible conHTTP CONNECT
- no usa un nombre de usuario o contraseña

¿En qué difiere el nuevo protocolo de comunicación?

El servidor de ESET PROTECT se comunica con los agentes de ESET Management por medio del protocolo gRPC. La comunicación usa TLS y HTTP2 para ser compatibles con los servidores Proxy. También hay nuevas características de auto-recuperación y una conexión persistente que mejora el rendimiento de la comunicación en general.

¿Cómo afecta al rendimiento?

Usar HTTP Proxy no tiene un impacto significativo sobre el rendimiento.

¿Cuándo debo usar el Proxy?

Recomendamos usar el Proxy si la infraestructura cumple con una o más de las siguientes condiciones:

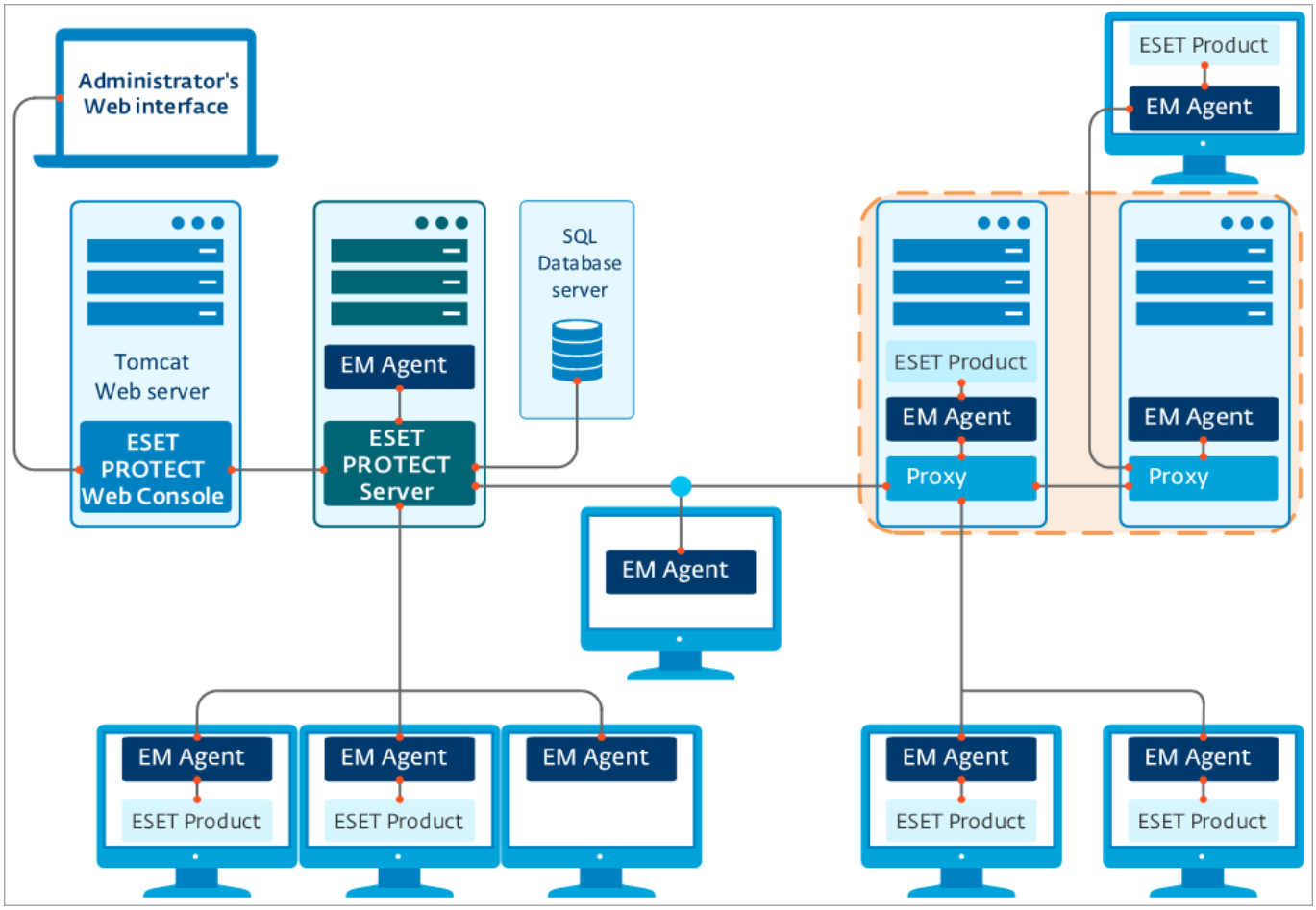
- Si las máquinas de su Agente no pueden conectarse directamente con el Servidor de ESET PROTECT.
- Si posee una ubicación remota o una sucursal y desea usar el Proxy para gestionar la comunicación:
  - entre el Servidor ESET PROTECT y el Proxy
  - entre el Proxy y los equipos cliente en una ubicación remota

Cómo configurar el HTTPS Proxy

Para usar el proxy, el nombre de host de HTTP Proxy debe configurarse en la Política del Agente (**Configuración avanzada** > **HTTP Proxy**). Puede utilizar diferentes proxies para almacenar en caché y reenviar. Vea la configuración de la política a continuación:

- **Proxy global**: utiizará una única solución proxy tanto para descargas de caché como para reenviar la comunicación del Agente.
- **Diferentes proxies por servicio**: utilizará distintas soluciones de proxy para el almacenamiento en caché y para reenviar la comunicación.

¿Qué otras funciones posee el Apache HTTP Proxy?



Apache HTTP Proxy

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

Para instalar Apache HTTP Proxy, lea las instrucciones para Windows, Linux o aparato virtual.

Funciones del Apache HTTP Proxy

Función	La solución proxy que proporciona esta función
Almacenamiento en caché de descargas y actualizaciones	Apache HTTP Proxy u otras soluciones proxy
Resultados del almacenamiento en caché de ESET LiveGuard Advanced	Únicamente Apache HTTP Proxyconfigurado
Replicación de la comunicación de los Agentes ESET Management con el Servidor ESET PROTECT	Apache HTTP Proxy u otras soluciones proxy

Función de almacenamiento en caché

Apache HTTP Proxydescargas y cachés:

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

- Actualizaciones de componentes del producto

Los datos en caché se distribuyen a los clientes de extremo en su red. El almacenamiento en caché puede disminuir significativamente el tráfico de Internet en su red

En comparación con la Herramienta de replicación, la cual descarga datos disponibles en los servidores de actualización ESET, Apache HTTP Proxy reduce la carga de la red, ya que solo descarga los datos que le solicitan los componentes ESET PROTECT o los productos de extremo ESET. Si un cliente final solicita una actualización, Apache HTTP Proxy la descarga desde los servidores de actualización ESET, guarda la actualización en el directorio de caché y luego lo entrega a cada cliente de extremo. Si otro cliente final solicita la misma actualización, Apache HTTP Proxy le entrega la descarga al cliente directamente desde el caché, por lo que no existe una descarga adicional desde los servidores de actualización ESET.

Almacenamiento en caché para productos de extremo de ESET

La configuración de almacenamiento en caché del Agente y el extremo ESET Management no es idénica. El Agente ESET Management puede administrar la configuración para los productos de seguridad ESET en los dispositivos de los clientes. Puede configurar proxy para ESET Endpoint Security:

- localmente desde GUI

- desde la consola web ESET PROTECT, utilizando una política (la manera recomendada de administrar las configuraciones de los dispositivos de los clientes)

Resultados del almacenamiento en caché de ESET LiveGuard Advanced

El Apache HTTP Proxy también puede almacenar en caché resultados proporcionados por ESET LiveGuard Advanced. El almacenamiento en caché requiere de una configuración específica, la cual está incluída en Apache HTTP Proxy y distribuída por el ESET. En caso de ser posible, se recomienda utilizar almacenamiento en caché con ESET LiveGuard Advanced. Vea la documentación del servicio para obtener más detalles.

Uso de Apache HTTP Proxy para la comunicación entre el Agente y el Servidor

Cuando se configura correctamente, Apache HTTP Proxy puede usarse para recolectar y reenviar datos desde los componentes de ESET PROTECT en una ubicación remota. Se puede utilizar una solución proxy para almacenar las actualizaciones en caché (se recomienda Apache HTTP Proxy) y otra proxy para la comunicación entre el Agente y el Servidor. Se puede utilizar Apache HTTP Proxy para ambas funciones simultáneamente, pero no se recomienda para redes con más de 10 000 equipos cliente por cada equipo proxy. Para los entornos empresariales (más de 1000 equipos administrados), recomendamos que use un servidor Apache HTTP Proxy dedicado.

Lea más sobre sobre la función del Proxy.

Cómo configurar el HTTPS Proxy

Para usar el proxy, el nombre de host de HTTP Proxy debe configurarse en la Política del Agente (**Configuración avanzada** > **HTTP Proxy**). Puede utilizar diferentes proxies para almacenar en caché y reenviar. Vea la configuración de la política a continuación:

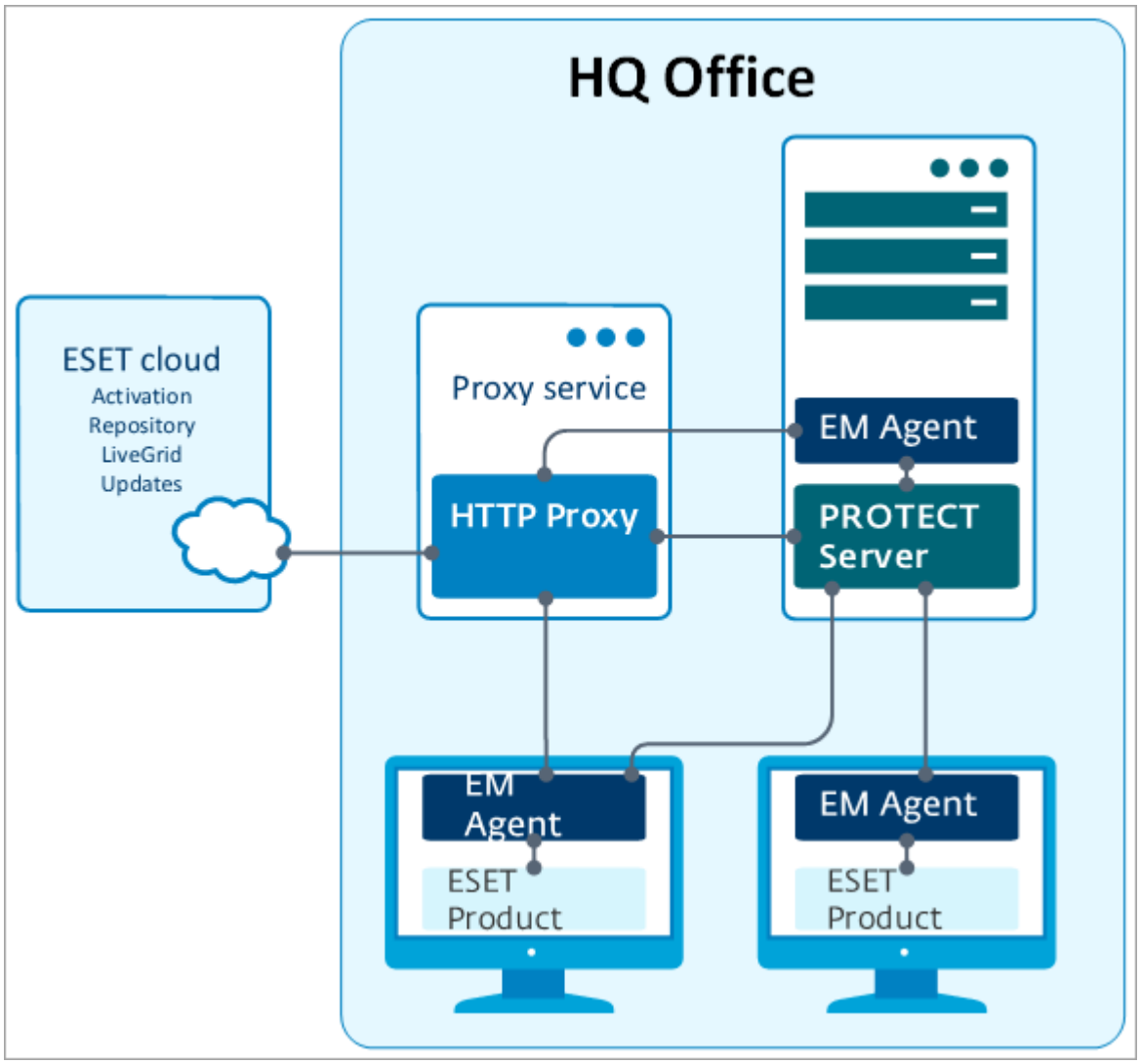
- **Proxy global**: utiizará una única solución proxy tanto para descargas de caché como para reenviar la

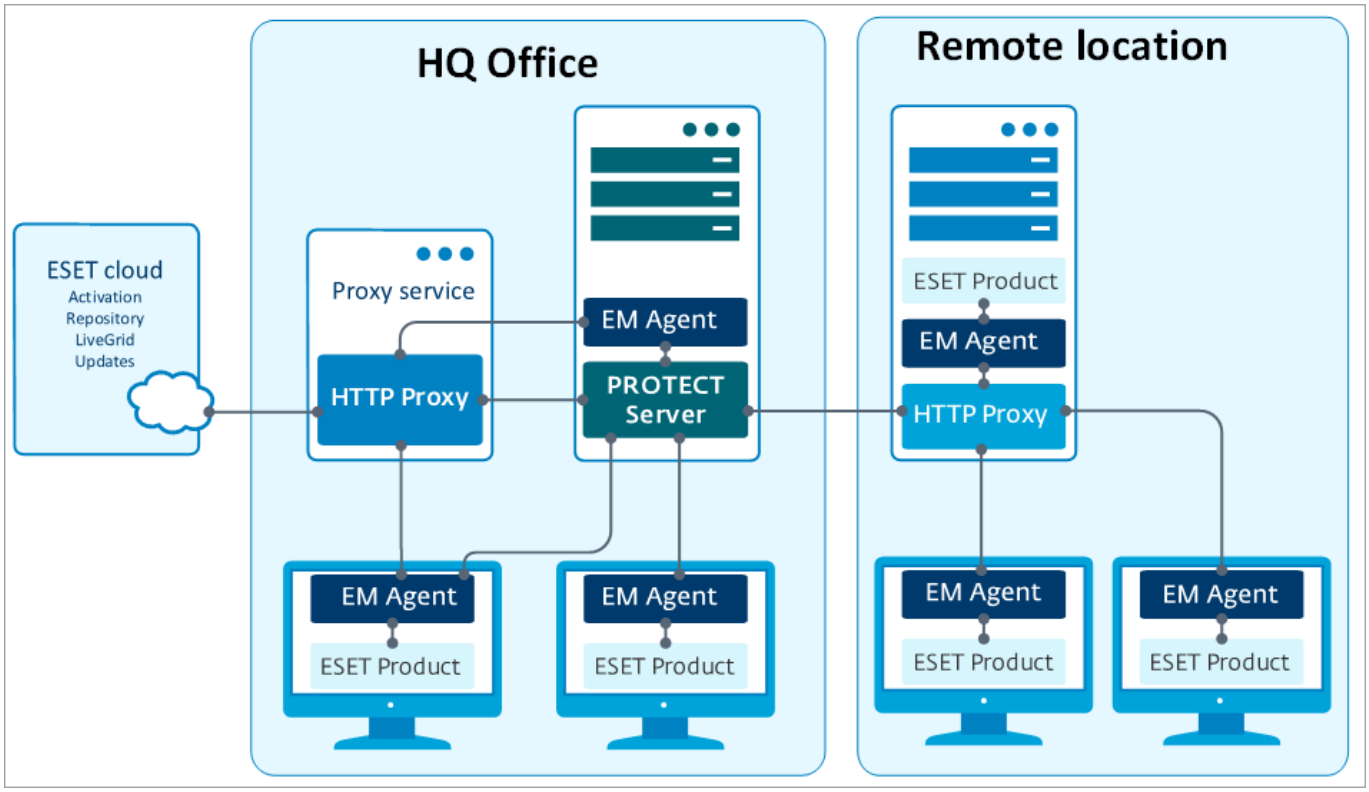
comunicación del Agente.

• **Diferentes proxies por servicio**: utilizará distintas soluciones de proxy para el almacenamiento en caché y para reenviar la comunicación.

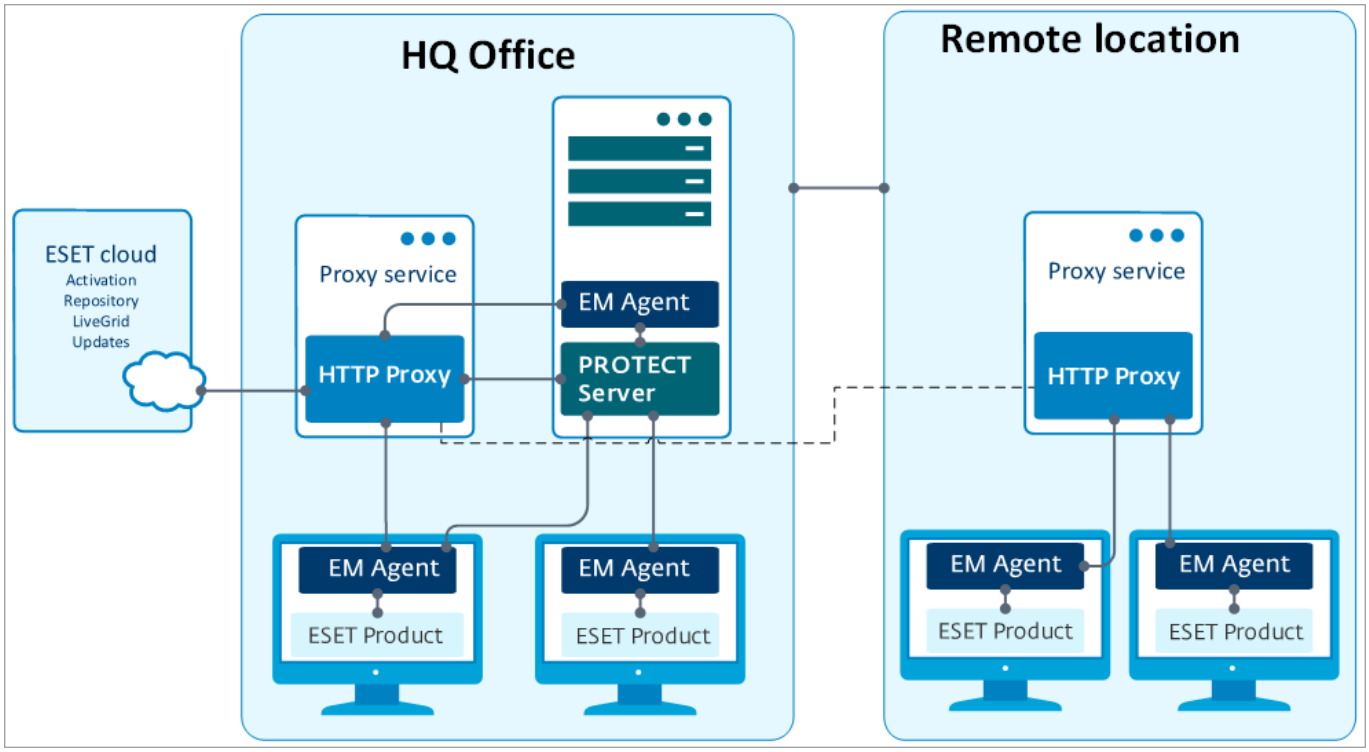
Apache HTTP Proxy y la infraestructura

El siguiente esquema ilustra un servidor proxy (Apache HTTP Proxy) usado para distribuir el tráfico de la nube ESET a todos los componentes de ESET PROTECT y productos de extremo de ESET.





Puede usar una cadena de proxy para agregar otro servicio de proxy a una ubicación remota. Tenga en cuenta que ESET PROTECT no admite el encadenamiento de proxies cuando estos requieren autenticación. Puede usar su propia solución proxy de red transparente; sin embargo, es posible que se requieran configuraciones adicionales además de las mencionadas aquí.



Para actualizaciones de motor de detección sin conexión, use la Herramienta de replicación (disponible para Windows y Linux) en lugar de Apache HTTP Proxy.

Agente

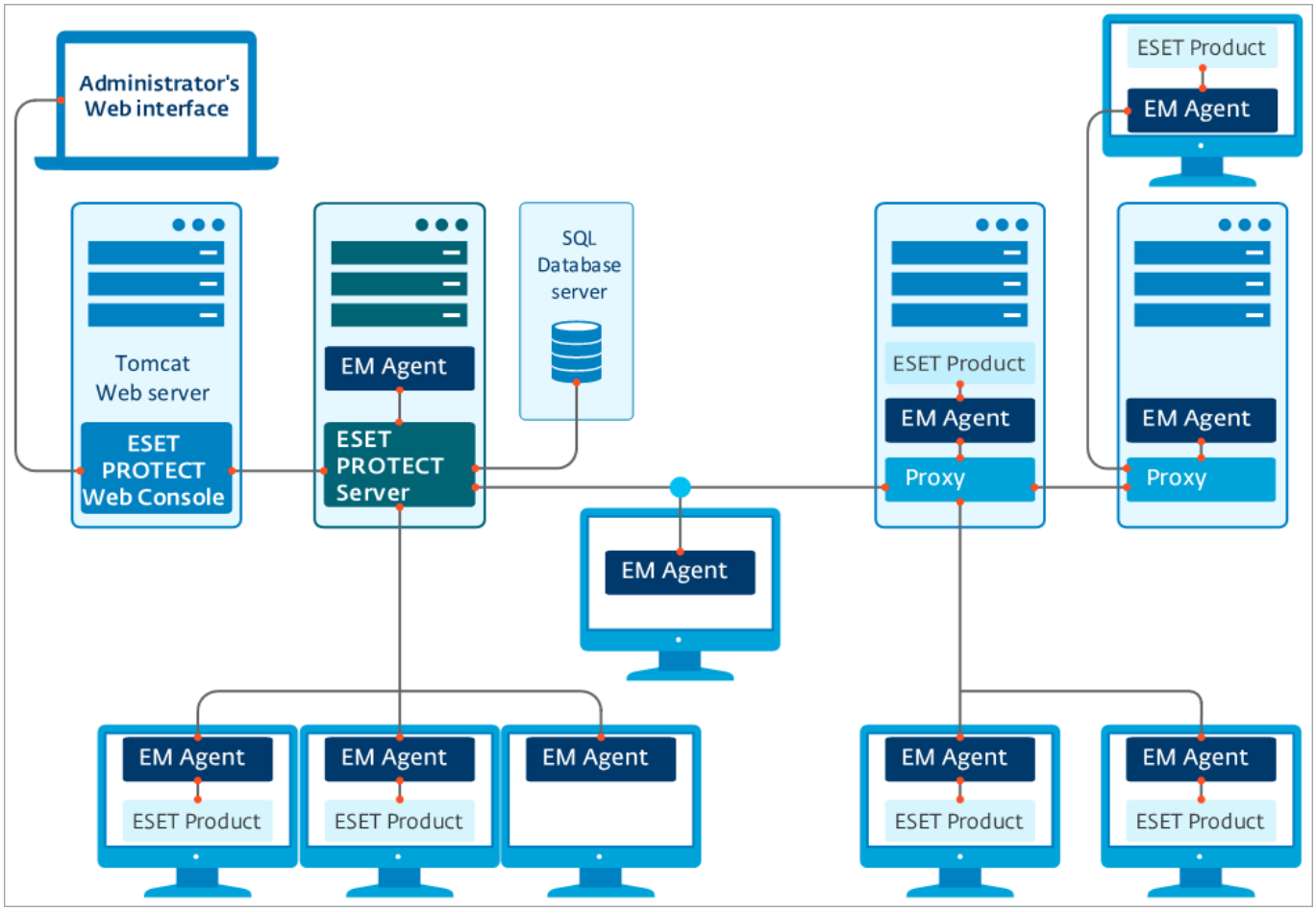
ElESET Management Agente es una parte esencial de ESET PROTECT. Los clientes no se comunican con el Servidor ESET PROTECT directamente, más bien el agente facilita esta comunicación. El Agente recopila la información del cliente y la envía al Servidor ESET PROTECT. Si el Servidor ESET PROTECT envía una tarea para el cliente, dicha tarea se envía al agente que, luego, la envía al cliente. El Agente ESET Management está usando un nuevo y mejorado protocolo de comunicación.

Para simplificar la implementación de la protección de terminales, el Agente ESET Management independiente está incluido en el conjunto de programas de ESET PROTECT. Es un servicio simple, altamente modular y ligero que abarca toda la comunicación entre el Servidor ESET PROTECT y cualquier producto o sistema operativo de ESET. En lugar de comunicarse directamente con el Servidor ESET PROTECT, los productos de ESET se comunican a través del Agente. Los equipos cliente que tienen el Agente ESET Management instalado y pueden comunicarse con el Servidor ESET PROTECT se denominan "administrados”. Puede instalar el agente en cualquier equipo sin importar si se ha instalado otro software de ESET.

Los beneficios son los siguientes:

- Fácil configuración: es posible implementar el Agente como parte de la instalación corporativa estándar.
- Administración de seguridad en el sitio: dado que el Agente se puede configurar para almacenar varios escenarios de seguridad, el tiempo de reacción frente a una detección se reduce de manera significativa.
- Administración de seguridad fuera de línea: el Agente puede responder a un suceso incluso si no está conectado al Servidor ESET PROTECT.

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



Sensor de Rogue Detection

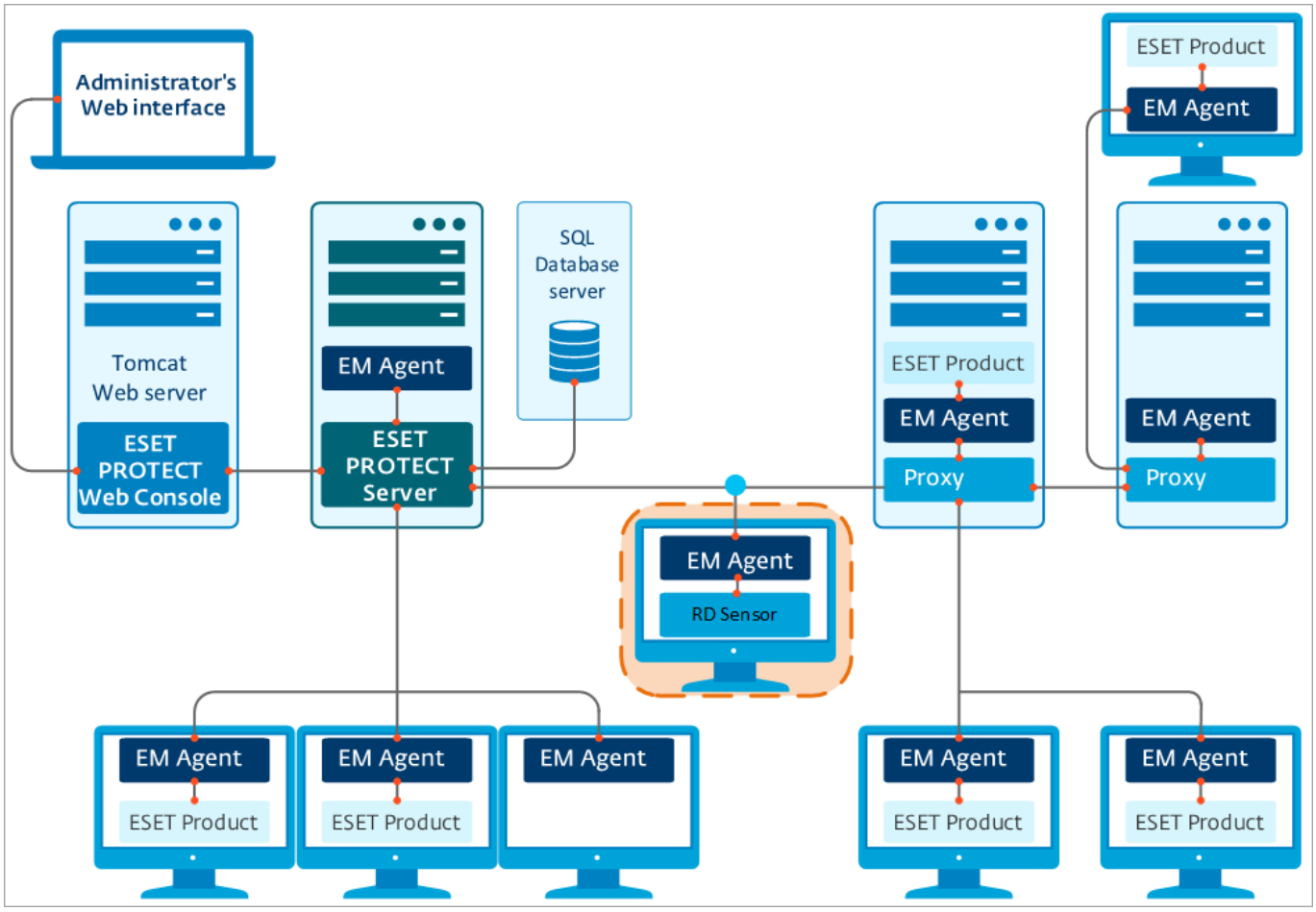
El Rogue Detection Sensor (RD Sensor) es una herramienta para la detección de sistemas no autorizados que examina su red en busca de equipos. El sensor es conveniente porque puede localizar equipos nuevos de ESET PROTECT sin la necesidad de buscarlos y agregarlos en forma manual. Las máquinas detectadas se ubican e informan inmediatamente en un informe predefinido, lo que le permite moverlas a grupos estáticos específicos y proceder con las tareas de administración.

RD Sensor detecta activamente las transmisiones ARP. Cuando RD Sensor detecta un nuevo componente de red activo, envía unidifusiones ARP, realiza la identificación mediante la huella digital del host (usando varios puertos) y envía al Servidor ESET PROTECT información sobre los equipos detectados. El Servidor ESET PROTECT evalúa luego si los equipos encontrados en la red son desconocidos para el Servidor ESET PROTECT o si ya están administrados.

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

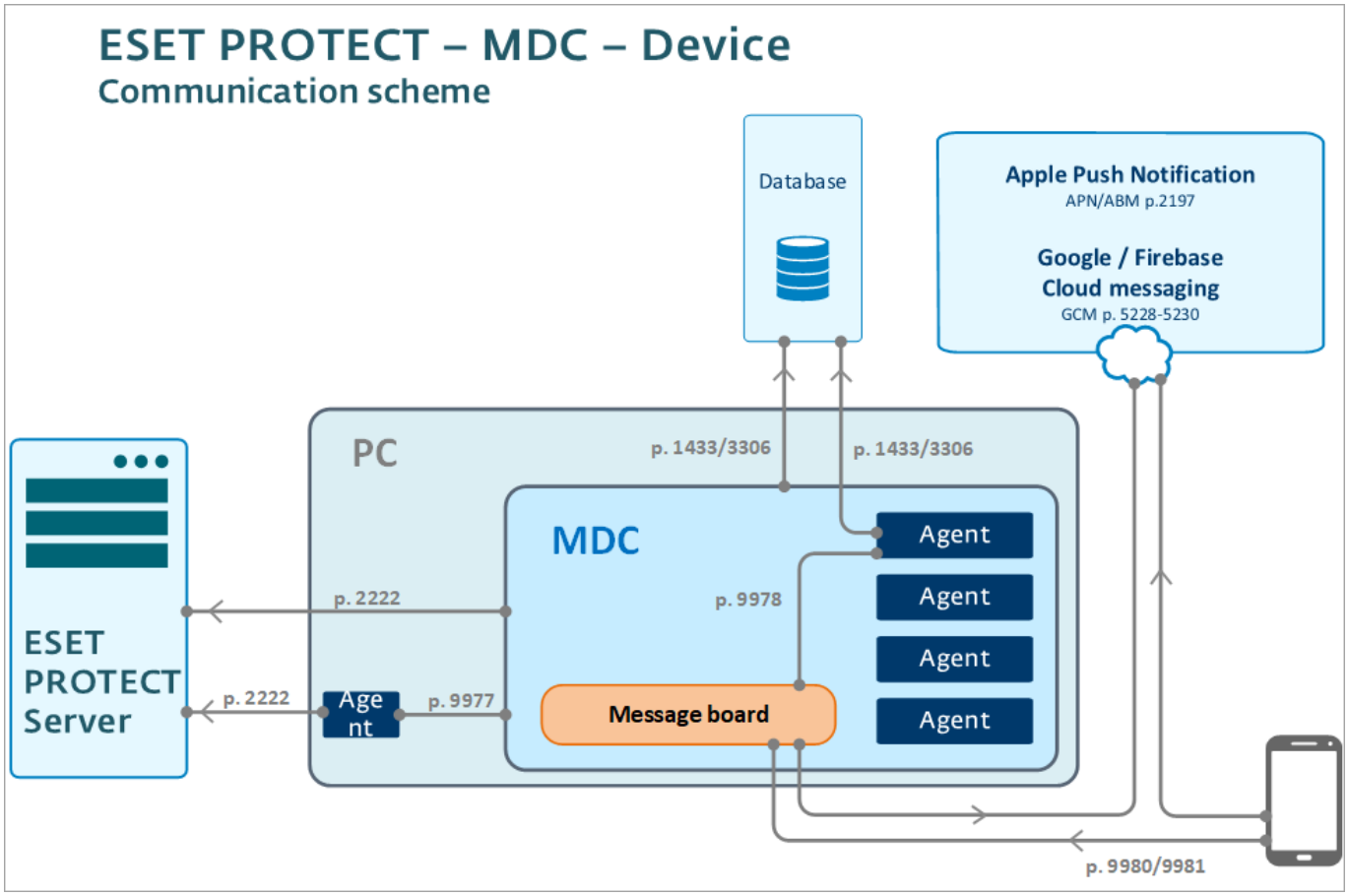
Si hay varios segmentos de red, Rogue Detection Sensor debe instalarse por separado en cada segmento de red para producir una lista completa de todos los dispositivos de toda la red.

Cada equipo dentro de la estructura de la red (dominio, LDAP, red de Windows) se agrega automáticamente a la lista de equipos del Servidor ESET PROTECT a través de una tarea de sincronización del servidor. Usar el RD Sensor es una forma conveniente de encontrar equipos que no están en el dominio o en otra estructura de la red y agregarlos al servidor de ESET PROTECT. El RD Sensor recuerda los equipos que ya han sido descubiertos y no enviará la misma información dos veces.



Conector de dispositivo móvil

El Conector de dispositivo móvil de ESET PROTECT es un componente que permite Administrar los dispositivos móviles con ESET PROTECT, lo que le permite gestionar dispositivos móviles (Android e iOS) y administrar ESET Endpoint Security para Android.



Ver la imagen más grande

> Le recomendamos que despliegue su componente MDM en un dispositivo host aparte de donde está alojado el Servidor de ESET PROTECT.

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

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

Para más de 80 dispositivos móviles, los requisitos de hardware no son mucho mayores. La latencia entre el envío de la tarea desde ESET PROTECT y la ejecución de la tarea en el dispositivo móvil se incrementará proporcionalmente a la cantidad de dispositivos en su entorno.

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

Diferencias entre proxy Apache HTTP, Herramienta de

replicación y conectividad directa

La comunicación de productos ESET involucra las actualizaciones del motor de detección y del módulo del programa, como también el intercambio de datos de ESET LiveGrid® (consulte la tabla a continuación) y la información de la licencia.

ESET PROTECT descarga los últimos productos para su distribución a equipos cliente desde el repositorio. Una vez distribuido, el producto está listo para ser implementado en el equipo de destino.

Una vez instalado un producto de seguridad ESTE, debe ser activado, lo que significa que el producto necesita verificar la información de la licencia con el servidor de licencias. Tras la activación, se actualizan los módulos del motor de detección y del programa de manera regular.

ESET LiveGrid®Early Warning System permite garantizar que ESET esté informado continuamente y de manera inmediata acerca de nuevas infiltraciones, para poder proteger a nuestros clientes rápidamente. El sistema permite que se envíen nuevas detecciones al Laboratorio de investigación de ESET, donde serán analizadas y procesadas.

La mayoría del tráfico de red se genera mediante las actualizaciones del módulo del programa. De manera general, el producto de seguridad ESET descarga aproximadamente 23,9 MB de actualizaciones del módulo en un 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 pueden almacenarse en caché.

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

Hay dos maneras de disminuir la carga de red cuando se distribuyen actualizaciones a una red de equipos, el Proxy Apache HTTP o la Herramienta de replicación (disponible para Windows y Linux).

> Lea este artículo de la base de conocimiento para configurar el encadenamiento de la herramienta de replicación (configure la herramienta de replicación para descargar actualizaciones desde otra herramienta de replicación).

Tipos de comunicación de ESET

Tipo de comunicación	Frecuencia de comunicación	Impacto del tráfico de red	Comunicación enviada por proxy	Opción de caché de proxy1	Opción de replicación2	Opción de entorno sin conexión
Implementación del agente (instaladores Push / Live desde el repositorio)	Una vez	Aproximadamente 50 MB por cliente	SÍ	SÍ3	NO	SÍ (GPO / SCCM, instaladores reales editados)4

Tipo de comunicación	Frecuencia de comunicación	Impacto del tráfico de red	Comunicación enviada por proxy	Opción de caché de proxy[1]	Opción de replicación[2]	Opción de entorno sin conexión
Instalación de extremo (instalación del software desde el repositorio)	Una vez	Aproximadamente 100 MB por cliente	SÍ	SÍ[3]	NO	SÍ (GPO / SCCM, instalación mediante la URL del paquete)[4]
Módulo del motor de detección module / Actualización del módulo del programa	más de 6 veces al día	23,9 MB por mes[5]	SÍ	SÍ	SÍ	SÍ (sin conexión Mirror Tool y servidor personalizado HTTP)[6]
Actualización del archivo de versión update.ver	aprox. 8 veces al día	2,6 MB por mes[7]	SÍ	NO	-	-
Activación / Verificación de licencia	4 veces al día	insignificante	SÍ	NO	NO	SÍ (archivos fuera de línea generados en ESET Business Account)[8]
Reputación basada en la nube de ESET LiveGrid®	En el momento	11 MB por mes	SÍ	NO	NO	NO

1.Para obtener información sobre impactos / beneficios del caché del proxy, consulte ¿Cuándo comenzar a usar el Proxy Apache HTTP?

2.Para obtener información sobre el impacto de la replicación, consulte ¿Cuándo comenzar a usar el Mirror Tool?

3.Le recomendamos implementar un agente/extremo una vez por instalación/actualización (uno por versión específica), para que el instalador se guarde en caché.

4.Para implementar el Agente ESET Management en una red amplia, consulte Implementación del agente mediante GPO y SCCM.

5.Es posible que la actualización inicial del motor de detección sea más grande de lo normal según la antigüedad del paquete de instalación, ya que se descargarán las nuevas actualizaciones del motor de detección y módulos. Le recomendamos instalar un cliente de manera inicial, y permitir que se actualice, para que se guarden las actualizaciones del motor de detección y del módulo del programa.

6.Sin conexión a internet, Mirror Tool no puede descargar las actualizaciones del motor de detección. Puede usar Apache Tomcat como servidor HTTP para descargar actualizaciones a un directorio disponible para la Herramienta de replicación (disponible para Windows y Linux).

7.Cuando verifique las actualizaciones del motor de detección, siempre se descarga y analiza el archivo *update.ver*. De manera predeterminada, las tareas programadas de los productos endpoint de ESET consultan una nueva actualización cada hora. Asumimos que la estación de trabajo del 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 puede guardar en el caché actualizaciones para los productos de la versión 4 y 5 mediante el Proxy Apache HTTP. Para distribuir actualizaciones para estos productos, use la Herramienta de replicación.

Cuándo comenzar a usar el proxy Apache HTTP

En base a las pruebas prácticas, recomendamos que implemente el proxy Apache HTTP si posee una red de 37 o más equipos.

Para realizar un caché efectivo, es fundamental que la hora y la fecha del servidor HTTP Proxy estén definidas correctamente. Las diferencias de unos minutos podrían provocar que el mecanismo de caché no funcione de manera efectiva y que se descarguen más archivos que los necesarios.

El análisis del ancho de banda de red usado solo por actualizaciones en una red de prueba de 1.000 equipos donde se realizaron numerosas instalaciones y desinstalaciones demostró lo siguiente:

- un equipo individual descarga 23,9 MB/mes en actualizaciones en promedio si se lo conecta directamente a Internet (sin utilizar un Proxy HTTP Apache)
- con uso del proxy Apache HTTP, las descargas de la red completa llegaron a un total de 900 MB/mes

Una comparación simple de los datos de actualizaciones descargadas en un mes con una conexión a internet directa o un proxy Apache HTTP en una red de equipos:

Número de equipos en la red empresarial	25	36	50	100	500	1.000
Conexión directa a internet (MB/mes)	375	900	1.250	2.500	12.500	25.000
Proxy Apache HTTP (MB/mes)	30	50	60	150	600	900

¿Cuándo comenzar a usar Mirror Tool?

Si posee un entorno sin conexión, es decir, que los equipos en la red no se conectan a Internet durante un período prolongado de tiempo (meses, un año), la Herramienta de replicación (disponible para Windows y Linux) es la única manera de distribuir las actualizaciones del módulo del producto, ya que descarga todas las actualizaciones de nivel y nano disponibles con cada solicitud de actualización nueva si hay una nueva actualización disponible.

i Lea este artículo de la base de conocimiento para configurar el encadenamiento de la herramienta de replicación (configure la herramienta de replicación para descargar actualizaciones desde otra herramienta de replicación).

La mayor diferencia entre el proxy Apache HTTP y la Herramienta de replicación es que el proxy Apache HTTP descarga solamente las actualizaciones faltantes (por ejemplo, actualización Nano 3), mientras que la Mirror Tool descarga todas las actualizaciones de nivel y Nano disponibles (o solo las actualizaciones de nivel, en caso de especificarse), independientemente de la actualización que le falte a un módulo del producto en particular.

Las actualizaciones streamed no están disponibles con la Herramienta de replicación. Se recomienda optar por la actualización a través del HTTP Proxy por sobre la replicación siempre que sea posible. Incluso si un equipo está en modo sin conexión, pero tiene acceso a otra máquina conectada a Internet y puede ejecutar un HTTP Proxy para poner en caché las actualizaciones de archivos, seleccione esta opción.

En la misma red de 1.000 equipos, evaluamos la Herramienta de replicación en lugar del proxy Apache HTTP. El análisis demostró que se descarga 5500 MB de actualizaciones al mes. El tamaño de las actualizaciones descargadas no aumentó al agregar más equipos a la red. Continúa siendo una disminución enorme de carga en comparación con la configuración donde los clientes se conectan directamente a Internet, pero la mejora en el rendimiento no es tan sustancial con cuando se usa el proxy HTTP.

N. º de equipos en la red empresarial	25	36	50	100	500	1.000
Conexión directa a internet (MB/mes)	375	900	1.250	2.500	12.500	25.000
Herramienta de replicación (MB/mes)	5.500	5500	5500	5500	5500	5.500

Incluso si hubiera más de 1.000 equipos en una red, el uso del ancho de banda respecto a las actualizaciones no aumentaría significativamente, ya sea con el uso del proxy HTTP o de la Herramienta de replicación.

Requisitos y dimensionamiento del sistema

Su sistema debe cumplir con una serie de requisitos previos de hardware, base de datos, red y software para instalar y utilizar ESET PROTECT.

Sistemas operativos compatibles

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

Windows

La siguiente tabla muestra 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	✔	✔	✔	✔

Sistema operativo	Servidor	Agente	RD Sensor	MDM
Windows Server 2012 CORE x64	✔	✔	✔	✔
Windows Server 2012 R2 x64	✔	✔	✔	✔
Windows Server 2012 R2 CORE x64	✔	✔	✔	✔
Windows Storage Server 2012 R2 x64	✔	✔	✔	✔
Windows Server 2016 x64	✔	✔	✔	✔
Windows Storage Server 2016 x64	✔	✔	✔	✔
Windows Server 2019 x64	✔	✔	✔	✔
Windows Server 2022 x64	✔	✔	✔	✔

Sistema operativo	Servidor	Agente	RD Sensor	MDM
Windows 7 x86 SP1 con las actualizaciones más recientes de Windows (al menos KB4474419 y KB4490628)		✔	✔	
Windows 7 x64 SP1 con las actualizaciones más recientes de Windows (al menos KB4474419 y KB4490628)		✔	✔	
Windows 8 x86		✔	✔	
Windows 8 x64	*	✔	✔	*
Windows 8.1 x86		✔	✔	
Windows 8.1 x64	*	✔	✔	*
Windows 10 x86		✔	✔	
Windows 10 x64 (todas las versiones oficiales)	*	✔	✔	*
Windows 10 en ARM		✔		
Windows 11 x64	*	✔	✔	*

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

En sistemas MS Windows más antiguos:
• Tenga siempre instalado el Service Pack más reciente, especialmente en sistemas más antiguos como Server 2008 y Windows 7.
• ESET PROTECT no admite la administración de equipos que ejecutan Windows 7 (sin SP), Widows Vista y Windows XP.
• A partir del 24 de marzo de 2020, ESET ya no será compatible de manera oficial ni brindará soporte técnico para ESET PROTECT (Aervidor y MDM) instalados en los siguientes sistemas operativos de Windows: Windows 7, Windows Server 2008 (todas las versiones).
No es compatible con sistemas operativos ilegales o pirateados.

Desde enero de 2019, las actualizaciones públicas de Oracle JAVA SE 8 para uso empresarial, comercial o de producción requieren una licencia comercial. Si no compra una suscripción de JAVA SE, puede pasar a una alternativa sin costo. Consulte las versiones compatibles de JDK.

Puede ejecutar ESET PROTECT en un sistema operativo sin servidor, sin la necesidad de ESXi. Instalar VMware Player en un Sistema operativo de escritorio e implementar el ESET PROTECTAparato virtual.

Linux

La siguiente tabla muestra 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	✔	✔	✔	✔

Sistema operativo	Servidor	Agente	RD Sensor	MDM
Debian 11 x64		✔	✔	
Oracle Linux 8		✔	✔	
Amazon Linux 2		✔	✔	

* Red Hat Entreprise Linux Server 8.x no es compatible con la generación de informes de *.pdf*; vea más detalles en Problemas conocidos de ESET PROTECT.

macOS

Sistema operativo	Agente
macOS 10.12 Sierra	✔
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 es compatible como cliente. El Agente ESET Management y los productos ESET para macOS se pueden instalar en macOS. Sin embargo, no se puede instalar el servidor ESET PROTECT en macOS.

Móvil

Sistema operativo	EESA	Propietario del dispositivo EESA	MDM iOS	ABM de MDM iOS
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+			✔	✔

Sistema operativo	EESA	Propietario del dispositivo EESA	MDM iOS	ABM de MDM iOS
iOS 14.x+			✔	✔
iOS 15			✔	✔
iOS 16			✔	✔
iPadOS 13.x+			✔	✔
iPadOS 14.x+			✔	✔
iPadOS 15			✔	✔

* iOS DEP sólo está disponible en algunos países.

Recomendamos que mantenga actualizado el SO de su dispositivo móvil con la última versión para continuar recibiendo parches de seguridad importantes.

Requisitos para iOS 10.3 y posterior:

Desde la versión de iOS 10.3, es posible que no se confíe automáticamente en una AC que no se instala como parte del perfil de inscripción. Para resolver este problema, siga estos pasos:
a)Use un certificado emitido por el emisor de certificados de confianza de Apple.
b)Instale el certificado de confianza manualmente antes de la inscripción. Esto significa que deberá instalar la raíz de AC manualmente en el dispositivo móvil antes de la inscripción y habilitar la plena confianza para el certificado instalado.

Requisitos para iOS 12:

Consulte 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)** a través del 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 de **al menos 2048 bits**. El algoritmo de hash del certificado debe ser **SHA-2 con una longitud de resumen**, (alguna veces denominado "huella digital") de al menos 256 (es decir, **SHA-256 o mayor**). Puede generar un certificado con estos requisitos en ESET PROTECT con Seguridad avanzada activada.
- Los certificados deben contener la **cadena completa de certificados, incluida la raíz de AC**. La raíz de AC incluida en el certificado se usa para establecer la confianza con los dispositivos y se instala como parte del perfil de inscripción de MDM.

Requisitos para iOS 13:

- La administración de dispositivos móviles con iOS 13 requiere del cumplimiento de los requisitos del nuevo certificado de comunicación de Apple (MDM HTTPS). Los certificados emitidos antes del 1 de julio de 2019 también deben cumplir con estos requisitos.
- El certificado de HTTPS firmado por ESMC CA no cumple con estos requisitos.

> Se recomienda de manera enfática que no actualice sus dispositivos móviles a la versión de iOS 13 antes de cumplir con los requisitos del certificado de comunicación de Apple. Dicha acción ocasionará que sus dispositivos dejen de conectarse a ESET PROTECT MDM.

- Si ya actualizó sin el certificado adecuado y sus dispositivos dejaron de conectarse a ESET PROTECT MDM, primero necesita cambiar el certificado HTTPS actual usado para la comunicación con dispositivos iOS por el certificado que cumple con los requisitos del certificado de comunicación de Apple (MDM HTTPS) y, después de eso, volver a registrar sus dispositivos iOS.
- Si no actualizó a la versión de iOS 13, asegúrese de que su certificado MDM HTTPS actual, que se usa para la comunicación con dispositivos iOS, cumpla con los requisitos del certificado de comunicación de Apple (MDM HTTPS). De lo contrario, puede continuar y actualizar sus dispositivos iOS a la versión iOS 13. Si no cumple con los requisitos, cambie el certificado MDM HTTPS actual por el certificado HTTPS que cumple con los requisitos del certificado de comunicación de Apple (MDM HTTPS) y continúe con la actualización de los dispositivos iOS a la versión iOS 13.

Entornos de suministro de escritorio compatibles

El suministro de escritorio facilita la gestión de dispositivos y brinda una transferencia más rápida de equipos de escritorio a usuarios finales.

Generalmente los escritorios con suministros son físicos o virtuales. Para los entornos virtualizados que usan el sistema operativo Streamed (servicios de suministro Citrix), consulte la lista de hipervisores compatibles.

ESET PROTECT es compatible con:

- sistemas con disco no persistente
- Entornos VDI
- identificación de equipos clonados

Hipervisores y extensiones del 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 a equipos físicos y virtuales)

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

Dimensionamiento del hardware y la infraestructura

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

Cantidad de clientes	ESET PROTECTServidor + servidor de la base de datos SQL				
	Núcleos de CPU	Velocidad del reloj de la CPU (GHz)	RAM (GB)	Unidad de disco1	IOPS2 de disco
Hasta 1.000	4	2.1	4	Individual	500
5.000	8	2.1	8		1.000
10,000 3	4	2.1	16	Separado	2.000
20.000	4	2.1	16		4.000
50.000	8	2.1	32		10.000
100.000	16	2.1	Más de 64		20.000

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

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

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

Cantidad de clientes	Comando
Hasta 5.000 clientes	`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 la situación de ejemplo para un entorno de 10 000 clientes.

Recomendaciones de unidad de disco

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

- La instancia del servidor SQL puede compartir recursos con el Servidor ESET PROTECT para maximizar el uso y minimizar la latencia. Ejecute el servidor de ESET PROTECT y el servidor de la base de datos en un solo equipo para aumentar el rendimiento de ESET PROTECT.
- El rendimiento de un servidor SQL mejora si ubica la base de datos y los archivos de registro de transacción en unidades separadas, preferentemente en unidades SSD físicas separadas.
- Si tiene una sola unidad de disco, le recomendamos usar una unidad SSD.
- Le recomendamos que utilice la arquitectura todo flash. Los discos sólidos (SSD) son mucho más rápidos que los HDD estándar.
- Si tiene una configuración de RAM alta, es suficiente configurar el SAS con R5. La configuración probada: 10 discos SAS de 1,2 TB en R5: dos grupos de paridad en 4+1 sin almacenamiento en caché adicional.
- El rendimiento no mejora cuando se utiliza una empresa de SSD nivel IOPS superior.
- La capacidad de 100 GB es suficiente para cualquier cantidad de clientes. Es probable que necesite una capacidad más elevada si realiza una copia de seguridad de la base de datos con frecuencia.
- No use una unidad de red porque el rendimiento de ESET PROTECT será más lento.
- Si tiene una infraestructura de almacenamiento de varios niveles que permite la migración del almacenamiento en línea, le recomendamos que empiece por compartir niveles más lentos y supervise el rendimiento de ESET PROTECT. Si nota que la latencia de lectura/escritura supera los 20 ms, puede realizar un traslado sin interrupciones de la capa de almacenamiento a un "mesón" más rápido para utilizar el backend más económico. Puede hacer lo mismo en un hipervisor (si utiliza ESET PROTECT como máquina virtual).

Recomendaciones de dimensionamiento para distintos recuentos de clientes

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

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

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

Recomendaciones de implementación

Mejores prácticas para la implementación de ESET PROTECT

Cantidad de clientes	Hasta 1.000	1.000 - 5.000	5.000 - 10.000	10.000 - 50.000	50.000 - 100.000	100 000+
ESET PROTECTEl Servidor y el Servidor de la base 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 Aparato virtual ESET PROTECT	✔	✔	No recomendado	X	X	X
Uso del servidor de VM	✔	✔	✔	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 (después de la implementación, durante el uso estándar)	10 minutos	10 minutos	20 minutos	30 minutos	40 minutos	60 minutos

* Para evitar llenar la base de datos ESET PROTECT, no recomendamos este escenario si también utiliza ESET Inspect.

Intervalo de conexión

El servidor de ESET PROTECT está conectado a los agentes de ESET Management con conexiones permanentes. A pesar de la conexión permanente, la transmisión de datos se produce solo 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 configurar el intervalo de conexión de clientes adecuado. Asegúrese de mantener la cantidad total de conexiones de agente y servidor por debajo de 1.000 por segundo incluso en configuraciones de hardware de alto rendimiento.

Cuando un servidor está sobrecargado o existe un brote de malware (por ejemplo, conectamos 20.000 clientes a un servidor que solo tiene capacidad para prestar servicio a 10.000 clientes a un intervalo de diez minutos), este omite algunos de los clientes que están conectados. Los clientes no conectados intentarán conectarse al Servidor ESET PROTECT más tarde.

Servidor único (empresa pequeña)

Para administrar redes pequeñas (1.000 clientes o menos) use un solo equipo con el servidor de ESET PROTECT y todos los componentes de ESET PROTECT instalados. En los entornos de SMB / redes pequeñas, recomendamos considerar la instalación ESET PROTECT de Linux o el aparato virtual, donde corresponda.

Sucursales remotas con proxies

Si los equipos del cliente no tienen visibilidad directa en el servidor de ESET PROTECT, use un proxy para reenviar la comunicación de productos ESET. El proxy HTTP no agrega la comunicación ni disminuye el tráfico de replicación.

Alta disponibilidad (empresarial)

En entornos empresariales (más de 10.000 clientes), tenga en cuenta lo siguiente:

- RD Sensor ayuda a buscar en su red y descubrir nuevos equipos.
- Puede instalar el servidor ESET PROTECT en un clúster de conmutación por error.
- Configure el proxy HTTP para una cantidad elevada de clientes.

Configuración de la consola web para soluciones empresariales o sistemas de bajo rendimiento

De manera predeterminada, la consola web de ESET PROTECT que se instala mediante el Instalador todo en uno para Windows reserva un límite de memoria de 1024 MB para Apache Tomcat.

Puede modificar la configuración predeterminada de la consola web según su infraestructura:

- En un entorno empresarial, la consola web predeterminada puede sufrir inestabilidad al trabajar con una gran cantidad de objetos. Cambie la configuración de Tomcat para evitar cortes de memoria. Antes de realizar estos cambios, asegúrese de que su sistema tenga RAM suficiente (16 GB o más).
- Si tiene un sistema de bajo rendimiento con recursos de hardware limitados, puede reducir el uso de la memoria de Tomcat.

> Los valores de memoria indicados a continuación son solo recomendaciones. Puede modificar los ajustes de memoria de Tomcat en función de sus recursos de hardware.

Windows

1. Abra *tomcat9w.exe* o ejecute la aplicación `Configure Tomcat`.
2. Cambie a la ficha **Java**.
3. Cambiar el uso de la memoria:
   a. Aumentar (empresarial): Cambie los valores **Pool de memoria inicial** a 2048 MB y **Pool de memoria máximo** a 16384 MB.
   b. Disminuir (sistemas de bajo rendimiento): Cambie los valores **Pool de memoria inicial** a 256 MB y **Pool de memoria máximo** a 2048 MB.
4. Reinicie el servicio Tomcat.

LINUX y aplicación virtual de ESET PROTECT

1.Abra la Terminal como root o use `sudo`.

2.Abra el archivo

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

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

3.Agregue la siguiente línea al archivo:

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

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

4.Guarde el archivo y reinicie el servicio de Tomcat.

```
service tomcat restart
```

Implementación para 10 000 clientes

A continuación, encontrará los resultados de rendimiento para un entorno virtual con 10 000 clientes en ejecución por un año.

Configuración del servidor de hipervisor

Componente	Valor
VMware	ESXi 6.7 Actualización 2 y posteriores (versión 15 de VM)
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 máquinas específicas
La base de datos y ESET PROTECT se ejecutan en máquinas virtuales separadas con configuraciones idénticas de hardware.

Software que se usa en máquinas virtuales

ESET PROTECT:

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

Base de datos:

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

Descripción del entorno de ESET PROTECT

- 10 000 clientes conectados
- Aproximadamente 2000 grupos dinámicos y 2000 plantillas para grupos dinámicos
- Aproximadamente 255 grupos estáticos
- 20 usuarios
- Intervalo de conexión de 15 minutos para agentes de ESET Management
- Una vez que el entorno ha estado en ejecución durante un año, el tamaño de la base de datos es 15 GB

Recuento de CPU	RAM (GB)	Rendimiento
8	64	Alto
4	32	Normal
2	16	Bajo
2	8	Muy bajo (No recomendado)

Base de datos

Especifique el servidor y el conector de la base de datos que desea usar cuando instala el servidor de ESET PROTECT. Puede usar un servidor de base de datos existente que actualmente se ejecute en su entorno, pero debe cumplir con los siguientes requisitos.

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

- Si usa una edición anterior de Windows (servidor 2012 o SBS 2011), Microsoft SQL Server Express 2014 se instalará de manera 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 de cada base de datos relacionada. No recomendamos el uso de Microsoft SQL Server Express:
- En entornos empresariales o redes de gran tamaño.
- Si desea usar ESET PROTECT con ESET Inspect.

Servidores de la base de datos y conectores de la base de datos compatibles

ESET PROTECT es compatible con dos tipos de servidores de la base de datos: Microsoft SQL Server eMySQL.

ESET PROTECT no admite MariaDB. MariaDB es una base de datos predeterminada en la mayoría de los entornos Linux actuales y se instala al seleccionar instalar MySQL.

Servidor de base de datos compatibles	Versiones de base de datos compatibles	Conectores de base de datos compatibles
Microsoft SQL Server	• Ediciones Exprés y No exprés • 2014, 2016, 2017, 2019	• Servidor SQL • Servidor de SQL cliente nativo 10.0 • Controlador ODBC para el servidor de SQL 11, 13, 17, 18
MySQL	• 5.6* • 5.7 • 8.0	Versiones de 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 actualizar su servidor de la base de datos de MySQL a la versión 5.7 y posterior.

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

Requisitos de hardware del servidor de la base de datos

Consulte las instrucciones sobre hardware y dimensionamiento.

Recomendaciones de rendimiento

Para tener un mejor rendimiento, le recomendamos que use la base de datos más reciente compatible con Microsoft SQL Server como la base de datos de ESET PROTECT. Aunque ESET PROTECT es compatible con MySQL, usar MySQL puede afectar en forma negativa el rendimiento del sistema al trabajar con grandes cantidades de datos, incluidos los tableros, las detecciones y los clientes. El mismo hardware con Microsoft SQL Server puede manejar una cantidad considerablemente mayor de clientes que con MySQL.

Puede decidir si instala un servidor de la base de datos de SQL en:

- El mismo equipo que el servidor de ESET PROTECT.
- El mismo equipo, pero en otro disco.
- Un servidor específico para la instalación de un servidor de la base de datos de SQL.

Recomendamos que use un equipo o varios con recursos dedicados si desea administrar más de 10.000 clientes.

Base de datos	Cliente SMB	Cliente empresarial	Límite de clientes	Windows	Linux
MS SQL Express	✔	(opcional)	5.000	✔	

Base de datos	Cliente SMB	Cliente empresarial	Límite de clientes	Windows	Linux
Servidor MS SQL	✔	✔	Ninguno	✔	
MySQL	✔	✔	10.000	✔	✔

Información adicional

El servidor ESET PROTECT no usa una copia de seguridad integrada. Recomendamos especialmente realizar una copia de seguridad de su servidor de base de datos para prevenir la pérdida de datos.

- No instale SQL Server en un controlador de dominio (por ejemplo, Windows SBS/Essentials). Recomendamos que instale ESET PROTECT en un servidor diferente o que no seleccione el componente SQL Server Express durante la instalación (esto requiere que use un SQL Server o un MySQL existente para ejecutar la base de datos ESET PROTECT).

- Si planea usar la cuenta de usuario con base de datos dedicada que tendrá acceso solo a la base de datos ESET PROTECT, debe 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 que será usada por ESET PROTECT.

- Consulte las instrucciones de instalación y configuración de MySQL para Windows y MySQL para Linux para trabajar correctamente con ESET PROTECT.

- MS SQL Server en Linux no es compatible. Sin embargo, puede conectar el servidor de ESET PROTECT en Linux con el Servidor MS SQL en Windows.

- Si instala el servidor de ESET PROTECT y MS SQL Server en equipos diferentes, puede habilitar una conexión cifrada a la base de datos.

- La configuración del 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 la consola web de ESET PROTECT.

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 las versiones alfa/beta/RC de ApacheTomcat.

Java

Apache Tomcat requiere Java/OpenJDK de 64 bits.

Si tiene muchas versiones de Java instaladas en su sistema, le recomendamos desinstalar las versiones anteriores de Java y solo dejar la última versión 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 pasar a una alternativa sin costo. Consulte las versiones compatibles de JDK.

Navegadores web, productos de seguridad ESET, e idiomas compatibles

Los siguientes sistemas operativos son compatibles con ESET PROTECT:

- Windows, Linux y macOS

La consola web ESET PROTECT se puede ejecutar en los siguientes navegadores web:

Navegador web
Mozilla Firefox
Microsoft Edge
Google Chrome
Safari
Opera

Para vivir la mejor experiencia con la consola web de ESET PROTECT, le recomendamos que tenga actualizados los navegadores web.

Si usa Internet Explorer, la consola web de ESET PROTECT le informará que está usando un navegador web no compatible.

Últimas versiones de productos ESET que se pueden administrar mediante 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
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 para Linux	7.x, 8.x

Producto	Versión del producto
ESET Server Security para Linux	8.1+
ESET Endpoint Antivirus para 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	

Últimas versiones de productos ESET que se pueden administrar mediante 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 estos productos con el agente ESET Management 9. Para administrar el producto, use el agente ESET Management 8.1 o una versión anterior.

Las versiones de productos de seguridad ESET anteriores a las de la tabla de arriba no son administrables con ESET PROTECT 9.
Para obtener más información sobre la compatibilidad, visite la Política de Fin de Vida Útil para productos comerciales de ESET.

Productos compatibles con la activación mediante 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 iOS de Apple	7.0
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

Producto de ESET	Disponible desde la versión
ESET Mail Security para IBM Domino	7.0
ESET Security para Microsoft SharePoint Server	7.0
ESET File Security para Linux	7.0
ESET Endpoint Antivirus para 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
Indonesian (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 el producto está disponible en este idioma; no hay ayuda en línea disponible.

Red

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

Los equipos administrados por ESET PROTECT deben estar conectados al mismo LAN y/o se deben encontrar en el mismo dominio de *Active Directory* que su Servidor ESET PROTECT. El Servidor ESET PROTECT debe ser visible para los equipos cliente. Además, los equipos cliente deben comunicarse con su Servidor ESET PROTECT para usar la implementación remota y la función de llamada de reactivación.

ESET PROTECT para Windows/Linux es compatible con los protocolos de Internet IPv4 y IPv6. El Aparato Virtual ESET PROTECT es compatible solo con IPv4.

Puertos usados

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

Impacto del tráfico de red por la comunicación del Servidor ESET PROTECT y el Agente ESET Management

Las aplicaciones en los equipos cliente no se comunican con el Servidor ESET PROTECT directamente, el Agente ESET Management facilita esta comunicación. Esta solución es más sencilla de administrar y menos exigente sobre los datos transferidos por red. El tráfico de red depende del intervalo de conexión del cliente y los tipos de tareas que los clientes realizan. Incluso si ninguna tarea se ejecuta ni programa en un cliente, el Agente ESET Management se comunica con el Servidor ESET PROTECT una vez en cada intervalo de conexión. Cada conexión genera tráfico. Consulte la siguiente tabla para obtener ejemplos de tráfico:

Tipo de acción	Tráfico en un único intervalo de conexión
Tarea del cliente: Explorar sin desinfectar	4 kB
Tarea del cliente: Actualización de módulos	4 kB
Tarea del cliente: Solicitud de registro de SysInspector	300 kB
Política Antivirus - Máxima seguridad	26 kB

ESET ManagementIntervalo de replicación del Agente	Tráfico diario generado por el Agente ESET Management inactivo
1 minuto	16 MB
15 minutos	1 MB
30 minutos	0,5 MB
1 hora	144 kB
1 día	12 kB

Para calcular el tráfico general generado por los Agentes ESET Management, use la siguiente fórmula:

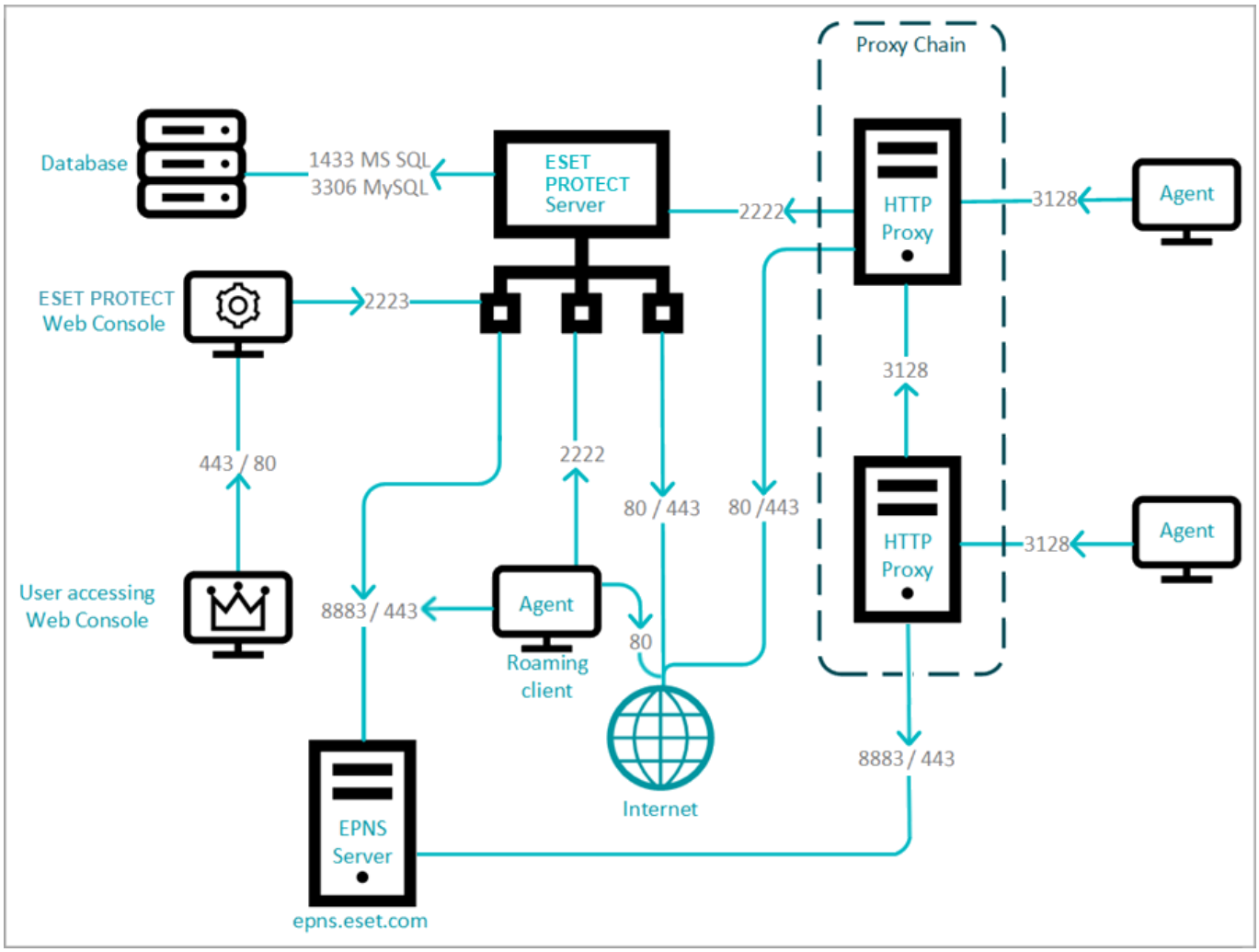
*Cantidad de clientes * (Tráfico diario de agente inactivo + (Tráfico para una tarea específica * incidencia diaria de*

la tarea))

Si utiliza el ESET Inspect, el Connector ESET Inspect genera un tráfico diario de 2 a 5 MB (varía en función de la cantidad de eventos).

Puertos usados

El Servidor ESET PROTECT puede instalarse en el mismo equipo que la base de datos, la Consola web ESET PROTECT y el Apache HTTP Proxy. El siguiente diagrama muestra la instalación separada y los puertos utilizados (las flechas indican el tráfico de red):



Las siguientes tablas enumeran los posibles puertos de comunicación usados cuando ESET PROTECT y sus componentes se instalan en la infraestructura. Otras comunicaciones se llevan a cabo por medio de los procesos del sistema operativo nativo (por ejemplo, NetBIOS sobre TCP/IP).

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

Equipo del cliente (Agente ESET Management) o de Apache HTTP Proxy

Protocolo	Puerto	Descripciones
TCP	2222	Comunicación entre los Agentes ESET Management y Servidor ESET PROTECT
TCP	80	Conexión al repositorio de ESET
MQTT	8883, 443	ESET Push Notification Service: llamadas de reactivación entre el servidor ESET PROTECT y el agente ESET Management, 443 es el puerto de conmutación por error.
TCP	3128	Comunicaciones con Apache HTTP Proxy
TCP	443	Comunicación con ESET LiveGuard Advanced (solo Proxy)

Agente ESET Management: puertos usados para la instalación remota del agente en un equipo de destino con sistema operativo Windows

Protocolo	Puerto	Descripciones
TCP	139	Usar el recurso compartido ADMIN$
TCP	445	Acceso directo a los recursos compartidos por medio de TCP/IP durante la instalación remota (una alternativa a TCP 139)
UDP	137	Resolución del nombre durante la instalación remota
UDP	138	Examinar durante la instalación remota

El equipo de la Consola web ESET PROTECT (si no es el mismo que el equipo del Servidor ESET PROTECT)

Protocolo	Puerto	Descripciones
TCP	2223	Comunicación entre la Consola web ESET PROTECT y el Servidor ESET PROTECT, usada para la Instalación asistida.
TCP	443/80	Tomcat transmitiendo la Consola web.
TCP	443	Fuente RSS para noticias de soporte: • https://era.welivesecurity.com:443 • https://support.eset.com:443/rss/news.xml

Equipo del Servidor ESET PROTECT

Protocolo	Puerto	Descripciones
TCP	2222	Comunicación entre el Agente ESET Management y el Servidor ESET PROTECT
TCP	80	Conexión al repositorio de ESET
MQTT	8883	Servicio de notificaciones push de ESET - Llamadas de reactivación entre el Servidor ESET PROTECT y el Agente ESET Management
TCP	2223	Resolución de DNS y reserva de MQTT
TCP	3128	Comunicaciones con Apache HTTP Proxy
TCP	1433 (MS SQL) 3306 (MySQL)	Conexión con una base de datos externa (solo si la base de datos se encuentra en otro equipo).
TCP	389	Sincronización de LDAP. Abrir también este puerto en su controlador AD.
UDP	88	Tickets de Kerberos (aplica únicamente al aparato virtual de ESET PROTECT)

Rogue Detection (RD) Sensor

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

Equipo del MDC ESET PROTECT

Protocolo	Puerto	Descripciones
TCP	9977 9978	Comunicación **interna** entre el conector de dispositivo móvil y el Agente ESET Management
TCP	9980	Inscripción de dispositivos móviles
TCP	9981	Comunicación del dispositivo móvil
TCP	2195	Envío de notificaciones a servicios de notificaciones push de Apple. (*gateway.push.apple.com*) hasta ESMC versión 7.2.11.1
TCP	2196	Servicio de comentarios de Apple (*feedback.push.apple.com*) hasta ESMC versión 7.2.11.1
HTTPS	2197	• Notificación push de Apple y comentarios (*api.push.apple.com*) ESMCversión 7.2.11.3 y posteriores.
TCP	2222	Comunicaciones (replicación) entre el Agente ESET Management, MDC y el Servidor ESET PROTECT
TCP	1433 (MS SQL) 3306 (MySQL)	Conexión con una base de datos externa (solo si la base de datos se encuentra en otro equipo)

Dispositivo MDM gestionado

Protocolo	Puerto	Descripciones
TCP	9980	Inscripción de dispositivos móviles
TCP	9981	Comunicación del dispositivo móvil
TCP	5223	Comunicación externa con los servicios de notificaciones push de Apple (iOS)
TCP	443	• Reserva solo con wifi, cuando los dispositivos no pueden llegar a los APN en el puerto 5223. (iOS) • Conexión del dispositivo Android con el servidor GCM. • Conexión con el 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*) • Categorización de aplicaciones instaladas en el dispositivo. Se utilizó para el control de aplicacionescuando se definió el bloqueo de algunas categorías de aplicaciones. (Android) (*https://play.eset.com*) • Para enviar una solicitud de soporte utilizando la función de solicitud de soporte (Android) (*https://suppreq.eset.eu*)
TCP	5228 5229 5230	Enviar notificaciones a Google Cloud Messaging(Android)* Enviar notificaciones a Firebase Cloud Messaging (Android)*
TCP	80	• Actualización de módulos (Android) (*http://update.eset.com*) • Utilizado solo en la versión web. Información sobre la última actualización de la versión de la aplicación y la descarga de una nueva versión. (Android) (*http://go.eset.eu*)

* El servicio GCM (Google Cloud Messaging) está en desuso y se eliminó a partir del 11 de abril de 2019. Se reemplazó por FCM (Firebase Cloud Messaging). Para esta fecha, MDM v7 reemplazó el servicio GCM con el servicio FCM y solo necesita permitir la comunicación para el servicio FCM.

Los puertos predefinidos 2222 y 2223 pueden modificarse en caso de que sea necesario.

Proceso de instalación

La guía de instalación cubre diversas maneras de instalar ESET PROTECT y está orientada principalmente a los clientes empresariales. Consulte la guía de pequeñas y medianas empresas si desea instalar ESET PROTECT en una plataforma Windows para administrar hasta 250 productos de terminales Windows ESET. Para obtener instrucciones para actualizar la instalación de ESET PROTECT existente, consulte los Procedimientos de actualización.

Los instaladores de ESET PROTECT están disponibles en la sección Descargar ESET PROTECT del sitio web de ESET. Hay diferentes formatos disponibles para soportar diferentes métodos de instalación. Está seleccionada la pestaña de **Instalador Todo en uno** de manera predeterminada. Haga clic en la pestaña adecuada para descargar un VA o un instalador independiente. Se encuentran disponibles las siguientes descargas:

- El paquete ESET PROTECT instalador todo en uno para Windows en formato zip.
- Una imagen ISO que contiene todos los instaladores de ESET PROTECT (excepto Aparatos virtuales ESET PROTECT).
- Aparatos virtuales (archivos OVA). Se recomienda la implementación del Aparato virtual ESET PROTECT

para los usuarios que desean ejecutar ESET PROTECT en un entorno virtualizado o prefieren la instalación sin problemas. Consulte nuestra completa guía de implementación de aparatos virtuales ESET PROTECT para obtener instrucciones detalladas.

- Instaladores individuales para cada componente : para las plataformas Windows y Linux.

Métodos adicionales de instalación:

- Instalación en Microsoft Azure
- Instrucciones de instalación detalladas para Linux

No cambie el nombre del equipo del Servidor ESET PROTECT después de la instalación. Para más información, consulte cambio de dirección IP o nombre de host en un Servidor ESET PROTECT.

Si desea elegir que clase de instalación de ESET PROTECT es la adecuada para su entorno, consulte la tabla de decisiones a continuación que lo guiará a la mejor elección: Por ejemplo:

- No use una conexión a Internet lenta para ESET PROTECT en la nube.
- Elija un instalador todo en uno si es un cliente SMB.

Consulte también Dimensionamiento del hardware y la infraestructura.

Método de instalación	Tipo de cliente		Migración		Entorno para la instalación ESET PROTECT					Conexión a Internet		
	SMB	Empresa	Sí	No	Sin servidor	Servidor dedicado	Servidor compartido	Plataforma de virtualización	Servidor en la nube	Ninguno	Bueno	Malo
Todo en uno en Servidor Windows	✓	✓	✓			✓	✓		✓	✓	✓	✓
Todo en uno en Escritorio Windows	✓		✓		✓					✓	✓	✓
Aparato virtual	✓		✓					✓		✓	✓	✓
Microsoft Azure VM	✓			✓					✓		✓	
Componente Linux		✓	✓			✓	✓		✓	✓	✓	✓
Componente de 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 simple es usar el instalador todo en uno ESET PROTECT. Este método le permite instalar ESET PROTECT y sus componentes en una sola máquina.

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

Puede instalar ESET PROTECT mediante:

- Paquete de instalación todo en uno del Servidor ESET PROTECT, Proxy, Proxy de Apache HTTP o Conector

de dispositivo móvil

- Instaladores independientes para los componentes ESET PROTECT (instalación de componentes)

Los escenarios de instalación personalizados incluyen:

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

En la mayoría de los escenarios de instalación, debe instalar diferentes componentes de ESET PROTECT en distintas máquinas para admitir las arquitecturas de red, cumplir con los requisitos de rendimiento, o por otros motivos. Los siguientes paquetes de instalación están disponibles para componentes individuales de ESET PROTECT:

Instalación de componentes principales

- Servidor ESET PROTECT
- Consola web ESET PROTECT – Puede instalar la consola web de ESET PROTECT en un equipo diferente a donde se ejecuta el servidor de ESET PROTECT.
- Agente ESET Management (debe estar instalado en los equipos cliente, es opcional en el caso del Servidor ESET PROTECT)

Instalación de componentes opcionales

- RD Sensor
- Conector de dispositivo móvil
- Apache HTTP Proxy
- Herramienta de replicación

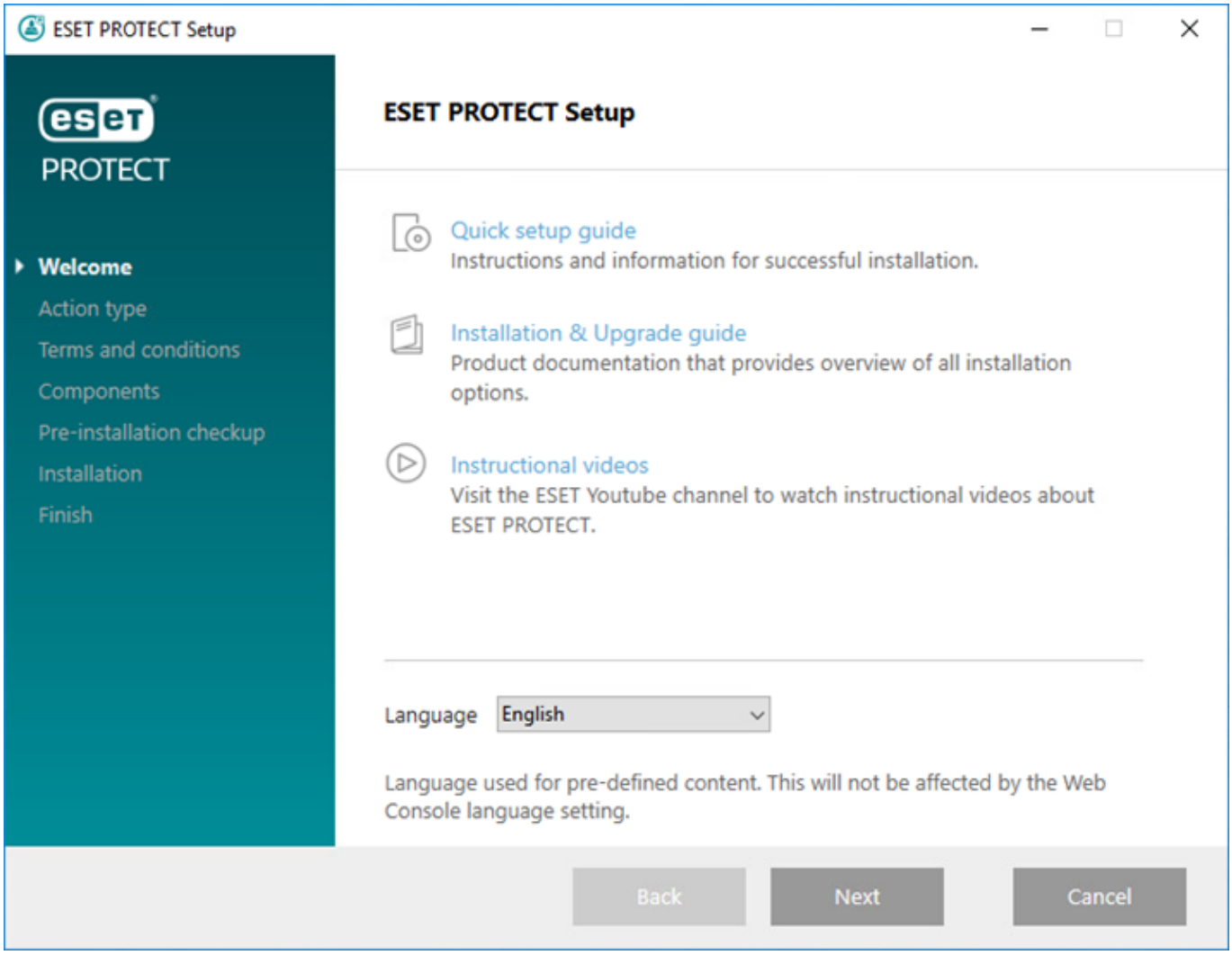
Consulte también la Instalación todo en uno de ESET PROTECT.

Para más información sobre cómo actualizar ESMC a la última versión de ESET PROTECT 9.1, consulte nuestros procedimientos de actualización.

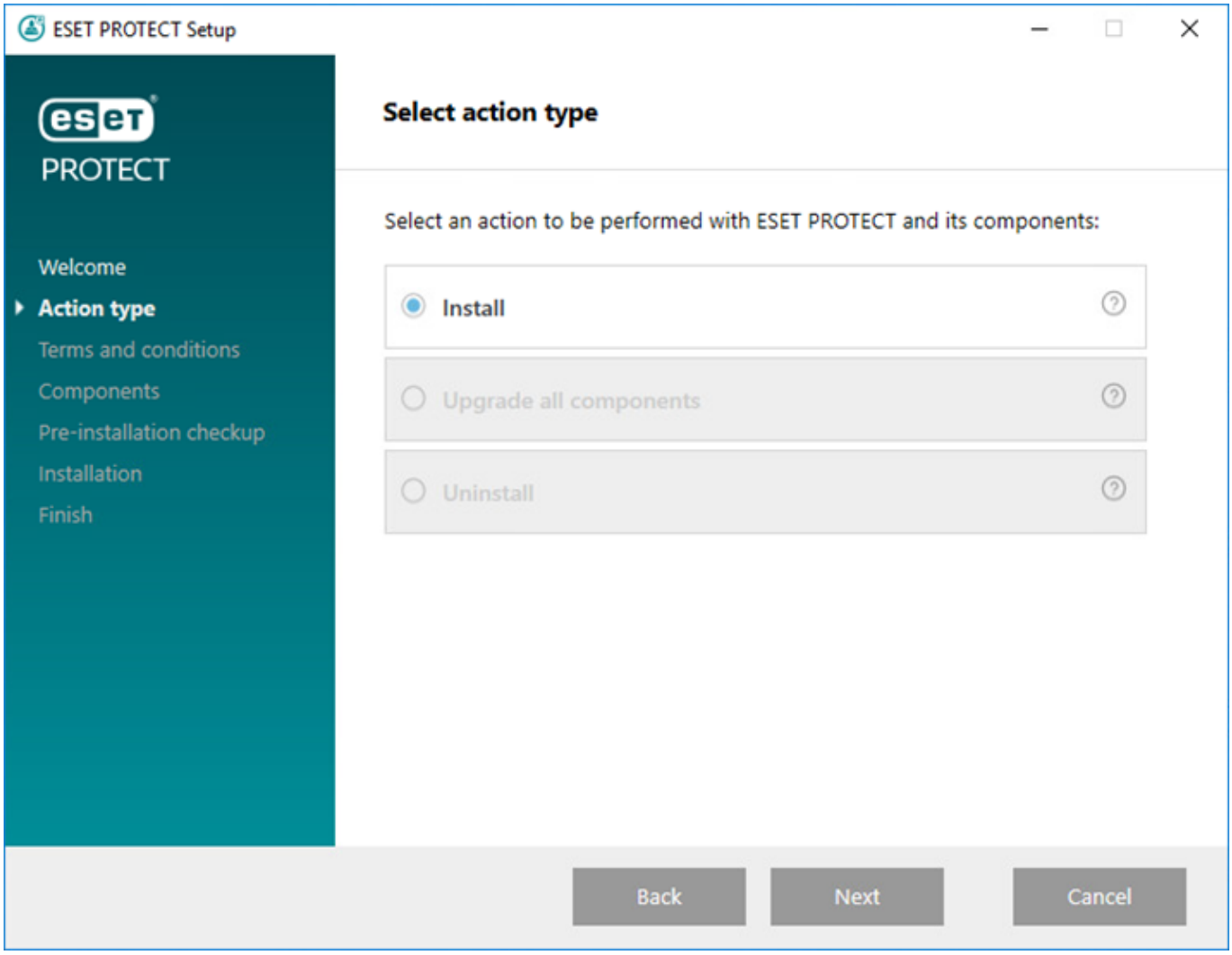
Instalar el servidor ESET PROTECT

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

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



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



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

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

Microsoft SQL Server Express

- El Instalador todo en uno de ESET PROTECT 9.1 instala Microsoft SQL Server Express 2019 de manera predeterminada.
  - Si usa una edición anterior de Windows (servidor 2012 o SBS 2011), Microsoft SQL Server Express 2014 se instalará de manera 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 de cada base de datos relacionada. No recomendamos el uso de Microsoft SQL Server Express:
> - En entornos empresariales o redes de gran tamaño.
> - Si desea usar ESET PROTECT con ESET Inspect.

- Si ya tiene instalada otra versión compatible de Microsoft SQL Server o MySQL o si planea conectarse a un SQL Server diferente, quite la marca de la casilla junto a **Microsoft SQL Server Express**.
- No instale SQL Server en un controlador de dominio (por ejemplo, Windows SBS/Essentials). Recomendamos que instale ESET PROTECT en un servidor diferente o que no seleccione el componente SQL Server Express durante la instalación (esto requiere que use un SQL Server o un MySQL existente para ejecutar la base de datos ESET PROTECT).

Agregar un certificado HTTPS personalizado para la consola web

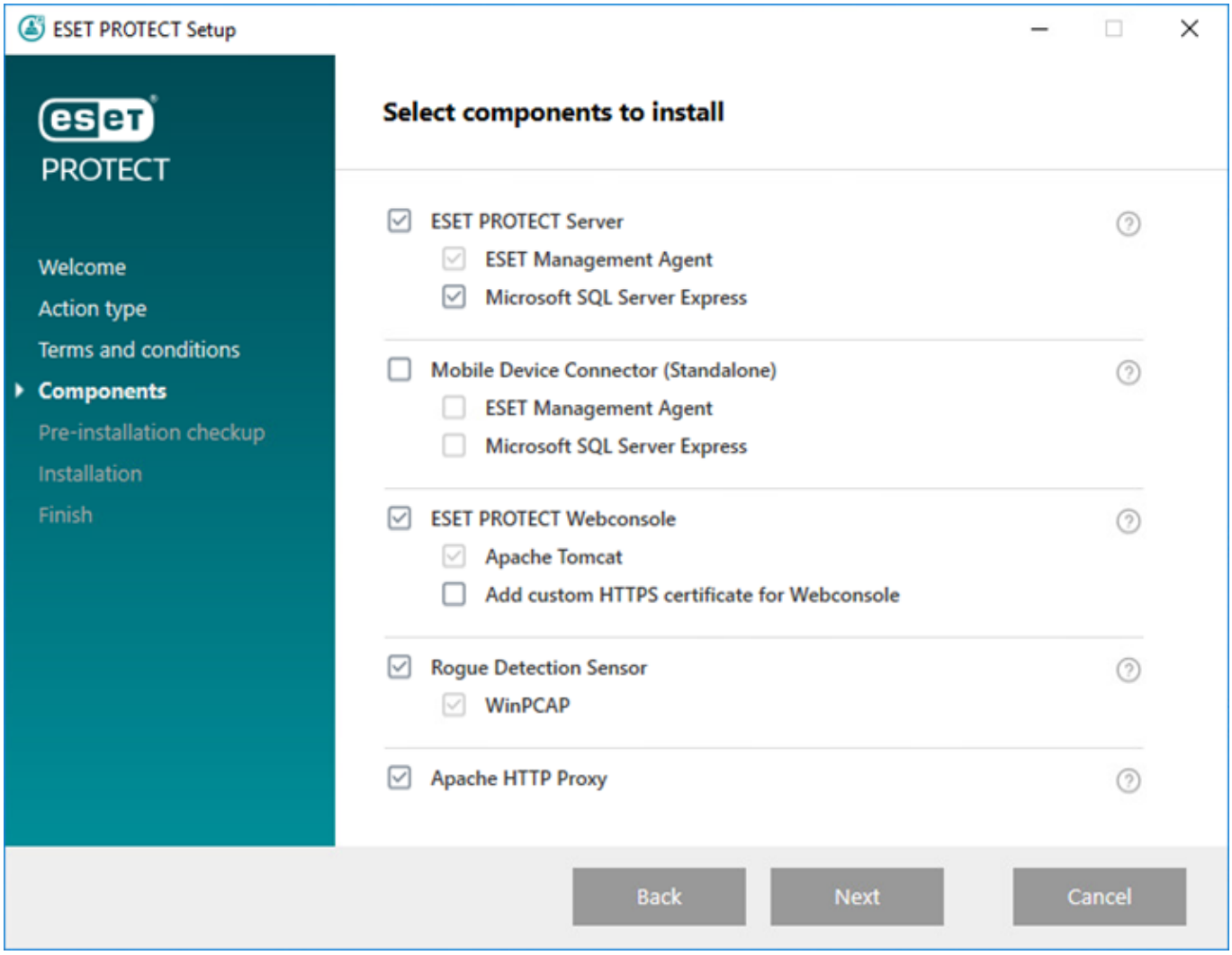
- Seleccione esta opción si desea agregar un certificado HTTPS personalizado para la consola web de ESET PROTECT.
- Si no selecciona esta opción, el instalador genera automáticamente un nuevo almacén de claves para Tomcat (un certificado de HTTPS autofirmado).

Apache HTTP Proxy

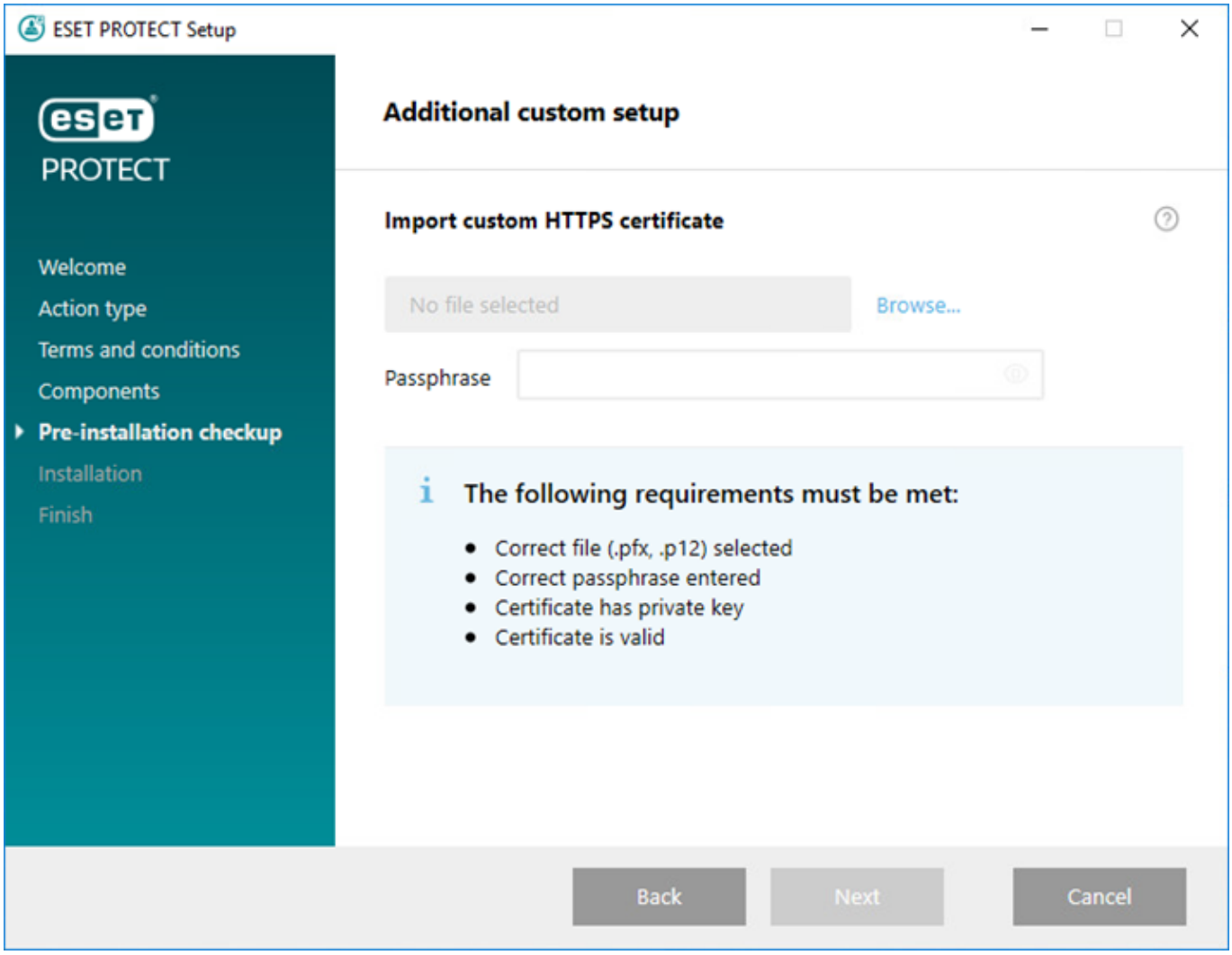
> La opción **Proxy HTTP Apache** está destinada únicamente para redes más pequeñas o centralizadas, sin clientes de itinerancia. Si selecciona esta opción, el instalador configura los clientes para la comunicación a través de túnel con ESET mediante el proxy instalado en el mismo equipo que el servidor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

- El uso del Proxy HTTP puede ahorrarle bastante ancho de banda en las descargas de Internet y mejorar las velocidades de descarga para las actualizaciones de productos. Se recomienda seleccionar la casilla de verificación junto al **Apache HTTP Proxy** si gestiona más de 37 equipos desde ESET PROTECT. También puede elegir instalar Instalar el proxy Apache HTTP más adelante.
- Para obtener más información, consulte ¿Qué es Apache HTTP Proxy? y Diferencias entre Apache HTTP Proxy, herramienta de replicación y conectividad directa.
- Seleccione **Apache HTTP Proxy** para instalar el Proxy HTTP Apache, crear y aplicar políticas (llamadas **Uso del Proxy HTTP**, aplicadas al grupo **Todo**) para los siguientes productos:
  - ESET Endpoint para Windows
  - ESET Endpoint para macOS (OS X) y Linux
  - ESET Management Agent
  - Seguridad de archivos de ESET para Windows Server (6+)
  - ESET Server Security para Windows (8 o posterior)
  - Caché local compartido de ESET

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



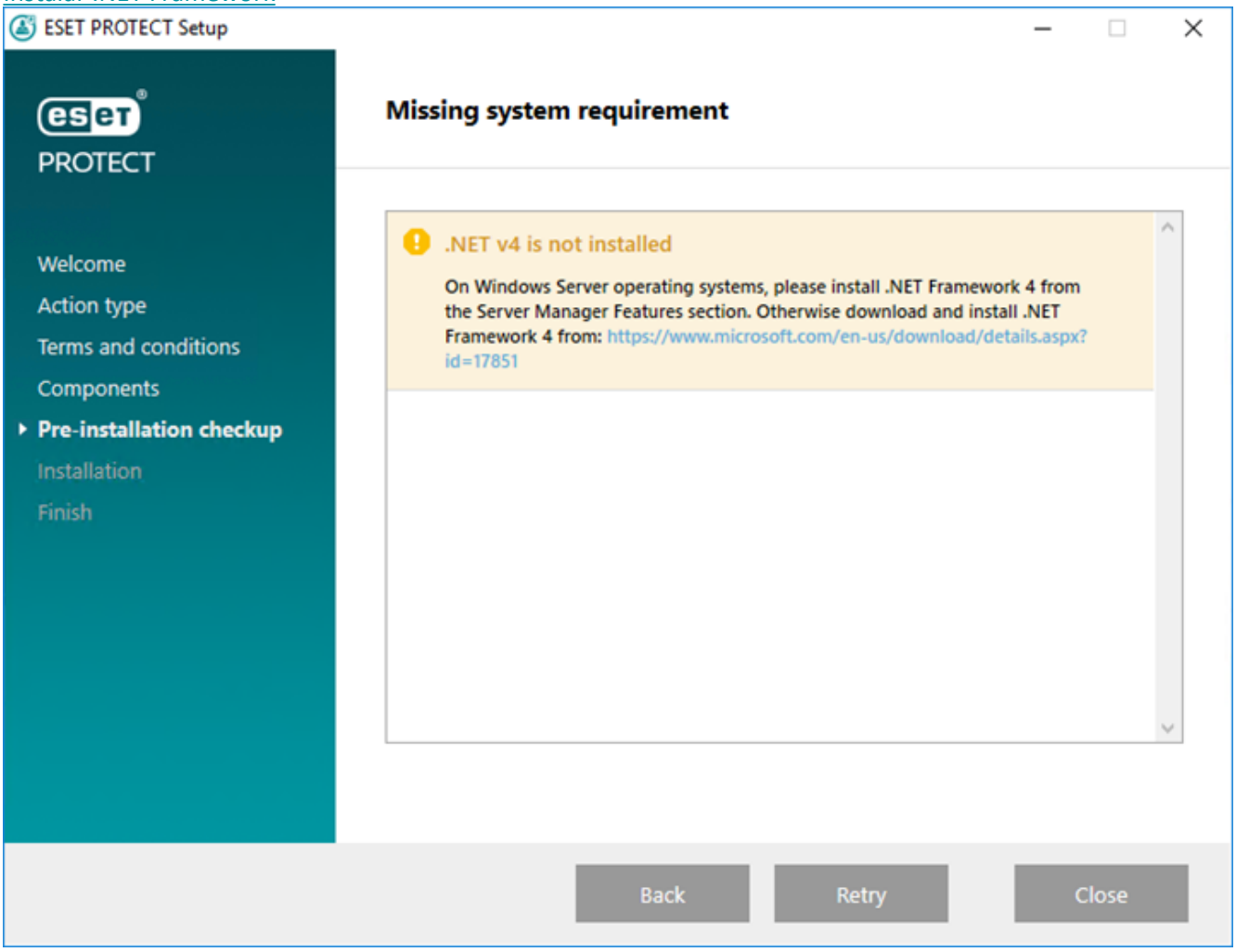
5. Si seleccionó **Agregar un certificado HTTPS personalizado para la consola web**, haga clic **Navegar** y seleccione un certificado válido (archivo *.pfx* o .p12) y escriba su **frase de contraseña** (o deje el campo en blanco si no hay frase de contraseña). El instalador instalará el certificado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



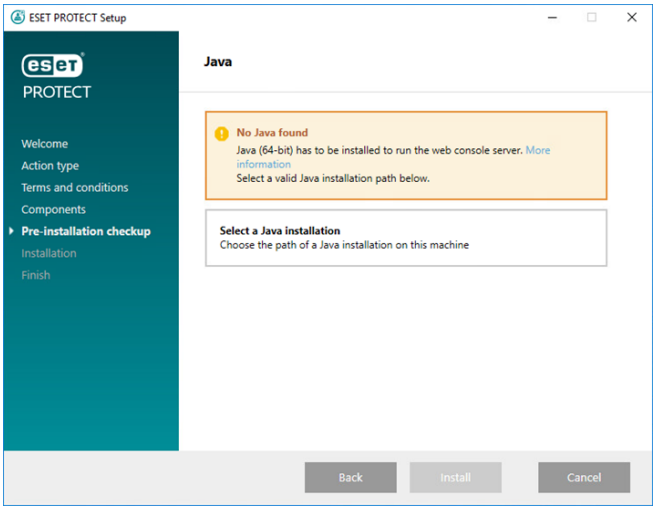
6. Si se encuentran errores durante la verificación de los prerrequisitos, abórdelos de la manera correspondiente. Asegúrese de que su sistema cumpla con todos los prerrequisitos.

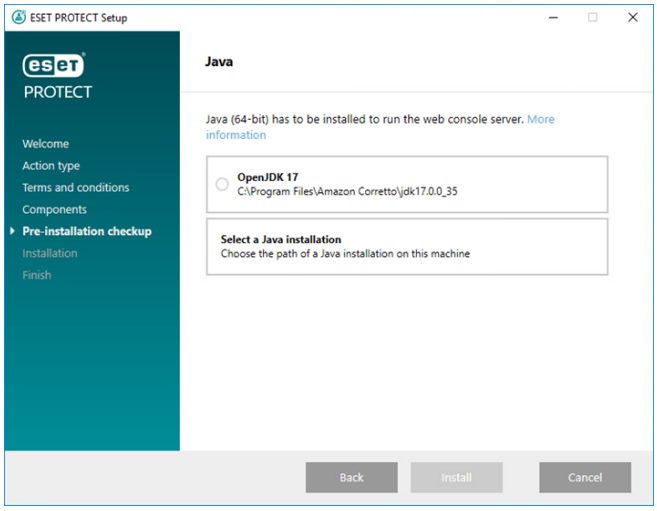
.NET v4 no está instalado

Instalar .NET Framework



No se encontró Java/no se detectó Java (64 bits)





Si tiene muchas versiones de Java instaladas en su sistema, le recomendamos desinstalar las versiones anteriores de Java y solo dejar la última versión 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 pasar a una alternativa sin costo. Consulte las versiones compatibles de JDK.

a)Para seleccionar Java ya instalado, haga clic en **Seleccionar una instalación de Java**, seleccione la carpeta donde está instalado Java (con una subcarpeta *bin*, por ejemplo *C:\Program Files\Amazon Corretto\jdk1.8.0_212*) y haga clic en **Aceptar**. El instalador le indica si ha seleccionado una ruta no válida.
b)Haga clic en **Instalar** para continuar o **Cambiar** para cambiar la ruta de instalación de Java.

Solo hay 32 MB libres en el disco del sistema

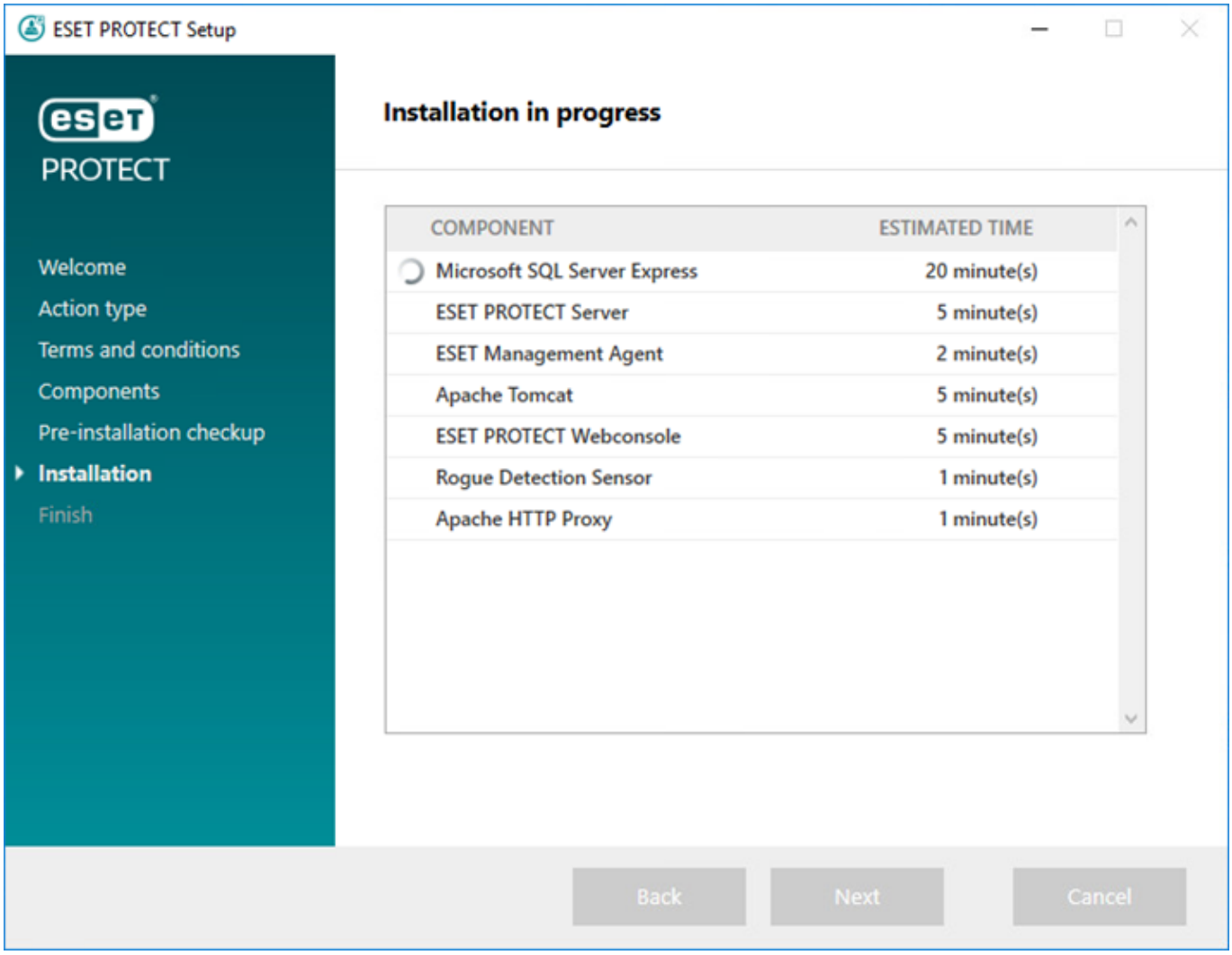
- El instalador podrá mostrar la siguiente notificación si su sistema no tiene suficiente espacio en disco para la instalación de ESET PROTECT.
- Debe contar con al menos 4400 MB de espacio libre en el disco para instalar ESET PROTECT y todos sus componentes.

ESET Remote Administrator versión 5.x o superior está instalado en el equipo.

La actualización directa no es compatible. Consulte Migración desde ERA 5.x o actualización desde ERA 6.x.

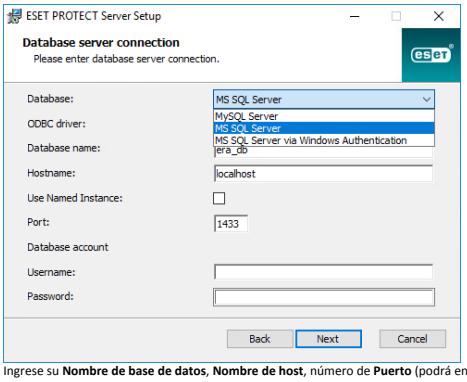
7. Cuando se complete el control de los requisitos previos y su entorno cumpla con todos los requisitos, se iniciará la instalación. Tenga en cuenta que el proceso de instalación puede llevar más de una hora, dependiendo de su sistema y la configuración de la red.

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



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

Configure la conexión a SQL/MySQL Server

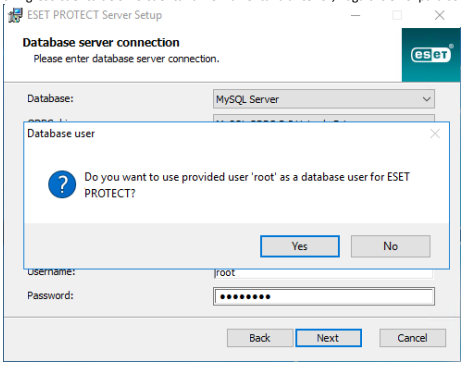


Ingrese su **Nombre de base de datos**, **Nombre de host**, número de **Puerto** (podrá encontrar esta información en Microsoft SQL Server Configuration Manager) y los detalles de la **Cuenta de la base de datos** (**Nombre de usuario** y **Contraseña**) en los campos adecuados y haga clic en **Siguiente**.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

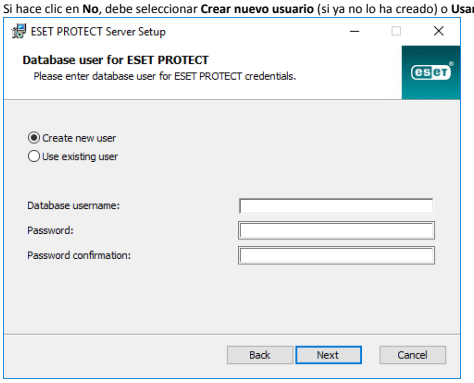
Usar instancia con nombre: si usa la base de datos MS SQL, puede seleccionar la casilla de verificación **Usar instancia con nombre** para usar una instancia de la base de datos con nombre. Puede configurarlo en el campo **Nombre de host** con el formato *HOSTNAME\DB_INSTANCE* (por ejemplo, *192.168.0.10\ESMC7SQL*).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

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

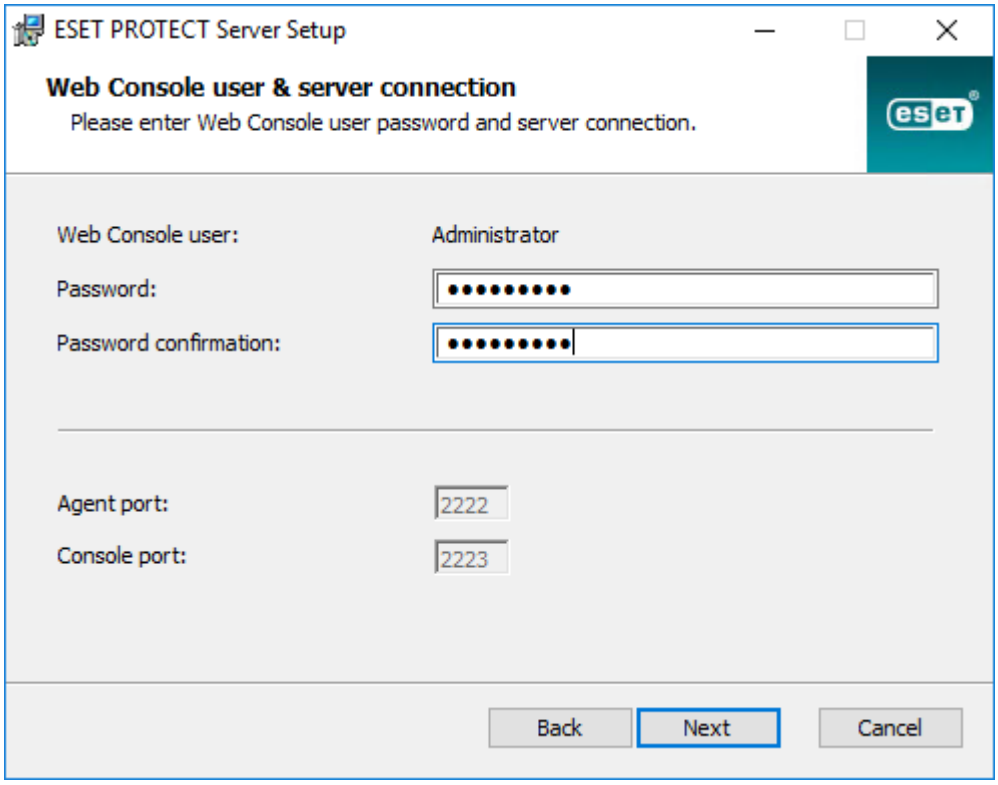
Si ingresó **cuenta de SA** o **cuenta raíz** en la ventana anterior, haga clic en **Sí** para continuar usando la cuenta raíz/SA como usuario de base de datos para ESET PROTECT.



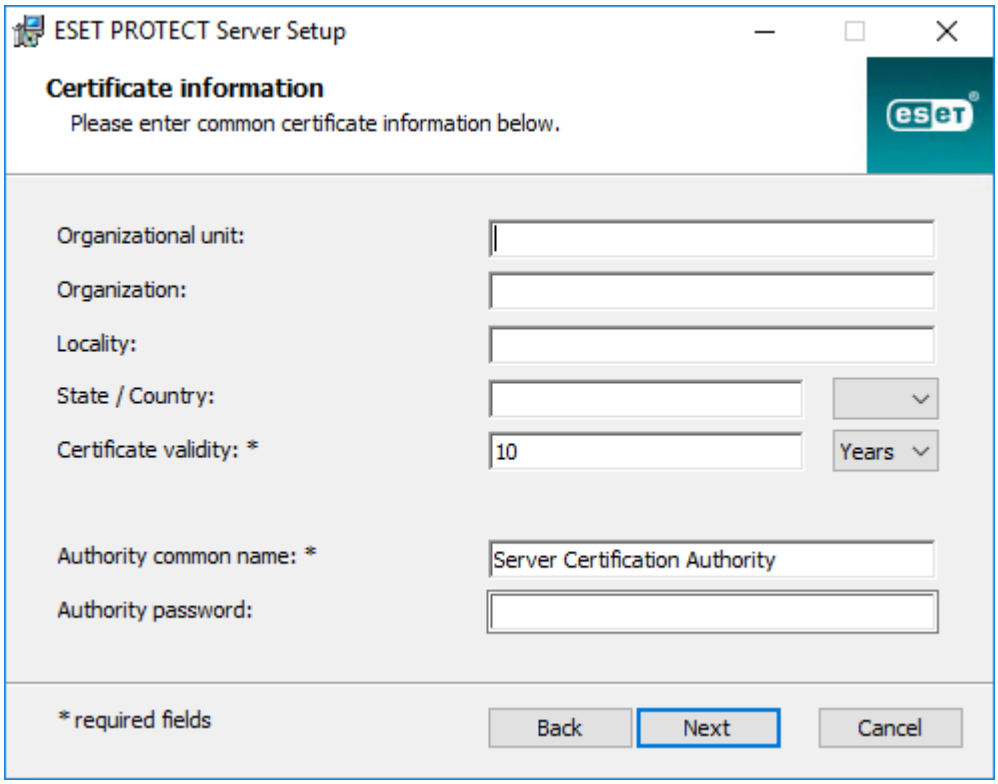
Si hace clic en **No**, debe seleccionar **Crear nuevo usuario** (si ya no lo ha creado) o **Usar usuario existente** (si tiene una cuenta de usuario de base de datos dedicada).



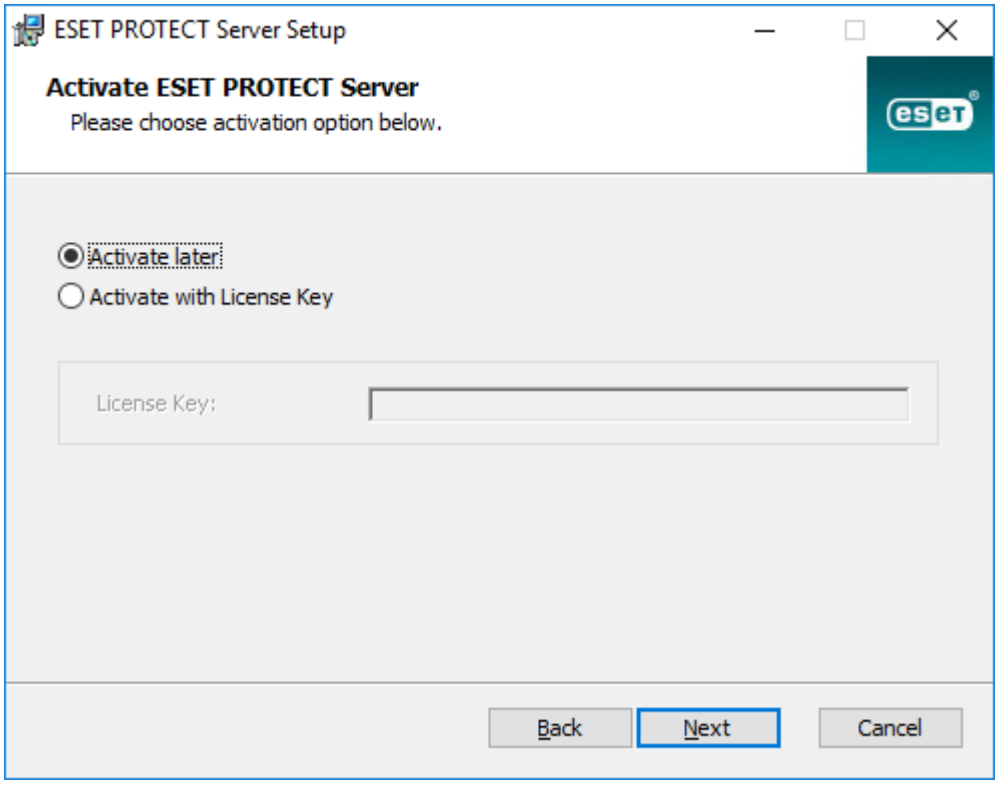
9. El instalador le solicitará que ingrese una contraseña para la cuenta de Administrador de la consola web. Esta contraseña es importante, ya que la usará para iniciar sesión en la Consola web ESET PROTECT. Haga clic en **Siguiente**.



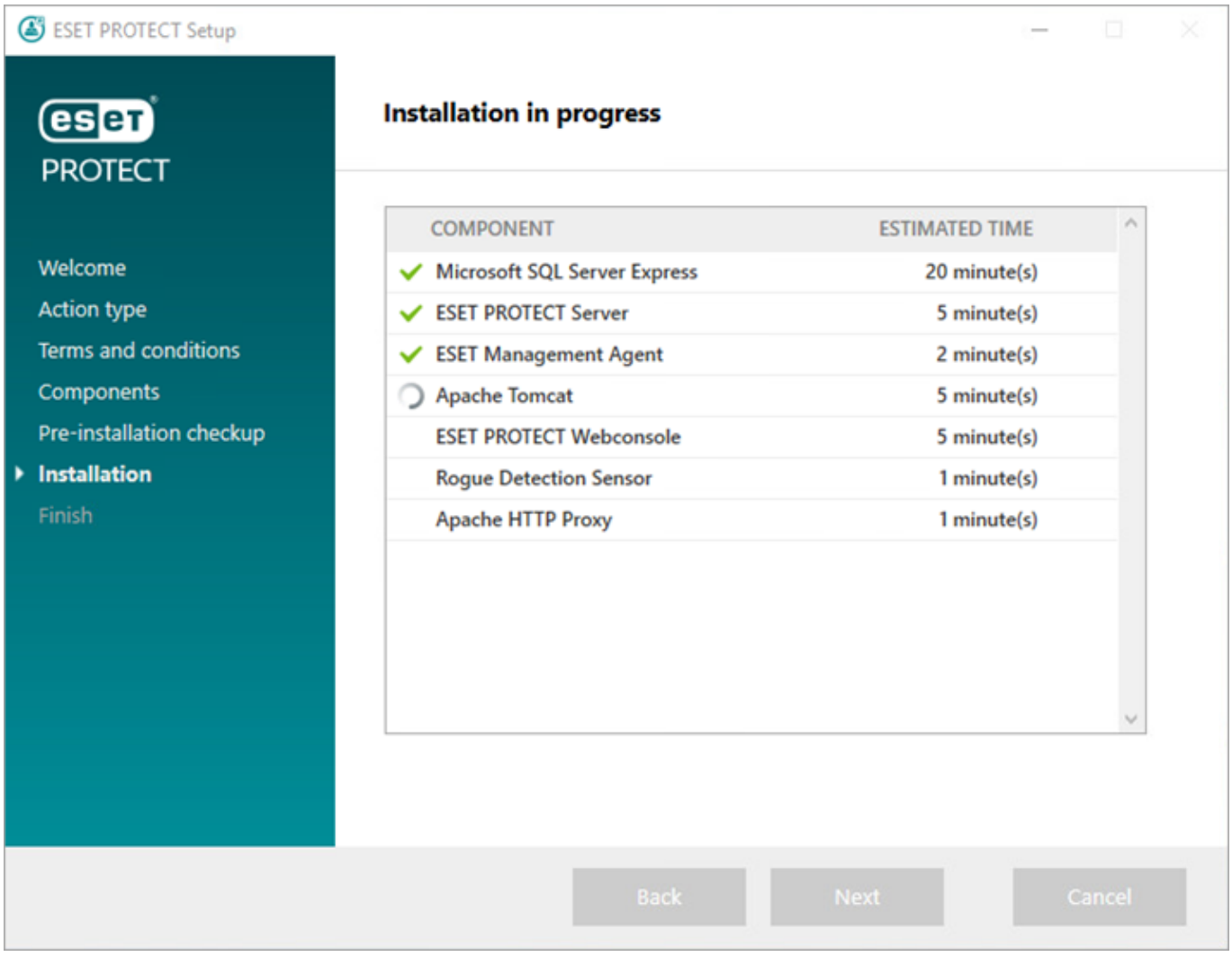
10. Deje los campos intactos o introduzca su información corporativa para que aparezca en los detalles de los certificados del Agente ESET Management y del servidor ESET PROTECT. Si opta por ingresar una contraseña en el campo **contraseña de autoridad**, asegúrese de recordarla. Haga clic en **Siguiente**.



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



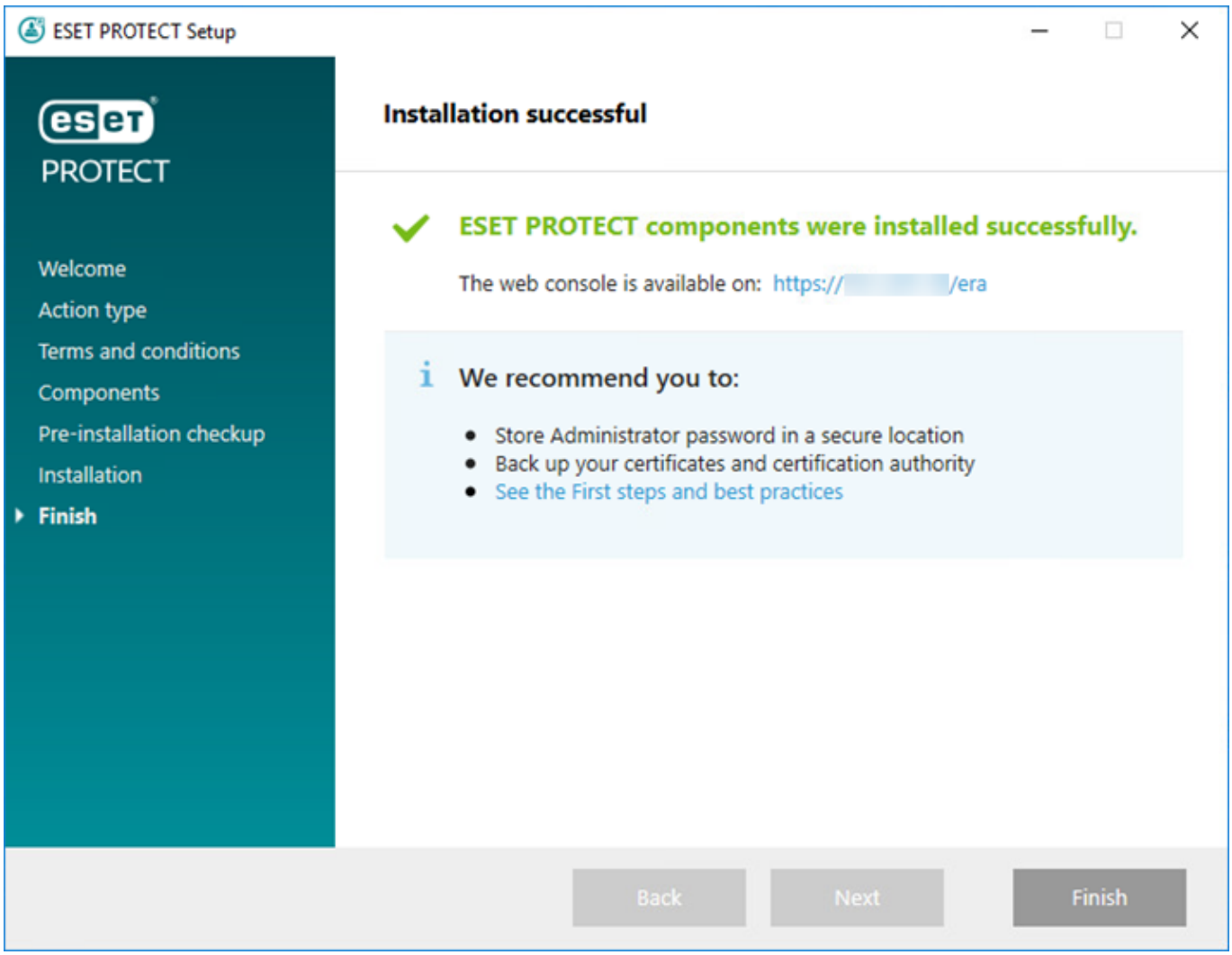
12. Verá el progreso de la instalación.



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

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

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



Si la instalación no se realizó correctamente:

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

- Consulte Resolución de problemas para obtener los pasos para resolver el problema.

Instalar el Dispositivo conector móvil de ESET PROTECT (Independiente)

Para instalar un conector de dispositivo móvil como herramienta independiente en un equipo diferente al Servidor ESET PROTECT, complete los siguientes pasos.

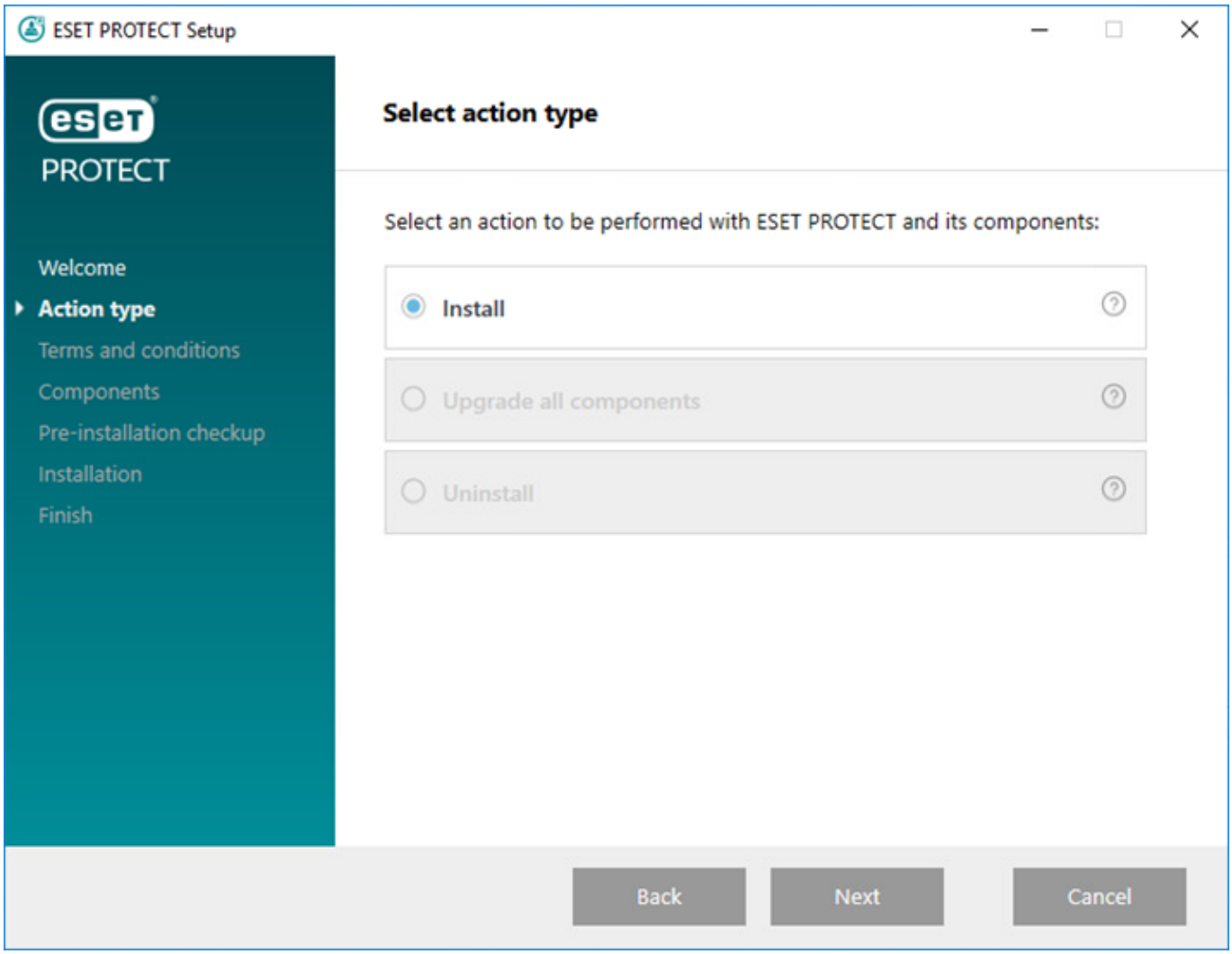
Se debe poder acceder al conector de dispositivo móvil desde Internet para que los dispositivos móviles se puedan administrar en todo momento sin importar su ubicación.

Tenga en cuenta que los dispositivos móviles se comunican con el Conector de dispositivo móvil, lo cual inevitablemente afecta el uso de los datos móviles. Esto se aplica especialmente a la itinerancia.

Siga los siguientes pasos para instalar el Conector de dispositivo móvil en Windows:

1. Lea primero los requisitos previos y asegúrese de que se cumplan.

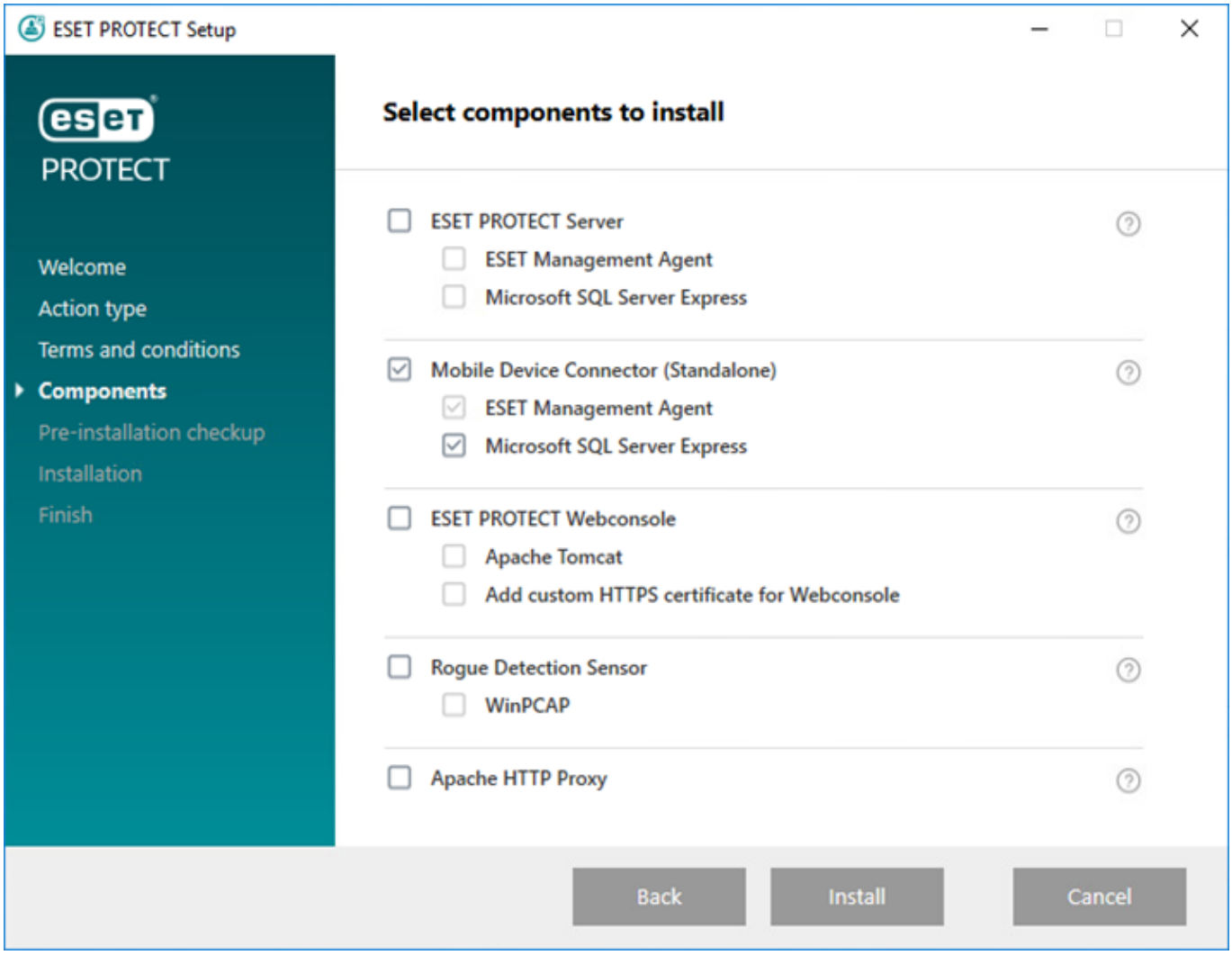
2. Haga doble clic en el paquete de la instalación para abrirlo, seleccione **Instalar** y haga clic en **Siguiente**.



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

4. Luego de aceptar el EULA, haga clic en **Siguiente**.

5. Seleccione solo la casilla de verificación junto a **Mobile Device Connector (Independiente)**. El Conector de dispositivo móvil de ESET PROTECT necesita una **base de datos** para operar. Seleccione **Microsoft SQL Server Express** si desea instalar la base de datos, o deje vacía la casilla de selección. Si desea conectarse con una base de datos existente, tendrá la opción de hacerlo durante la instalación. Haga clic en **Instalar** para proceder con la instalación.



6. Si instaló la base de datos como parte de esta instalación en el paso 5, ahora la base de datos estará instalada automáticamente y puede saltar al paso 8. Si decidió no instalar la base de datos en el paso 5, se le pedirá que conecte el componente MDM de su base de datos existente.

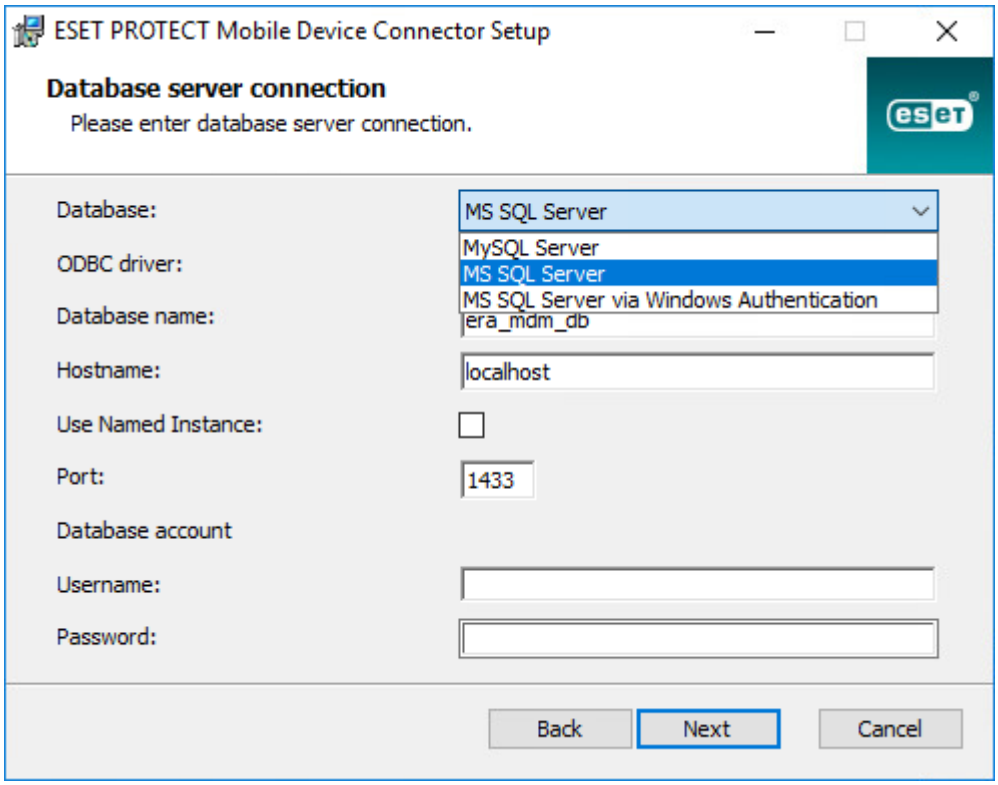
> Puede usar el mismo servidor de la base de datos que usa para la base de datos de ESET PROTECT, pero recomendamos que use un servidor de la BD diferente si planea registrar más de 80 dispositivos móviles.

7. El instalador necesita conectarse con una base de datos existente que usará el Conector de dispositivo móvil. Especifique los siguientes detalles de conexión:

- **Base de datos**: Servidor MySQL/Servidor MS SQL/Servidor MS SQL por medio de la autenticación de Windows
- **Controlador ODBC**: Controlador MySQL ODBC 5.1/Controlador unicode MySQL ODBC 5.2/Controlador unicode MySQL ODBC 5.3/Controlador unicode MySQL ODBC 8.0/Servidor SQL/Cliente nativo Servidor SQL 10.0/Controlador ODBC 11 para Servidor SQL/Controlador ODBC 13 para Servidor SQL/Controlador ODBC 17 para Servidor SQL/Controlador ODBC 18 para Servidor SQL
- **Nombre de la base de datos**: Se recomienda utilizar el nombre predefinido o cambiarlo si es necesario.
- **Nombre de host**: nombre de host o dirección de IP de su servidor de base de datos
- **Puerto**: usado para la conexión con el servidor de base de datos

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

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

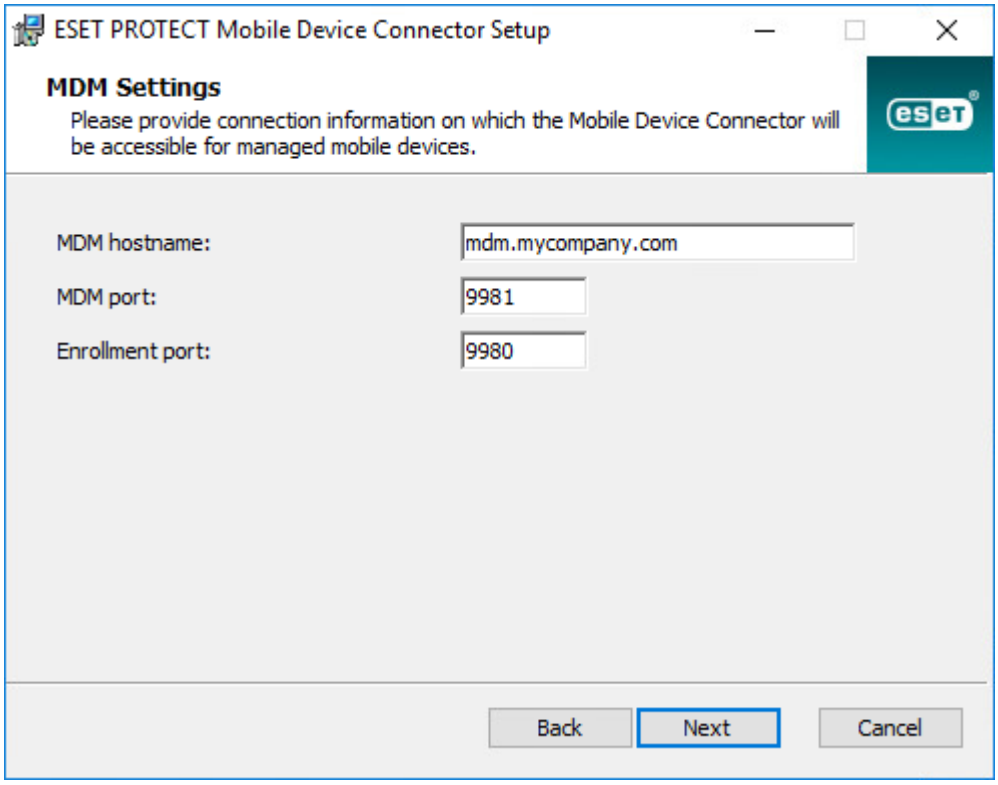


8. Si la conexión fue exitosa, se le pedirá que verifique que desea usar el usuario proporcionado como usuario de la base de datos para ESET PROTECT MDM.

9. Después de instalar exitosamente la nueva base de datos, o de que el instalador se haya conectado a la base de datos existente, puede proceder con la instalación de MDM. Especifique el **Nombre de host de MDM**: es el dominio público o dirección IP pública de su servidor MDM ya que se localiza mediante los dispositivos móviles desde Internet.

Debe introducir el nombre del host MDM en la misma forma que aparece en su **certificado de servidor HTTPS**; de lo contrario, el dispositivo móvil iOS rechazará la instalación del Perfil MDM. Por ejemplo, si hay una dirección IP especificada en el certificado HTTPS, escriba esta dirección IP en el campo **nombre de host de MDM**. Si se especifica una FQDN (por ejemplo, `mdm.mycompany.com`) en el certificado de HTTPS, ingrese dicho FQDN en el campo **Nombre de host de MDM**. Además, si se usa un comodín * (por ejemplo, `*.mycompany.com`) en el certificado de HTTPS, puede usar `mdm.mycompany.com` en el campo **Nombre de host de MDM**.

Tenga cuidado de llenar el campo **Nombre de host de MDM** en este punto de la instalación. Si la información o el formato no son correctos, el Conector de MDM no funcionará apropiadamente y la única forma de arreglarlo sería reinstalando el componente.



10. En el siguiente paso, verifique la conexión con la base de datos haciendo clic en **Siguiente**.

11. Conecte el Conector de MDM al Servidor de ESET PROTECT. Complete el **Host del servidor** y el **Puerto de servidor** requeridos para la conexión con el Servidor de ESET PROTECT y seleccione **Instalación asistida del servidor** o **Instalación fuera de línea** para proceder:

- **Instalación asistida del Servidor**: provee credenciales de administrador de Consola Web ESET PROTECT y el instalador descargará los certificados necesarios automáticamente. Verifique también los permisos necesarios para la instalación asistida por servidor.

    1.Ingrese el **Host del servidor**: nombre o dirección IP de su Servidor y **Puerto de Consola web** de ESET PROTECT (deje el puerto predeterminado 2223 si no está usando un puerto personalizado). También, ofrezca credenciales de cuenta de administrador de la consola web: **Nombre de usuario/Contraseña**.

    2.Cuando se pida que acepte el certificado, haga clic en **Sí**. Continúe en el paso 11.

- **Instalación fuera de línea**: proporciona un Certificado de Proxy y una Autoridad de certificación que se puede exportar desde ESET PROTECT. Como alternativa, puede usar su certificado personalizadoy una Autoridad de certificación apropiada.

    1.Haga clic en **Examinar**, junto a Certificado de pares, y navegue hasta la ubicación del **Certificado de pares** (este es el certificado de proxy que exportó desde ESET PROTECT). Deje en blanco el área de **Contraseña del certificado** porque este certificado no necesita una contraseña.

    2.Repita el procedimiento para la Autoridad de certificado y continúe en el paso 11.

> Si usa certificados personalizados con ESET PROTECT (en lugar de los predeterminados que se generaron automáticamente durante la instalación de ESET PROTECT), debe usarse estos mismos cuando se le solicite proveer un certificado Proxy.

12. Especifique la carpeta de destino para el Conector de dispositivo móvil (recomendamos usar la

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

Después de terminar la instalación de MDM, se le pedirá instalar un Agente. Haga clic en **Siguiente** para iniciar la instalación y aceptar los EULA si está de acuerdo y siga estos pasos:

1. Ingrese el **Host del servidor** (nombre de host o dirección de IP de su Servidor de ESET PROTECT) y el **Puerto del servidor** (el puerto predeterminado del servidor es 2222; si usa un puerto diferente, reemplace el puerto predeterminado por su número de puerto personalizado).

Asegúrese de que el **Host del servidor** coincide al menos con uno de los valores (idealmente FQDN) definidos en el campo **Host** del **Certificado del servidor**. De lo contrario, obtendrá un mensaje de error que dice “El certificado del servidor recibido no es válido”. La única excepción es en caso de haber un comodín (*) en el campo host del certificado del servidor, que significa que funcionará con cualquier **host de servidor**.

2. Si usa el proxy, seleccione la casilla de verificación **Usar Proxy**. Al seleccionar la casilla, el instalador continuará con **instalación fuera de línea**.

Esta configuración de proxy sólo se usa para (replicación) entre el Agente de ESET Management y el Servidor de ESET PROTECT, no para almacenar actualizaciones en caché.
- **Nombre de host del proxy**: nombre de host o dirección IP de la máquina del Proxy HTTP.
- **Puerto del Proxy**: el valor predeterminado es 3128.
- **Nombre de usuario**, **Contraseña**: ingrese las credenciales que usa su proxy si usa autenticación.

Puede cambiar la configuración de proxy más adelante en su política. El Proxy debe instalarse antes de que pueda configurar la conexión entre el Agente y el Servidor vía Proxy.

3. Seleccione una de las siguientes opciones de instalación y siga los pasos de la sección adecuada que aparece a continuación:

Instalación asistida por Servidor: necesitará credenciales de administrador de la Consola web ESET PROTECT (el instalador descargará los certificados necesarios automáticamente).

Instalación fuera de línea: necesitará proporcionar un Certificado de Agente y una Autoridad de certificación, que se pueden exportar de ESET PROTECT. Como alternativa, puede usar su certificado personalizado.

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

1.Ingrese el nombre de host o la dirección IP de la Consola web ESET PROTECT (la misma que el Servidor ESET PROTECT) en el campo **host del servidor**. Deje el **puerto de la consola web** en el puerto predeterminado 2223 si no usa un puerto personalizado. Además, ingrese sus credenciales de cuenta de la consola web en los **camposnombre de usuario y contraseña**. Para iniciar sesión como un usuario de dominio, seleccione la casilla de verificación situada junto a **Iniciar sesión en el dominio.**

- Asegúrese de que el **Host del servidor** coincide al menos con uno de los valores (idealmente FQDN) definidos en el campo **Host** del **Certificado del servidor**. De lo contrario, obtendrá un mensaje de error que dice “El certificado del servidor recibido no es válido”. La única excepción es en caso de haber un comodín (*) en el campo host del certificado del servidor, que significa que funcionará con cualquier **host de servidor**.
- No puede usar un usuario con autenticación de dos factores para instalaciones asistidas por el servidor.

2. Haga clic en **Sí** cuando se le pida si desea aceptar el certificado.

3. Seleccione **No crear equipo (se creará automáticamente durante la primera conexión)** o **Elegir grupo estático personalizado**. Si hace clic en **Seleccionar grupo estático personalizado** podrá seleccionar desde un listado de grupos estáticos existentes en ESET PROTECT. El equipo se agregará al grupo seleccionado.

4. Especifique la carpeta de destino para el Agente ESET Management (recomendamos usar la predeterminada), haga clic en **Siguiente** y luego en **Instalar**.

- Para continuar con la **instalación del agente fuera de línea,** 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 3128),**Nombre de usuario** y **Contraseña** y haga clic en **Siguiente**.

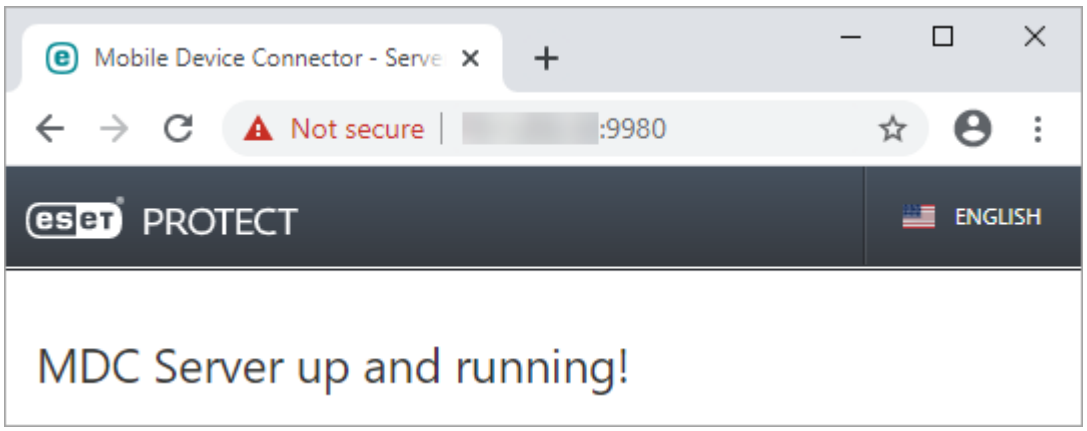
2. Haga clic en **Examinar** y navegue hasta la ubicación del certificado de pares (este es el certificado de agente que exportó desde ESET PROTECT). Deje en blanco el área de **Contraseña del certificado** porque este certificado no necesita una contraseña. No necesita buscar una **Autoridad de certificación** - deje el campo en blanco.

Si usa un certificado personalizado con ESET PROTECT (en vez del predeterminado que se generó automáticamente durante la instalación de ESET PROTECT), use sus certificados personalizados según corresponda.

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

3. Haga clic en **Siguiente** para instalar en la carpeta predeterminada o haga clic en **Cambiar** para elegir otra carpeta (recomendamos usar la ubicación predeterminada).

Después de completar la instalación, verifique si el Conector de dispositivo móvil se ejecuta correctamente abriendo *https://your-mdm-hostname:enrollment-port* (por ejemplo, *https://mdm.company.com:9980*) en su navegador web o desde un dispositivo móvil. Si la instalación fue exitosa, verá el siguiente mensaje:



Ahora puede activar MDM desde el administrador remoto ERA ESET PROTECT.

Instalación en Microsoft Azure

Para los usuarios que prefieran usar una solución gestionada, en lugar de mantener ESET PROTECT en el sitio, ESET ofrece ESET PROTECT en la plataforma en la nube de Microsoft Azure.

Para obtener más información, consulte el contenido de la base de conocimiento:

- Comenzar con ESET PROTECT: Azure
- ESET PROTECT VM for Microsoft Azure: Preguntas frecuentes
- Puede instalar ESET PROTECT 9.1 en Azure si sigue los pasos en este artículo de la base de conocimiento y con ESET PROTECT 9.1 Instalador todo en uno. O puede instalar ESMC 7.2 en Azure y luego actualizarlo a ESET PROTECT.

Instalación de componentes en Windows

En la mayoría de los escenarios de instalación, debe instalar diferentes componentes de ESET PROTECT en distintas máquinas para admitir las arquitecturas de red, cumplir con los requisitos de rendimiento, o por otros motivos. Los siguientes paquetes de instalación están disponibles para componentes individuales de ESET PROTECT:

Instalación de componentes principales

- Servidor ESET PROTECT
- Consola web ESET PROTECT – Puede instalar la consola web de ESET PROTECT en un equipo diferente a donde se ejecuta el servidor de ESET PROTECT.
- Agente ESET Management (debe estar instalado en los equipos cliente, es opcional en el caso del Servidor ESET PROTECT)

Instalación de componentes opcionales

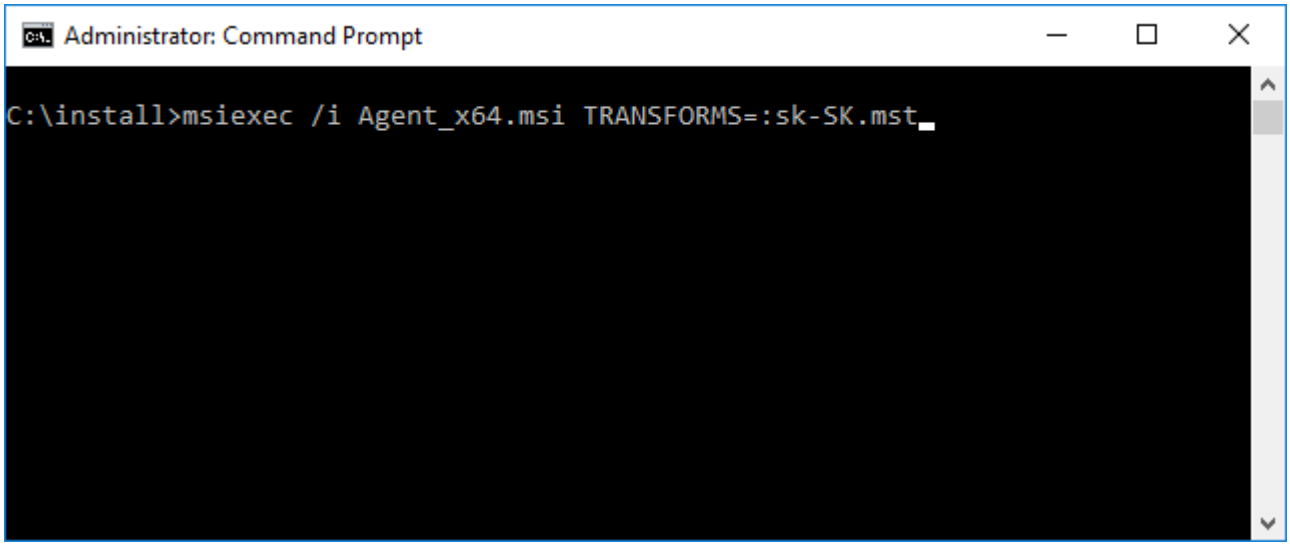
- RD Sensor
- Conector de dispositivo móvil
- Apache HTTP Proxy
- Herramienta de replicación

Consulte también la Instalación todo en uno de ESET PROTECT.

Para más información sobre cómo actualizar ESMC a la última versión de ESET PROTECT 9.1, consulte nuestros procedimientos de actualización.

Si desea ejecutar la instalación en su idioma local, necesita ejecutar el instalador MSI de un componente en particular de ESET PROTECT a través de la línea de comandos.

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



Para seleccionar el idioma en el que desea ejecutar el instalador, especifique el parámetro `TRANSFORMS` correspondiente de acuerdo con la siguiente tabla:

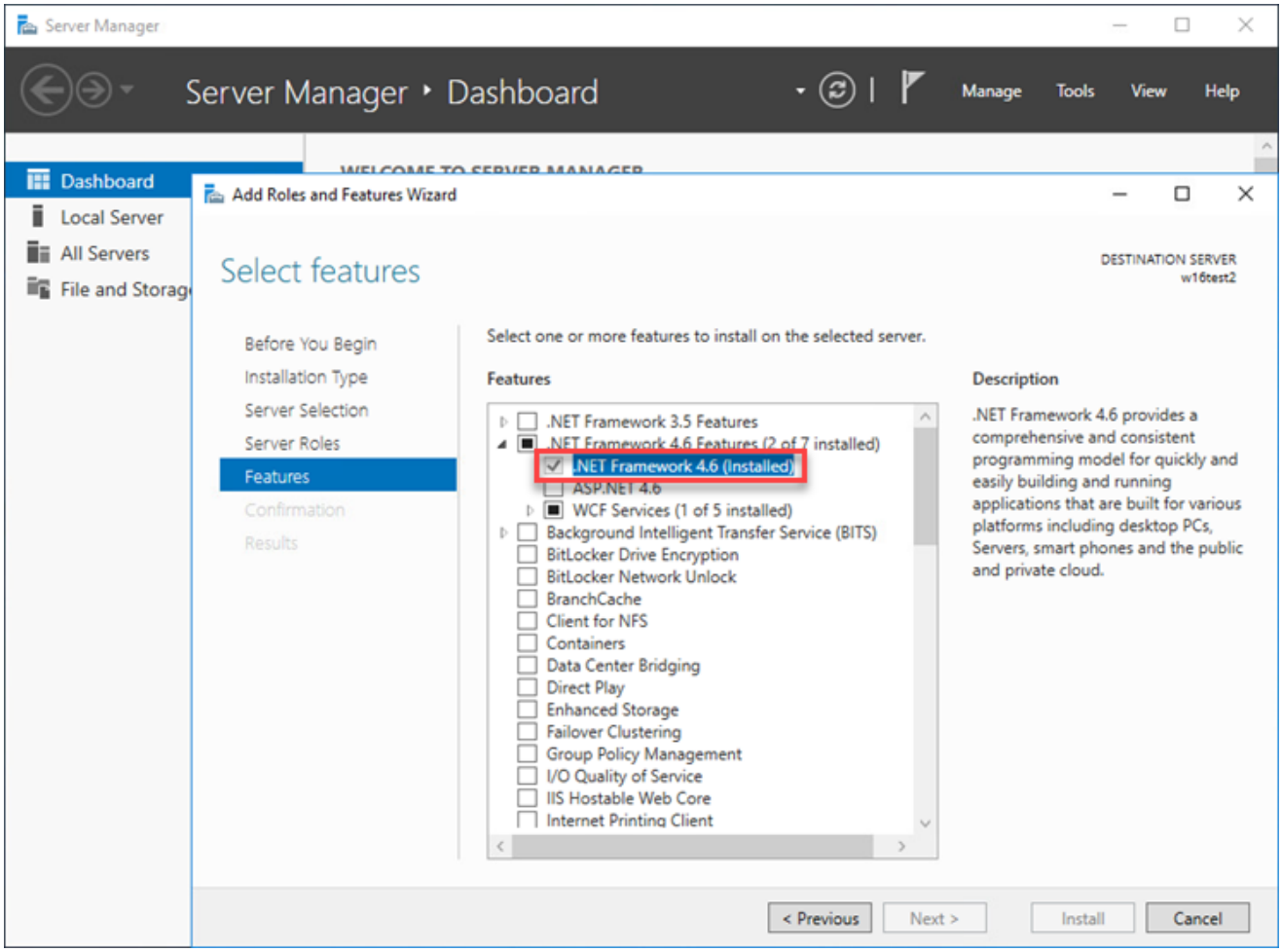
Idioma	Código
Inglés (Estados Unidos)	en-US
Árabe (Egipto)	ar-EG
Chino simplificado	zh-CN
Chino tradicional	zh-TW
Croata (Croacia)	hr-HR
Checo (República Checa)	cs-CZ
Francés (Francia)	fr-FR
Francés (Canadá)	fr-CA
Alemán (Alemania)	de-DE
Griego (Grecia)	el-GR
Húngaro (Hungría)*	hu-HU
Indonesian (Indonesia)*	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 el producto está disponible en este idioma; no hay ayuda en línea disponible.

Instalación del servidor: Windows

Requisitos previos

- Debe tener 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 y el conector de la base de datos compatibles (Microsoft SQL Server o MySQL) están instalados y en ejecución. Se recomienda que consulte los detalles de configuración del servidor de base de datos (Microsoft SQL Server o MySQL) para configurar correctamente la base de datos para usarla con ESET PROTECT. Lea nuestro artículo de la base de conocimiento para configurar su base de datos y su usuario de la base de datos para MS SQL o MySQL.
- Se instaló la consola web de ESET PROTECT para administrar el servidor de ESET PROTECT.
- 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 del Servidor de ESET PROTECT en Windows, siga los pasos a continuación:

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

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

2. Ejecute el instalador del Servidor ESET PROTECT y acepte el acuerdo de licencia de usuario final (EULA) si está de acuerdo.

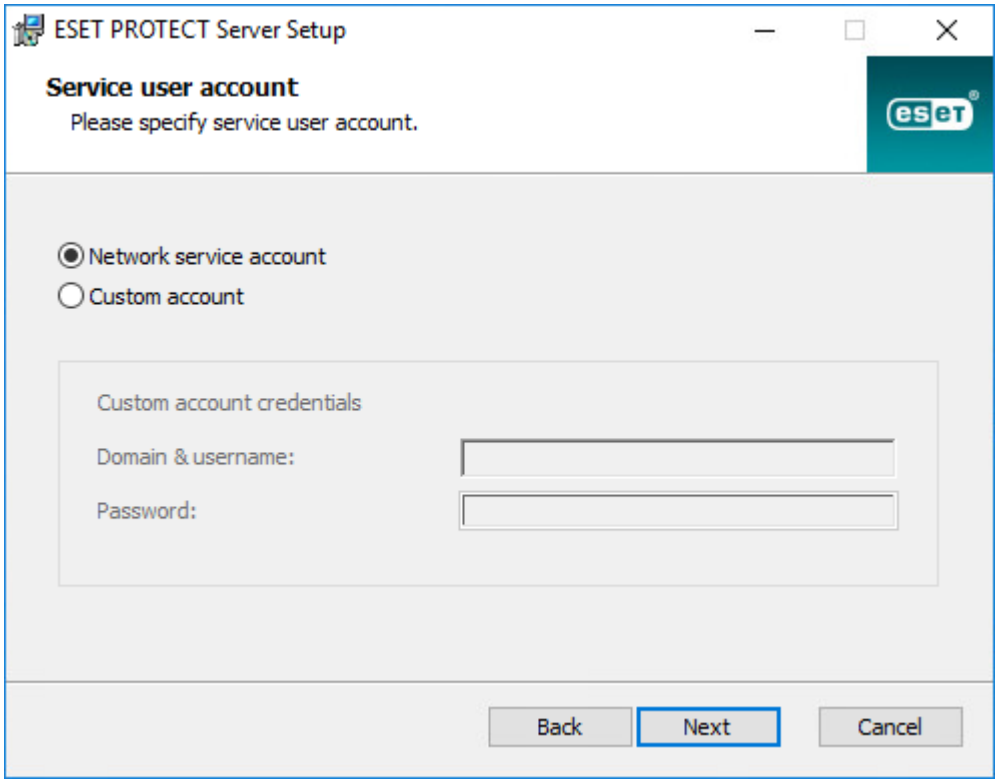
3. Desmarque la casilla de verificación al lado de **Participar en el programa de mejora del producto** si no está de acuerdo en enviar informes de fallas y datos de telemetría anónimos a ESET (versión y tipo de sistema operativo, versión de producto ESET y otra información específica del producto).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

4. Deje vacía la casilla de verificación junto a **Esto es instalación de clústeres** y haga clic en **Siguiente**. ¿Es esto una instalación de clústeres?

Si instala el Servidor ESET PROTECT en un Clúster de conmutación por error, seleccione la casilla de verificación junto a **Esto es instalación de clústeres**. Especifique la **Ruta de datos para la aplicación personalizada** para señalar al almacenamiento compartido del clúster. La información se debe almacenar en una ubicación accesible para todos los nodos del clúster.

5. Seleccione una **cuenta de usuario del servicio**. Esta cuenta se usará para ejecutar el servicio de servidores ESET PROTECT. Se encuentran disponibles las siguientes opciones:

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



6. Conexión a una base de datos. Todos los datos se almacenan aquí (contraseña de la Consola web ESET PROTECT, registros del equipo cliente, etc.):

• **Base de datos**: Servidor MySQL/Servidor MS SQL/Servidor MS SQL por medio de la autenticación de Windows

• **Controlador ODBC**: Controlador MySQL ODBC 5.1/Controlador unicode MySQL ODBC 5.2/Controlador unicode MySQL ODBC 5.3/Controlador unicode MySQL ODBC 8.0/Servidor SQL/Cliente nativo Servidor SQL 10.0/Controlador ODBC 11 para Servidor SQL/Controlador ODBC 13 para Servidor SQL/Controlador ODBC 17 para Servidor SQL/Controlador ODBC 18 para Servidor SQL

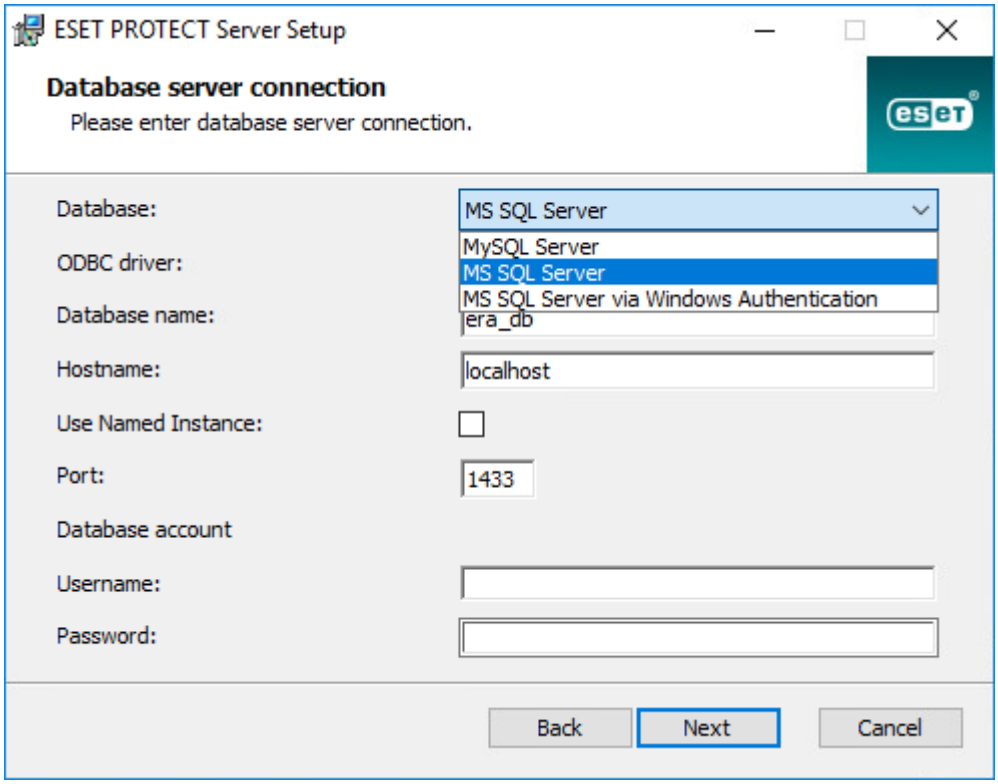
• **Nombre de la base de datos**: Se recomienda utilizar el nombre predefinido o cambiarlo si es necesario.

• **Nombre de host**: nombre de host o dirección de IP de su servidor de base de datos

• **Puerto**: usado para la conexión con el servidor de base de datos

• **Nombre de usuario/Contraseña** de la cuenta de administrador de la base de datos

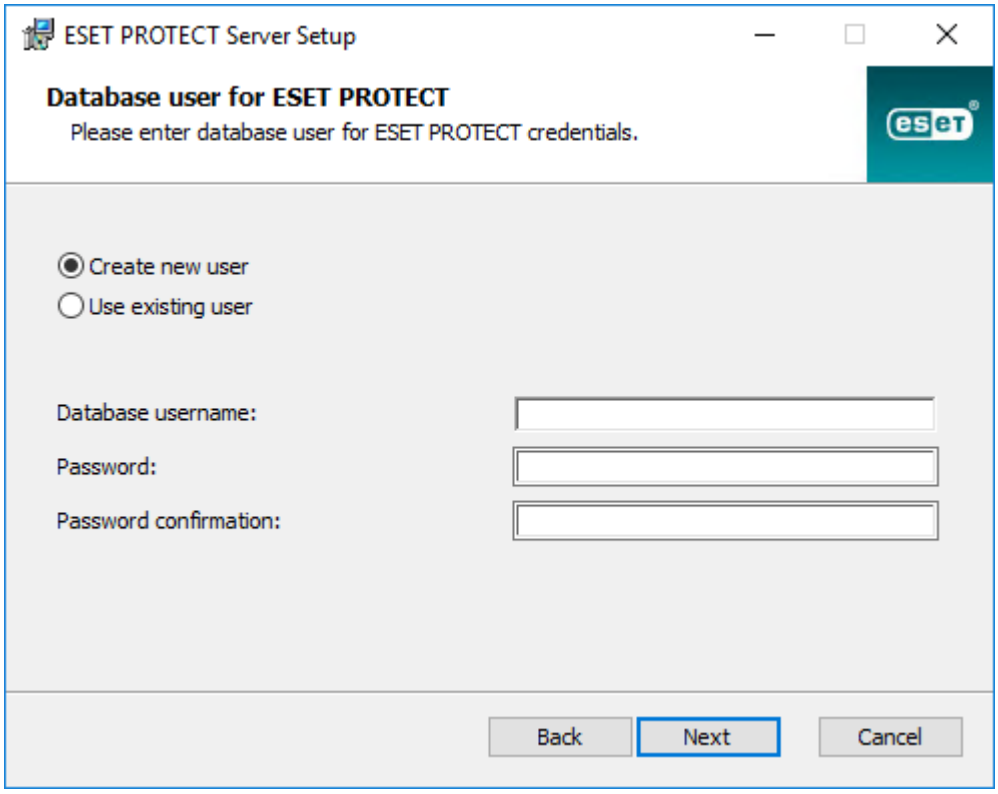
• **Usar instancia con nombre:** si usa la base de datos MS SQL, puede seleccionar la casilla de verificación **Usar instancia con nombre** para usar una instancia de la base de datos con nombre. Puede configurarlo en el campo **Nombre de host** con el formato *HOSTNAME\DB_INSTANCE* (por ejemplo, *192.168.0.10\ESMC7SQL*).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



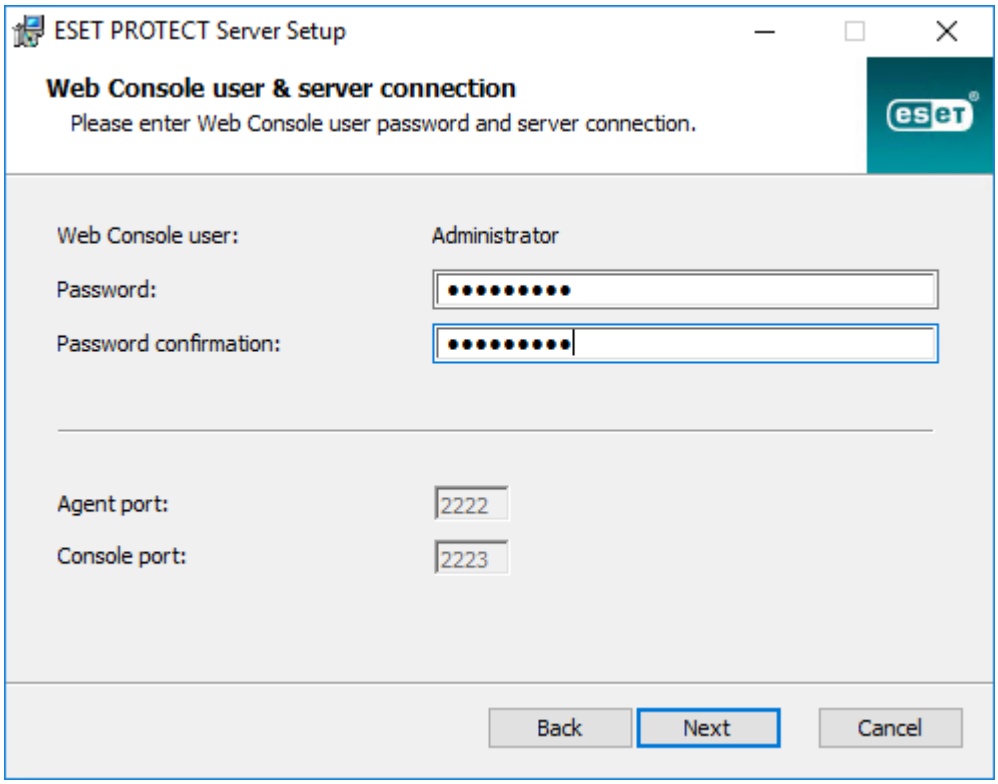
El servidor de ESET PROTECT almacena grandes blobs de datos en la base de datos. Por lo tanto, es necesario configurar MySQL para aceptar grandes paquetes a fin de que ESET PROTECT se ejecute de forma adecuada.

Este paso verificará su conexión a la base de datos. Si la conexión es correcta, puede continuar con el próximo paso.

7. Seleccione un usuario para ESET PROTECT que tenga acceso a la base de datos. Puede usar un usuario existente, o la configuración puede crear uno por usted.



8. Ingrese una contraseña para el acceso a la **consola web**.

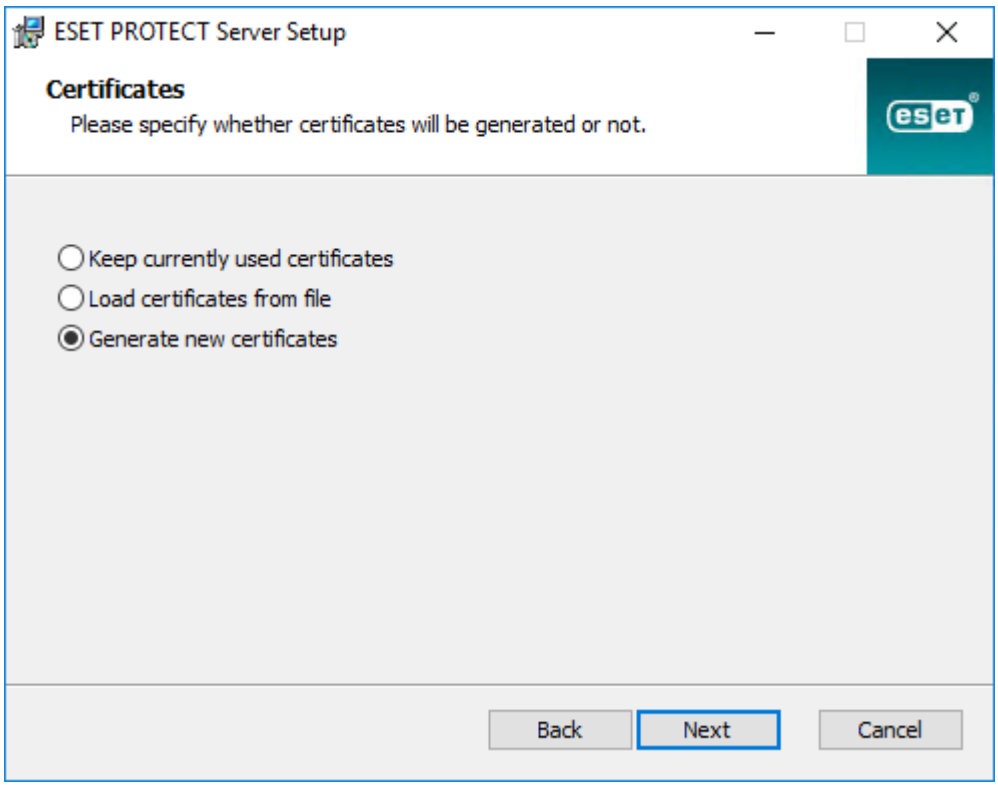


9. ESET PROTECT usa certificados para la comunicación entre el cliente y el servidor. Seleccione una de las siguientes opciones:

- **Mantener certificados actualmente usados**: esta opción se encuentra disponible únicamente si la base de datos ya se utilizaba con otro Servidor ESET PROTECT.

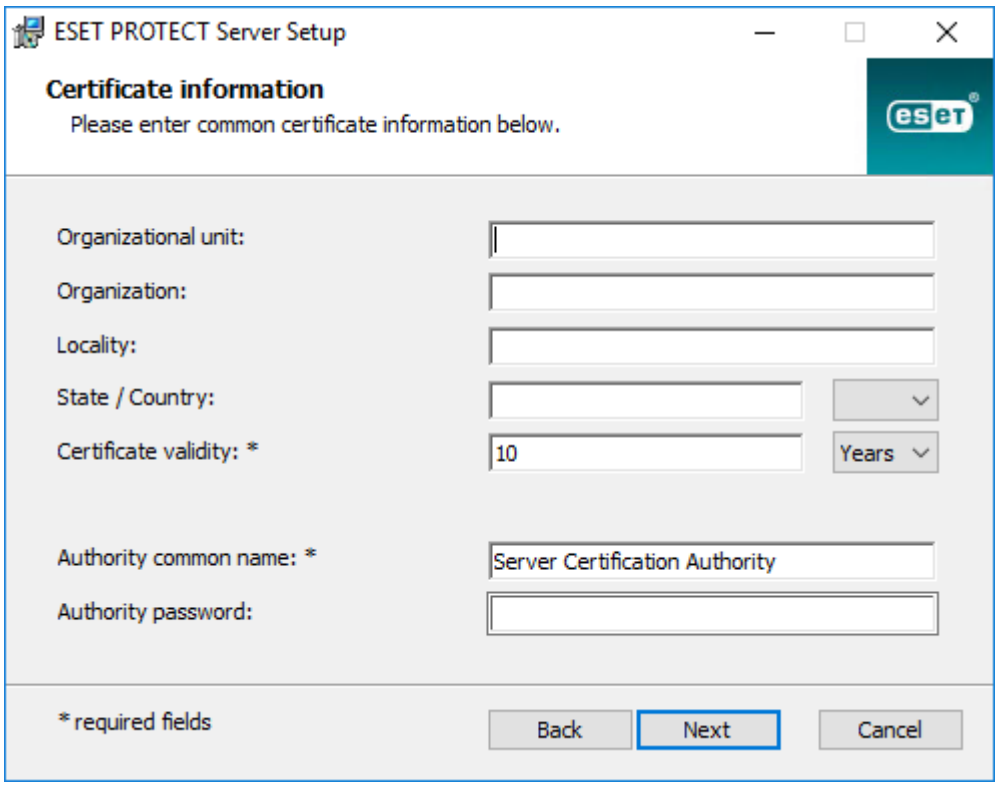
• **Cargar certificados del archivo**: seleccione el certificado del Servidor y la Autoridad de certificación existentes.

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



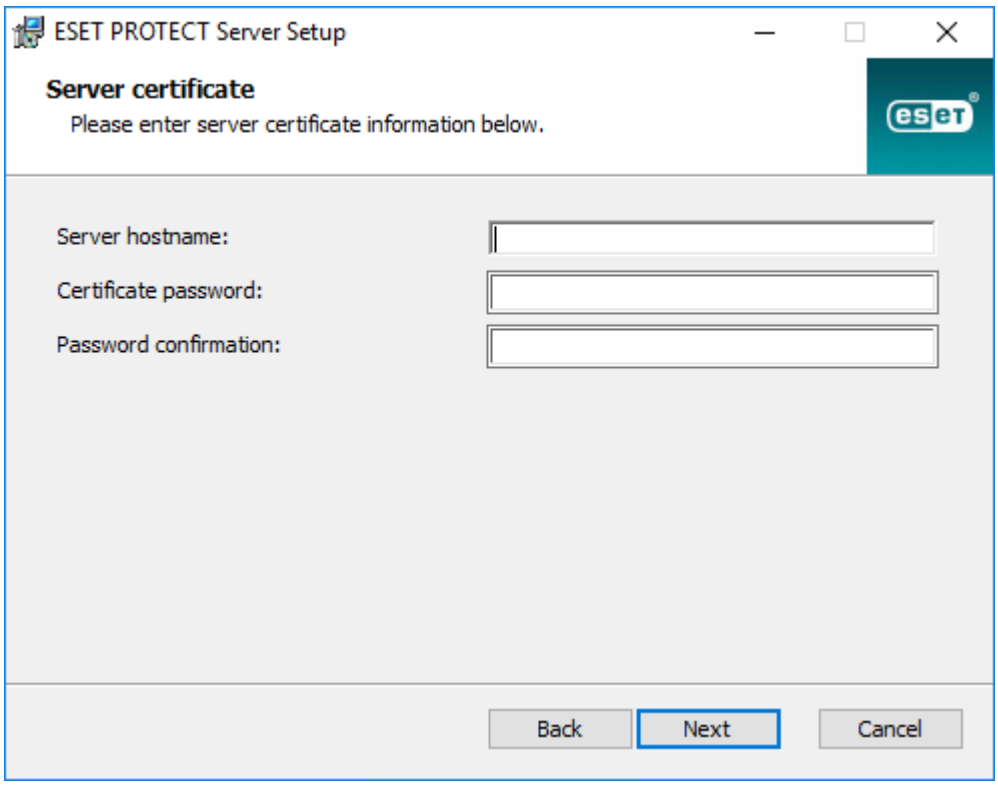
10. Siga este paso si ha seleccionado la opción **Generar certificados nuevos** en el paso anterior.

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

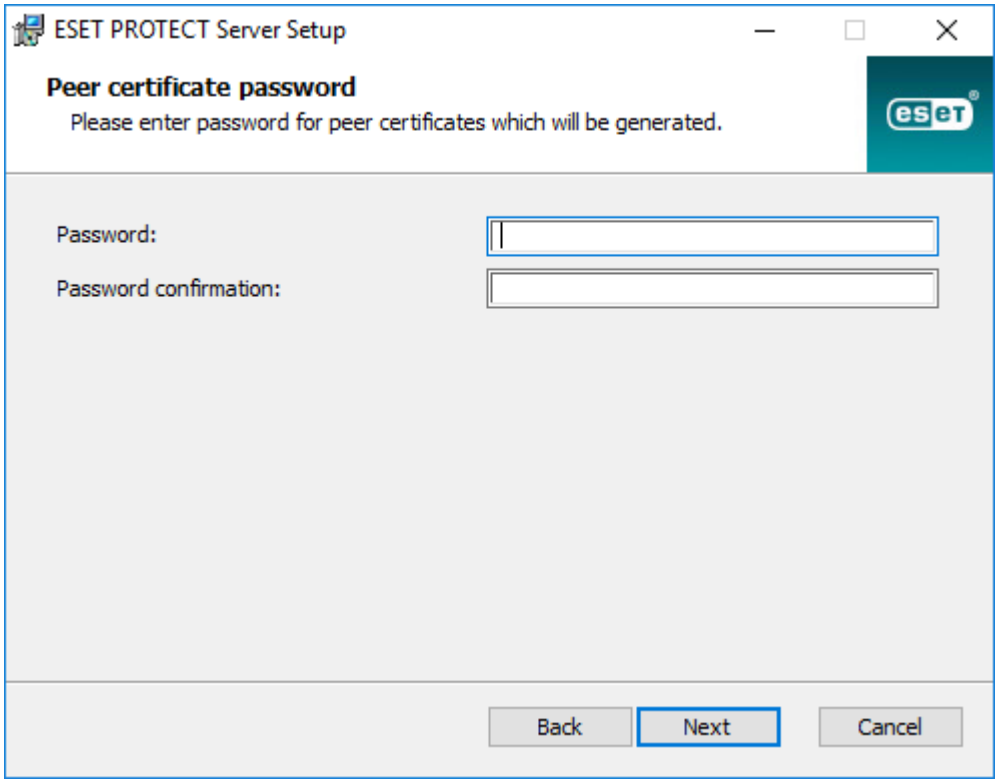


b)En el campo **Certificado del servidor**, escriba el **Nombre de host del servidor** y una **Contraseña del certificado** (opcional).

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



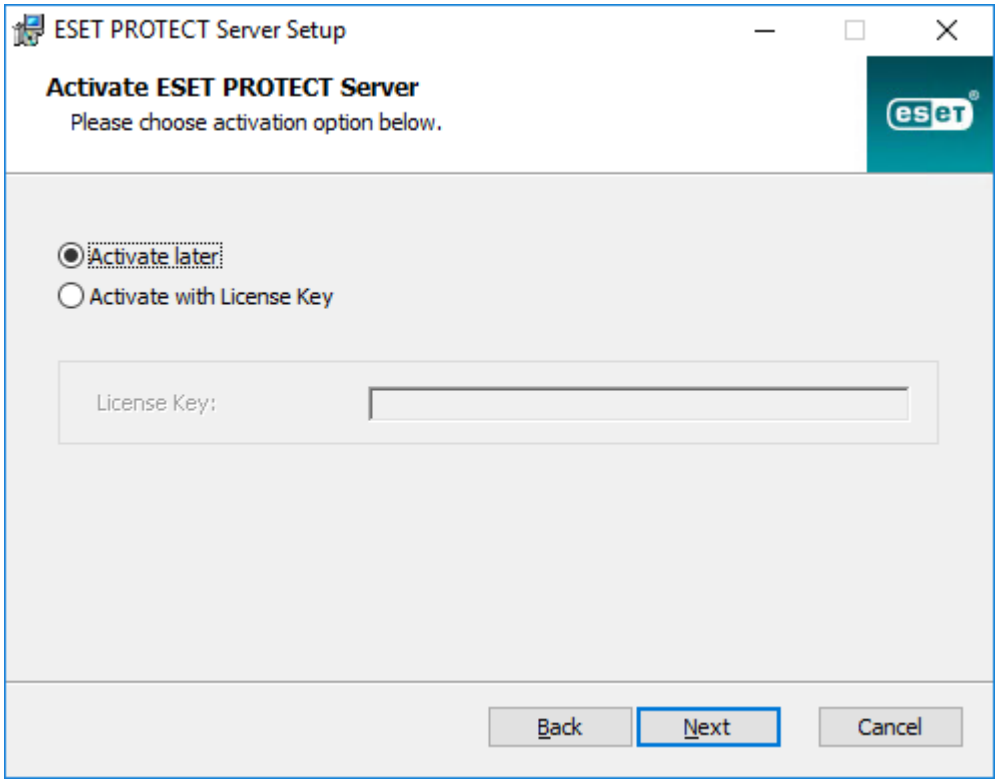
c)En el campo **Contraseña del certificado de par**, escriba la contraseña correspondiente a los certificados de agente y de pares de proxy.



11. La configuración puede realizar una tarea inicial de Sincronización del grupo estático. Seleccione el

método (**No sincronizar**, **Sincronizar con Windows Network**, **Sincronizar con Active Directory**) y haga clic en **Siguiente**.

12. Ingrese una clave de licencia válida o elija **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 servidor ESET PROTECT.

Cuando haya terminado de instalar el Servidor de ESET PROTECT, puede instalar el Agente de ESET Management en el mismo equipo (opcional) para activar la administración del Servidor de la misma forma que lo hace con el equipo del cliente.

Requisitos de Microsoft SQL Server

Se debe cumplir con los siguientes requisitos para Microsoft SQL Server:

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

- Si ya tiene Microsoft SQL Server instalado, establezca la autenticación a **Modo mixto (autenticación de SQL Server y autenticación de Windows)**. Para hacerlo, 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 que se detallan en este artículo de la base de conocimiento.

- Permita las conexiones TCP/IP al SQL Server. Para hacerlo, siga las instrucciones de este artículo de la base de conocimiento desde la parte **II. Permita las conexiones TCP/IP a la base de datos SQL**.

- Para configurar, administrar y gestionar 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/Essentials).

Recomendamos que instale ESET PROTECT en un servidor diferente o que no seleccione el componente SQL Server Express durante la instalación (esto requiere que use un SQL Server o un MySQL existente para ejecutar la base de datos ESET PROTECT).

Instalación y configuración de MySQL Server

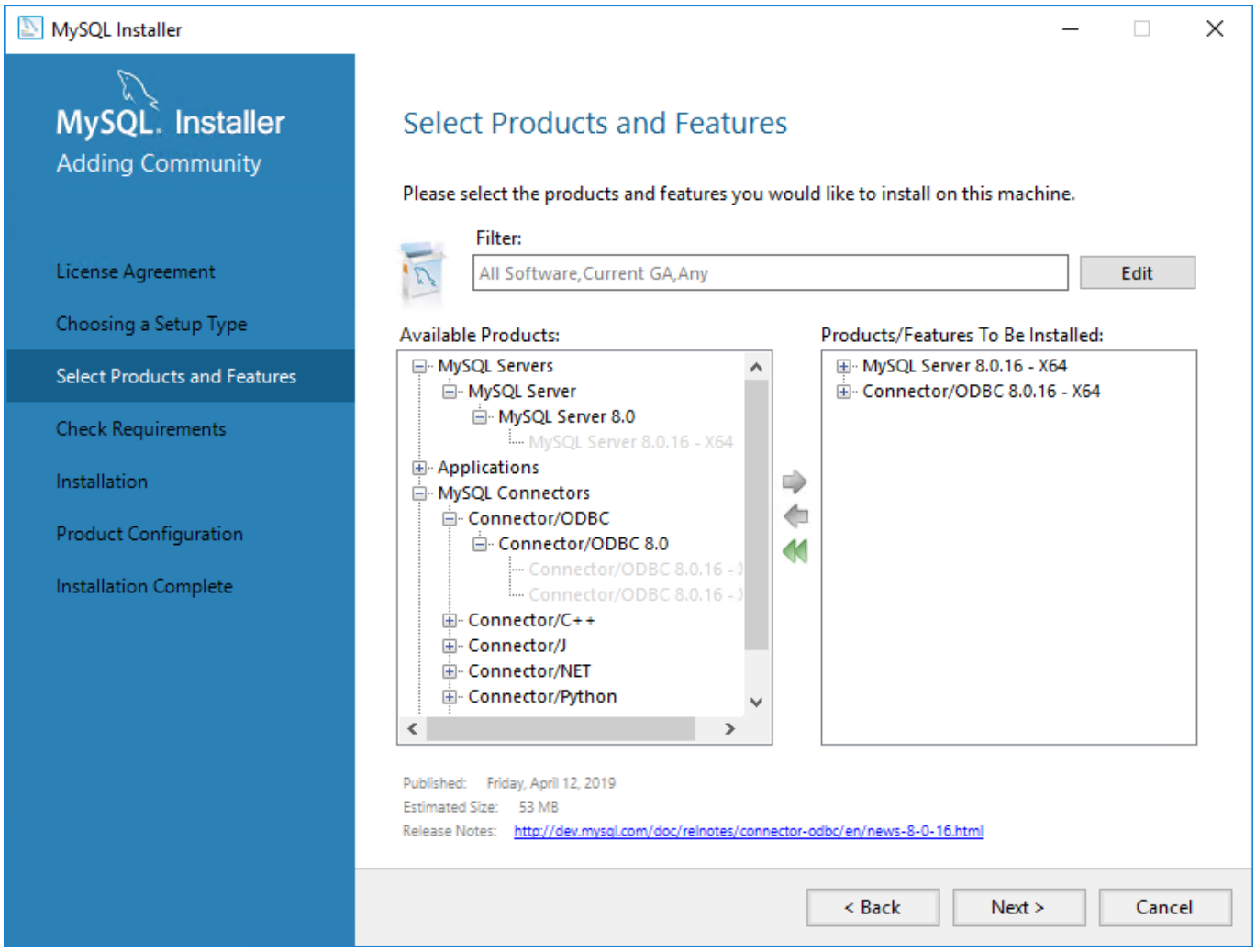
Instalación

Asegúrese de instalar una versión compatible de MySQL Server y ODBC Connector.

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

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

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



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

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

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

7. En el **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 su **contraseña raíz 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 preseleccionados y haga clic en **Siguiente**.

10. Haga clic en **Ejecutar** y espere hasta que finalice la instalación del servidor MySQL. 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. Encuentre y edite o añada la siguiente configuración en 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 su versión 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`	Como alternativa, puede deshabilitar la creación de registros binarios: `log_bin=0`	Versiones 8.x compatibles
`innodb_log_file_size=100M`	La multiplicación de los valores de estos dos parámetros debe ser como mínimo **200**. El valor mínimo para `innodb_log_files_in_group` es **2**, y el máximo es **100**;; además, el valor debe ser entero.	Versiones 8x compatibles 5.7 5.6.22 (y versiones posteriores 5.6.x)
`innodb_log_files_in_group=2`		
`innodb_log_file_size=200M`	Configure un valor mínimo de**200M**, pero no mayor de **3000M**.	5.6.20 y 5.6.21

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

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

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

5. Ingrese el siguiente comando en el Símbolo del sistema para verificar si se está ejecutando el servidor

MySQL:

```
sc query mysql80
```

Cuenta de usuario con base de datos dedicada

Si no desea usar una **cuenta SA** (MS SQL) o una **cuenta raíz** (MySQL), puede crear una **cuenta de usuario con base de datos dedicada**. Esta cuenta de usuario dedicada se usará para acceder solo a la base de datos ESET PROTECT. Le recomendamos crear una cuenta de usuario con base de datos dedicada dentro de su servidor de base de datos antes de comenzar con la instalación de ESET PROTECT. Además, necesitará crear una base de datos vacía a la que podrá acceder por ESET PROTECT mediante esta cuenta de usuario dedicada.

Debe otorgar un conjunto mínimo de privilegios a una cuenta de usuario de base de datos dedicada:

- Privilegios del usuario 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.

- Roles a nivel de la base de datos del Servidor Microsoft SQL: El usuario de la base de datos ESET PROTECT debe ser miembro del rol de la base de datos db_owner. Para obtener más información sobre los roles a nivel de la base de datos del Servidor Microsoft SQL, consulte https://msdn.microsoft.com/en-us/library/ms189121%28v=sql.100%29.aspx.

Puede encontrar una guía detallada sobre cómo configurar su base de datos y cuenta de usuario para MS SQL y MySQL en nuestro artículo de base de conocimiento.

Instalación del agente: Windows

Métodos disponibles

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

Método	Documentación	Descripción
Instalación basada en la GUI desde el instalador de *.msi*	• Este capítulo • KB	• El método de instalación **estándar**. • Este método puede ejecutarse como una instalación asistida por servidor o sin conexión. • Use este método cuando instale el agente en el equipo del servidor de ESET PROTECT.
ESET Remote Deployment Tool	• Ayuda en línea	• Recomendado para implementación masiva a través de una red local. • Se puede usar para implementar el instalador todo en uno (agente + producto de seguridad de ESET)
Instalador de agente todo en uno	• Crear instalador del Agente todo en uno • KB	• El instalador puede incluir también un producto de seguridad y una política incorporada. • El tamaño del instalador es varios cientos de MB.

Método	Documentación	Descripción
Script del instalador de agentes	• Crear instalador de scripts del agente • KB	• El instalador es un script ejecutable. Tiene un pequeño tamaño pero necesita acceso a la ubicación del instalador *.msi*. • El script puede editarse para usar un instalador local y Proxy HTTP.
Implementación de SCCM y GPO	• SCCM • GPO • KB	• Método avanzado de implementación masiva remota. • Con un pequeño archivo *.ini*.
Tarea de servidor: implementación del agente	• Ayuda en línea • KB	• Una alternativa a SCCM y GPO. • No es viable a través de Proxy HTTP. • Ejecutado por el servidor de ESET PROTECT desde la consola web de ESET PROTECT.

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

Instalación basada en la GUI

Siga los pasos indicados a continuación para instalar el componente del Agente de ESET Management de forma local en Windows:

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

2. Ejecute el instalador del Agente ESET Management y acepte el acuerdo de licencia de usuario final (EULA) si está de acuerdo.

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

4. Ingrese el **Host del servidor** (nombre de host o dirección de IP de su Servidor de ESET PROTECT) y el **Puerto del servidor** (el puerto predeterminado del servidor es 2222; si usa un puerto diferente, reemplace el puerto predeterminado por su número de puerto personalizado).

Asegúrese de que el **Host del servidor** coincide al menos con uno de los valores (idealmente FQDN) definidos en el campo **Host** del **Certificado del servidor**. De lo contrario, obtendrá un mensaje de error que dice “El certificado del servidor recibido no es válido”. Un comodín (*) en el campo host del certificado del servidor permitirá al certificado funcionar con cualquier **host de servidor**.

5. Si usa un proxy para la conexión entre el Agente y el Servidor, seleccione la casilla de verificación junto a **Usar Proxy**. Al seleccionar la casilla, el instalador continuará con instalación fuera de línea.

Esta configuración de proxy sólo se usa para (replicación) entre el Agente de ESET Management y el Servidor de ESET PROTECT, no para almacenar actualizaciones en caché.
- **Nombre de host del proxy**: nombre de host o dirección IP de la máquina del Proxy HTTP.
- **Puerto del Proxy**: el valor predeterminado es 3128.
- **Nombre de usuario**, **Contraseña**: ingrese las credenciales que usa su proxy si usa autenticación.

Puede cambiar la configuración de proxy más adelante en su política. El Proxy debe instalarse antes de que pueda configurar la conexión entre el Agente y el Servidor vía Proxy.

6. Seleccione una de las siguientes opciones de instalación y siga los pasos de la sección adecuada que aparece a continuación:

- Instalación asistida por Servidor: necesitará credenciales de administrador de Consola web de ESET PROTECT. El instalador descargará los certificados necesarios automáticamente.

No puede usar un usuario con autenticación de dos factores para instalaciones asistidas por el servidor.

- Instalación fuera de línea: necesitará proporcionar un Certificado de Agente y una Autoridad de certificación. Ambos pueden exportarse desde ESET PROTECT. Como alternativa, puede usar su certificado personalizado.

Instalación mediante la línea de comandos

El instalador *MSI* puede ejecutarse de forma local o remota. Descargue el agente ESET Management desde el sitio web de ESET.

Parámetro	Descripción y valores permitidos
P_HOSTNAME=	Nombre de host o dirección IP del servidorESET PROTECT.
P_PORT=	Puerto de servidor para la conexión del agente (opcional; si no se especifica, se usa el puerto predeterminado 2222).
P_CERT_PATH=	Ruta al certificado del agente en formato Base64 en el archivo *.txt* (exportado desde la consola web de ESET PROTECT).
P_CERT_AUTH_PATH=	Ruta a la autoridad de certificación 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 consulte el certificado del agente y la autoridad de certificación almacenados en los archivos *.txt*.
P_CERT_PASSWORD=	Use este parámetro para proporcionar una contraseña para el certificado del agente.
P_CERT_CONTENT=	Cadena del certificado del agente en formato Base64 (exportada desde la consola web de ESET PROTECT).
P_CERT_AUTH_CONTENT=	Cadena de la autoridad de certificación en formato Base64 (exportada desde la consola web de ESET PROTECT).
PASSWORD=	Contraseña de desinstalación de un Agente protegido con contraseña.

Parámetro	Descripción y valores permitidos
P_ENABLE_TELEMETRY=	**0**: deshabilitado (opción predeterminada); **1**: habilitado. Envío de informes de error y datos de telemetría a ESET (parámetro opcional).
P_INSTALL_MODE_EULA_ONLY=	**1**; use este parámetro para la instalación del agente ESET Management semi silenciosa. Podrá ver la ventana de instalación del agente y se le solicitará que acepte el Acuerdo de licencia de usuario final y que habilite/deshabilite la telemetría (P_ENABLE_TELEMETRY se ignora cuando se especifica). Otras configuraciones de instalación del agente se toman de los parámetros de la línea de comandos. Podrá ver la finalización del proceso de instalación del agente.
P_USE_PROXY=	**1**; use este parámetro para habilitar el uso de HTTP Proxy (que ya está instalado en su red) para la replicación entre el agente ESET Management y el servidor de ESET PROTECT (no para el almacenamiento en caché de actualizaciones).
P_PROXY_HTTP_HOSTNAME=	Nombre de host o dirección IP de Proxy HTTP.
P_PROXY_HTTP_PORT=	Puerto de Proxy HTTP para la conexión del agente.

Ejemplos de instalación mediante la línea de comandos

Reemplace el siguiente código naranja según sea necesario.

- Instalación silenciosa (parámetro `/q`) con conexión de puerto predeterminado, telemetría habilitada y certificado de agente y autoridad de certificación 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 de agente, para la autoridad de certificación y la contraseña del certificado del agente, así como los parámetros de 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 semi silenciosa:

```
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 asistida por servidor

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

1.Ingrese el nombre de host o la dirección IP de la Consola web ESET PROTECT (la misma que el Servidor ESET PROTECT) en el campo **host del servidor**. Deje el **puerto de la consola web** en el puerto predeterminado 2223 si no usa un puerto personalizado. Además, ingrese sus credenciales de cuenta de la consola web en los **camposnombre de usuario y contraseña**. Para iniciar sesión como un usuario de dominio, seleccione la casilla de verificación situada junto a **Iniciar sesión en el dominio.**

- Asegúrese de que el **Host del servidor** coincide al menos con uno de los valores (idealmente FQDN) definidos en el campo **Host** del **Certificado del servidor**. De lo contrario, obtendrá un mensaje de error que dice “El certificado del servidor recibido no es válido”. La única excepción es en caso de haber un comodín (*) en el campo host del certificado del servidor, que significa que funcionará con cualquier **host de servidor**.
- No puede usar un usuario con autenticación de dos factores para instalaciones asistidas por el servidor.

2. Haga clic en **Sí** cuando se le pida si desea aceptar el certificado.

3. Seleccione **No crear equipo (se creará automáticamente durante la primera conexión)** o **Elegir grupo estático personalizado**. Si hace clic en **Seleccionar grupo estático personalizado** podrá seleccionar desde un listado de grupos estáticos existentes en ESET PROTECT. El equipo se agregará al grupo seleccionado.

4. Especifique la carpeta de destino para el Agente ESET Management (recomendamos usar la predeterminada), haga clic en **Siguiente** y luego en **Instalar**.

Instalación del agente fuera de línea

Para continuar con la **instalación del agente fuera de línea,** 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 3128),**Nombre de usuario** y **Contraseña** y haga clic en **Siguiente**.

2. Haga clic en **Examinar** y navegue hasta la ubicación del certificado de pares (este es el certificado de agente que exportó desde ESET PROTECT). Deje en blanco el área de **Contraseña del certificado** porque este certificado no necesita una contraseña. No necesita buscar una **Autoridad de certificación** - deje el campo en blanco.

Si usa un certificado personalizado con ESET PROTECT (en vez del predeterminado que se generó automáticamente durante la instalación de ESET PROTECT), use sus certificados personalizados según corresponda.

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

3. Haga clic en **Siguiente** para instalar en la carpeta predeterminada o haga clic en **Cambiar** para elegir otra carpeta (recomendamos usar la ubicación predeterminada).

ESET Remote Deployment Tool

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

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

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

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

Instalación de la consola web: Windows

Puede instalar la consola web ESET PROTECT en Windows de dos maneras:

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

Puede instalar la consola web de ESET PROTECT en un equipo diferente a donde se ejecuta el servidor de ESET PROTECT.

Instalar la consola web con el instalador todo en uno

Requisitos previos

- Se instaló el servidor de ESET PROTECT.

Puede instalar la consola web de ESET PROTECT en un equipo diferente a donde se ejecuta el servidor de ESET PROTECT. Este procedimiento requiere pasos adicionales.

- Apache Tomcat es un componente obligatorio necesario para ejecutar la consola web de ESET PROTECT.
- Apache Tomcat requiere Java/OpenJDK de 64 bits. Si tiene muchas versiones de Java instaladas en su sistema, le recomendamos desinstalar las versiones anteriores de Java y solo dejar la última versión 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 pasar a una alternativa sin costo. Consulte las versiones compatibles de JDK.

Instalación

Para instalar el componente de la consola web ESET PROTECT en Windows con el instalador todo en uno:

Asegúrese de cumplir con todos los requisitos previos de 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 quiere instalar la versión más reciente de Apache Tomcat y el instalador todo en uno contiene una versión anterior 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 vaya a la carpeta *installers*.

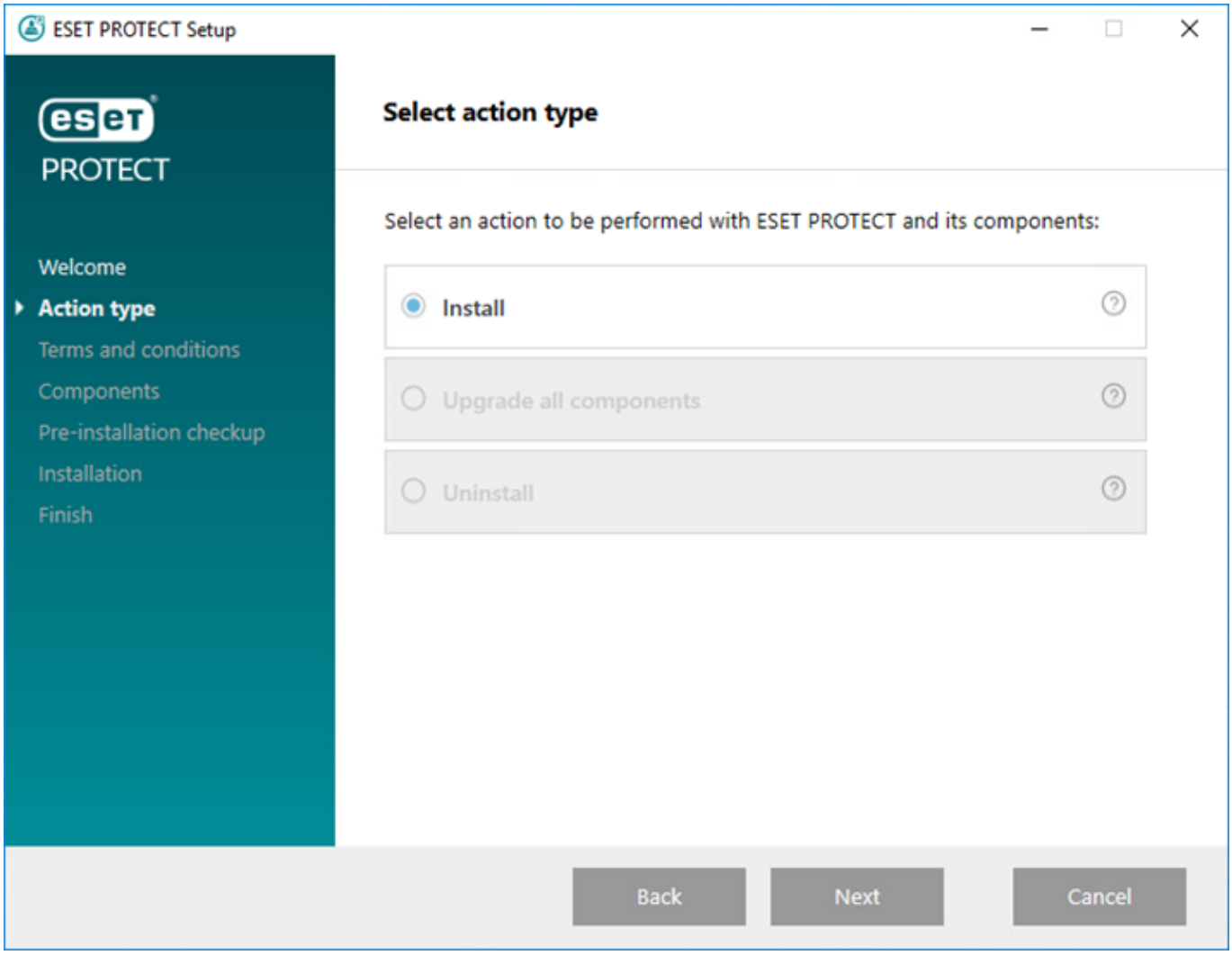
   b. Quite el archivo *apache-tomcat-9.0.x-windows-x64.zip* ubicado en la carpeta *installers*.

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

   d. Mueva el paquete con el archivo comprimido descargado a la carpeta *installers*.

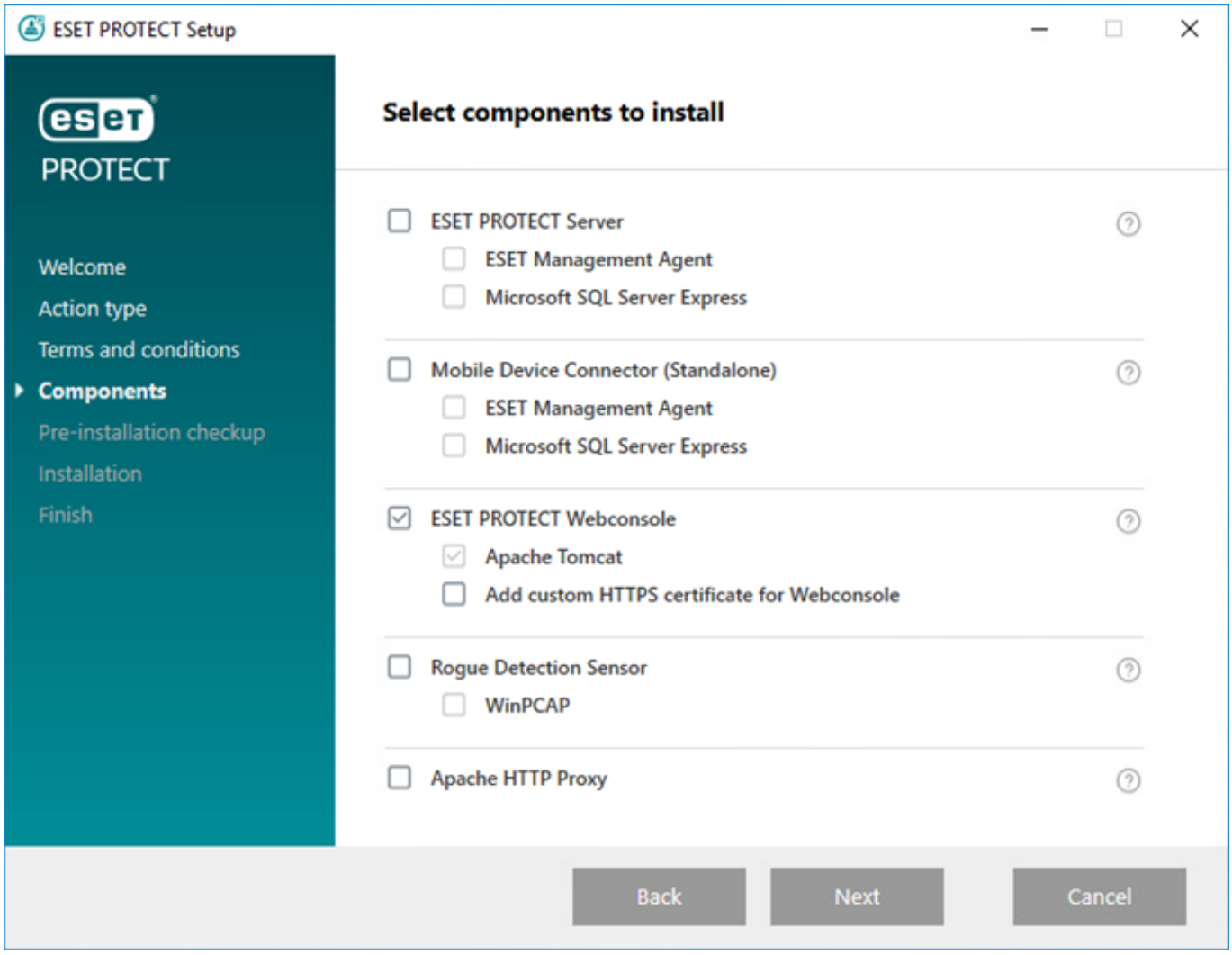
3. Para ejecutar el instalador todo en uno, haga doble clic en el archivo *Setup.exe* y, luego, en **Siguiente** en la pantalla de **Bienvenida**.

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



5. Luego de aceptar el EULA, haga clic en **Siguiente**.

6. En **Seleccionar los componentes a instalar**, seleccione únicamente la casilla de verificación consola web **ESET PROTECT** y haga clic en **Siguiente**.

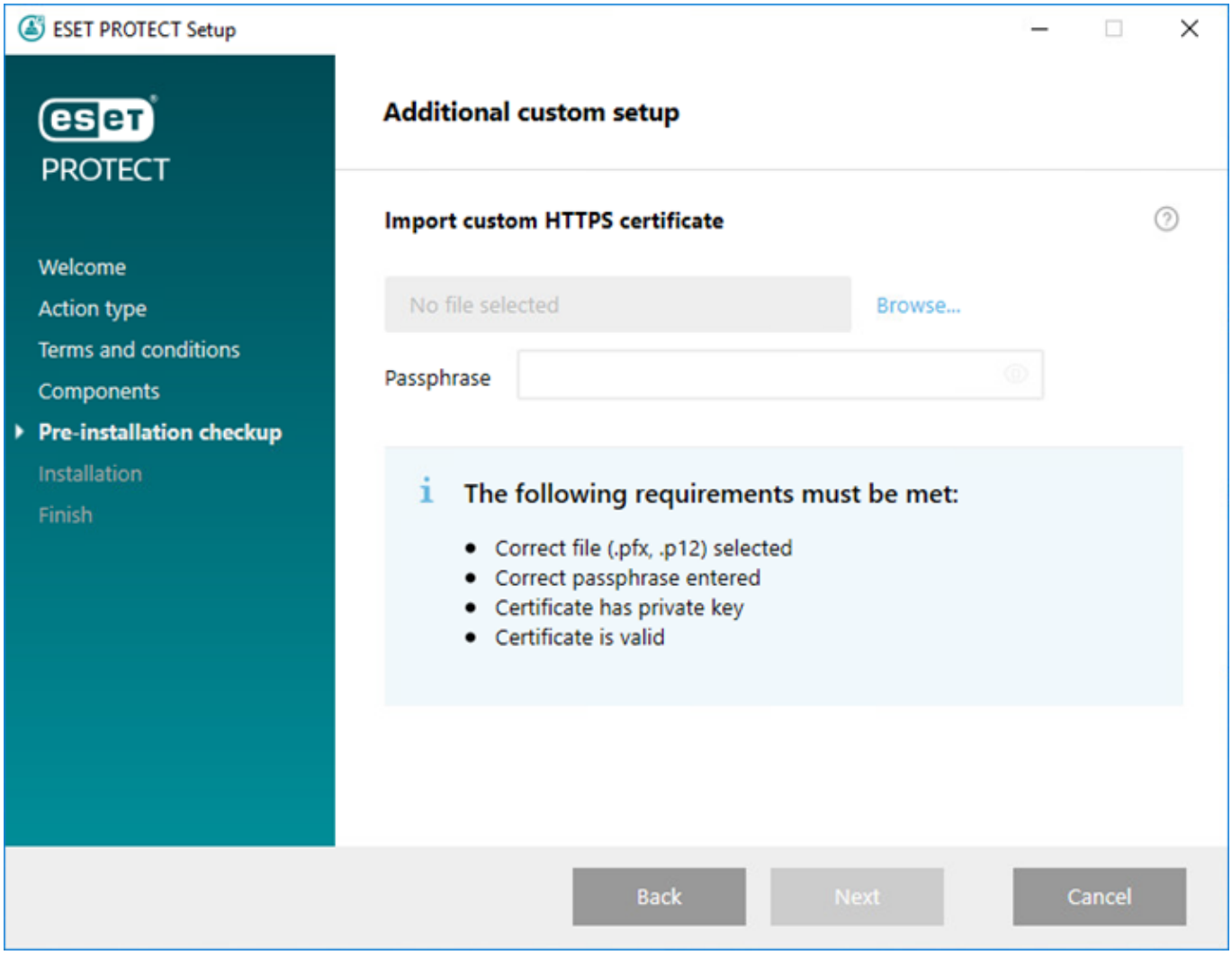


De manera opcional, puede seleccionar la casilla de verificación **Agregar un certificado HTTPS personalizado para la consola web**.

- Seleccione esta opción si desea agregar un certificado HTTPS personalizado para la consola web de ESET PROTECT.

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

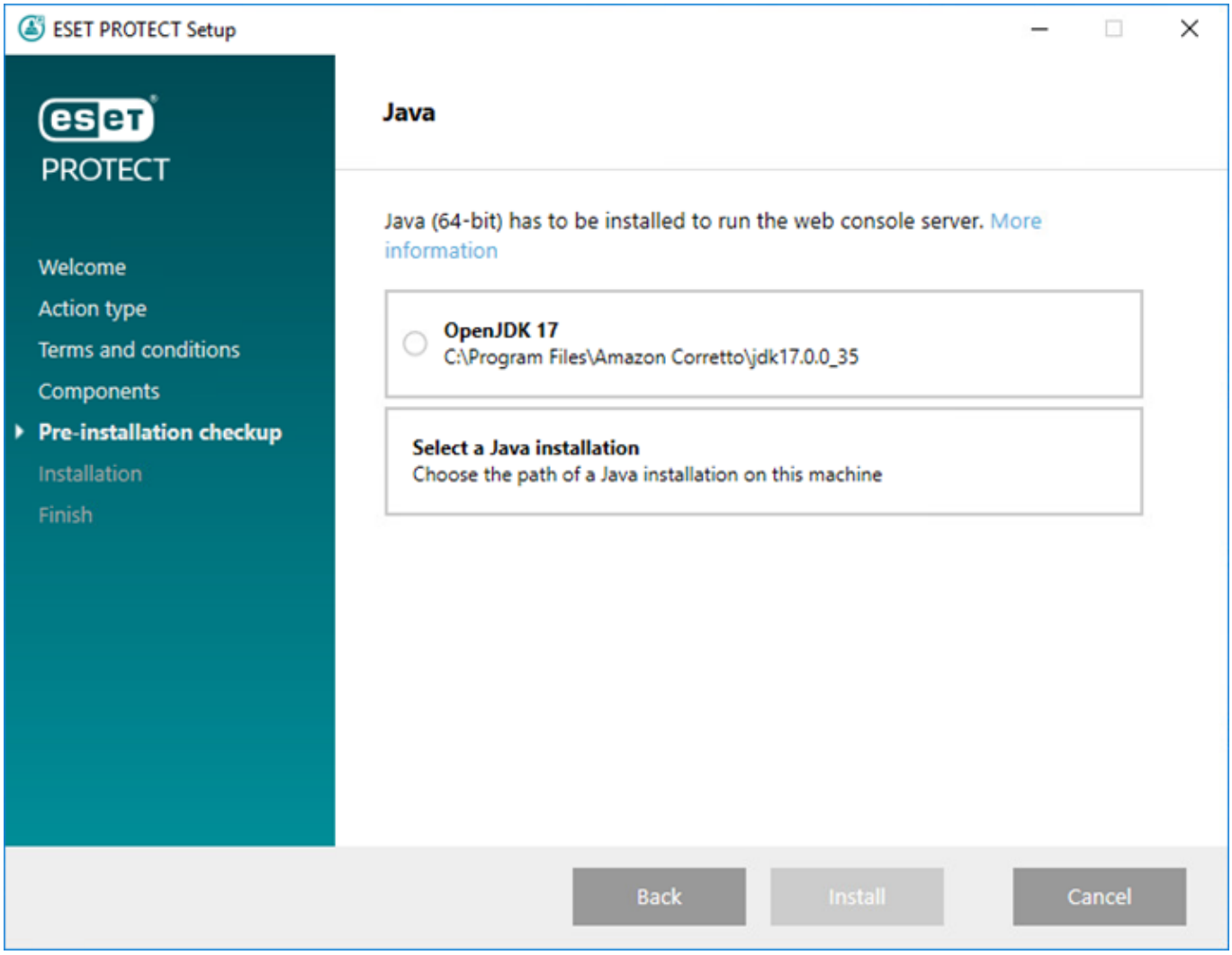
- Si seleccionó **Agregar un certificado HTTPS personalizado para la consola web**, haga clic **Navegar** y seleccione un certificado válido (archivo *.pfx* o .p12) y escriba su **frase de contraseña** (o deje el campo en blanco si no hay frase de contraseña). El instalador instalará el certificado para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



7. Seleccione una instalación de Java en el equipo. Compruebe estar usando la última versión de Java/OpenJDK.

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

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



8. Cuando la instalación esté completa, haga clic en **Finalizar**.

Si instaló la Consola Web de ESET PROTECT en un equipo diferente al del Servidor de ESET PROTECT, realice estos pasos adicionales para permitir la comunicación entre la Consola Web de ESET PROTECT y el Servidor de ESET PROTECT:
a)Detenga el servicio de Apache Tomcat: Vaya a **Inicio** > **Servicios** > haga clic con el botón derecho en el servicio Apache Tomcat y seleccione **Detener**.
b)Ejecute Notepad 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)Busque`server_address=localhost`.
d)Sustituya `localhost` por la dirección IP de su Servidor de ESET PROTECT y guarde el archivo.
e) Inicie el servicioApache Tomcat. Vaya a **Inicio** > **Servicios** > haga clic con el botón derecho en el servicio Apache Tomcat y seleccione **Iniciar**.

9. Abra la consola web de ESET PROTECT en su navegador web compatible, se mostrará una pantalla de inicio de sesión.

- Desde el equipo en el que se aloja la consola web ESET PROTECT: *https://localhost/era*

- Desde cualquier equipo con acceso a Internet a la consola web ESET PROTECT (sustituya *IP_ADDRESS_OR_HOSTNAME* con la dirección IP o el nombre de host de su consola webESET PROTECT): *https://IP_ADDRESS_OR_HOSTNAME/era*

Consulte también la Configuración adicional de la consola web para soluciones empresariales o sistemas de bajo rendimiento.

Instalar la consola web manualmente

La instalación manual de la consola web ESET PROTECT es un procedimiento avanzado. Le recomendamos instalar la consola web ESET PROTECT con el instalador todo en uno.

Requisitos previos

- Se instaló el servidor de ESET PROTECT.

Puede instalar la consola web de ESET PROTECT en un equipo diferente a donde se ejecuta el servidor de ESET PROTECT. Este procedimiento requiere pasos adicionales.

- Apache Tomcat es un componente obligatorio necesario para ejecutar la consola web de ESET PROTECT. Instale Apache Tomcat:

  a)Descargue la última versión compatible del archivo instalador Apache Tomcat (32-bit/64-bit Windows Service Installer) *apache-tomcat-[versión].exe* de https://tomcat.apache.org.

  a)Ejecute el instalador.

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

  c)Después de la instalación, asegúrese de que el servicio Apache Tomcat se esté ejecutando y que su tipo de inicio esté establecido en **Automático** (en **services.msc**).

- Apache Tomcat requiere Java/OpenJDK de 64 bits. Si tiene muchas versiones de Java instaladas en su sistema, le recomendamos desinstalar las versiones anteriores de Java y solo dejar la última versión 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 pasar a una alternativa sin costo. Consulte las versiones compatibles de JDK.

Instalación

Para instalar el componente de la Consola web ESET PROTECT en Windows, siga los pasos a continuación:

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

1. Visite la sección de descarga de ESET PROTECT para descargar un instalador independiente para el componente de ESET PROTECT. (Consola web *era.war*).

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

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

3. Apache Tomcat extrae automáticamente el archivo *era.war* en la carpeta *era* e instala la 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 instaló la consola web ESET PROTECT en el mismo equipo que el servidor de ESET PROTECT, reinicie el servicio de Apache Tomcat. Vaya a **Inicio** > **Servicios** > haga clic con el botón derecho en el servicio Apache Tomcat y seleccione **Detener**. Haga clic en Detener, espere 30 segundos y luego haga clic en**Inicio**.

Si instaló la Consola Web de ESET PROTECT en un equipo diferente al del Servidor de ESET PROTECT, realice estos pasos adicionales para permitir la comunicación entre la Consola Web de ESET PROTECT y el Servidor de ESET PROTECT:
a)Detenga el servicio de Apache Tomcat: Vaya a **Inicio** > **Servicios** > haga clic con el botón derecho en el servicio Apache Tomcat y seleccione **Detener**.
b)Ejecute Notepad 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)Busque`server_address=localhost`.
d)Sustituya `localhost` por la dirección IP de su Servidor de ESET PROTECT y guarde el archivo.
e) Inicie el servicioApache Tomcat. Vaya a **Inicio** > **Servicios** > haga clic con el botón derecho en el servicio Apache Tomcat y seleccione **Iniciar**.

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

- Desde el equipo en el que se aloja la consola web ESET PROTECT: *http://localhost:8080/era*

- Desde cualquier equipo con acceso a Internet a la consola web ESET PROTECT (sustituya *IP_ADDRESS_OR_HOSTNAME* con la dirección IP o el nombre de host de su consola webESET PROTECT): *http://IP_ADDRESS_OR_HOSTNAME:8080/era*

6. Configure la consola web después de la instalación:

- El puerto HTTP predeterminado se define en 8080 durante la instalación manual de Apache Tomcat. Le recomendamos que configure una conexión HTTPS para Apache Tomcat.

- Consulte también la Configuración adicional de la consola web para soluciones empresariales o sistemas de bajo rendimiento.

Instalación de HTTP Proxy

Acerca de Proxy HTTP

El proxy HTTP reenvía la comunicación cifrada entre el agente de ESET Management y el servidor de ESET PROTECT. De forma predeterminada, ESET PROTECT usa Apache HTTP Proxy como Proxy HTTP.

Use el Proxy HTTP solo si su agente ESET Management no tiene visibilidad de red para el servidor de ESET PROTECT. El Proxy HTTP no agrega la comunicación ni reduce el tráfico de red.

Se recomienda tener el agente ESET Management en la máquina con el Proxy HTTP, pero no es necesario. El agente ESET Management no puede administrar (configurar) la aplicación de Proxy HTTP.

- Arquitectura de Proxy HTTP

- Arquitectura de Apache HTTP Proxy

- Escenarios avanzados para Proxy HTTP

Antes de la instalación

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

Instalación y configuración

Puede instalar Apache HTTP Proxy desde un instalador separado o desde el instalador todo en uno de ESET PROTECT.

- La instalación desde el instalador todo en uno requiere que descargue el paquete completo, pero es más simple. Ejecute el instalador descargado y seleccione solo el **Apache HTTP Proxy** desde el selector de instaladores. Una vez que Apache esté instalado, debe configurarse.

- La instalación desde el instalador independiente es más avanzada; sin embargo, el tamaño de descarga son unos pocos MB. Consulte las instrucciones de instalación y configuración.

Configurar el proxy HTTP para una gran cantidad de clientes

Si usa un Apache HTTP Proxy de 64 bits, puede aumentar el límite de subprocesos para su Apache HTTP Proxy. Edite el archivo de configuración de *httpd.conf*, dentro de la carpeta Apache HTTP Proxy. Encuentre los siguientes ajustes en el archivo y actualice los valores para que coincidan con la cantidad de clientes.

Substituya el valor de ejemplo de `5000` con su cantidad. El valor máximo es `32000`.

```
ThreadLimit 5000
```

```
ThreadsPerChild 5000
```

No cambie el resto del archivo.

Instalación del RD Sensor: Windows

Requisitos previos

- WinPcap: usar la versión más reciente de WinPcap (al menos 4.1.0)

- La red debe estar configurada de forma correcta (puertos adecuados abiertos, comunicación entrante no bloqueada por un firewall, etc.).

- Servidor de ESET PROTECT accesible

- El Agente ESET Management debe estar instalado en el equipo local para que sea compatible con todas las características del programa

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

Instalación

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

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

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

2. Haga doble clic en el archivo instalador del RD Sensor para comenzar la instalación.

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

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

5. Seleccione la ubicación de instalación del 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 producir una lista completa de todos los dispositivos de toda la red.

Herramienta de replicación: Windows

¿Es usuario de Linux?

La herramienta de replicación es necesaria para la actualizaciones del motor de detección fuera de línea. Si los equipos de su cliente no tienen conexión a Internet y necesitan actualizaciones del motor de detección, puede usar la herramienta de replicación para descargar los archivos de actualización de los servidores ESET y almacenarlos localmente.

La Herramienta de replicación descarga solamente actualizaciones del motor de detección y otros módulos del programa; no descarga PCU (Actualizaciones de componentes del programa) ni datos de ESET LiveGrid®. Además, puede crear un repositorio fuera de línea completo. Alternativamente, puede actualizar individualmente los productos.

Requisitos previos

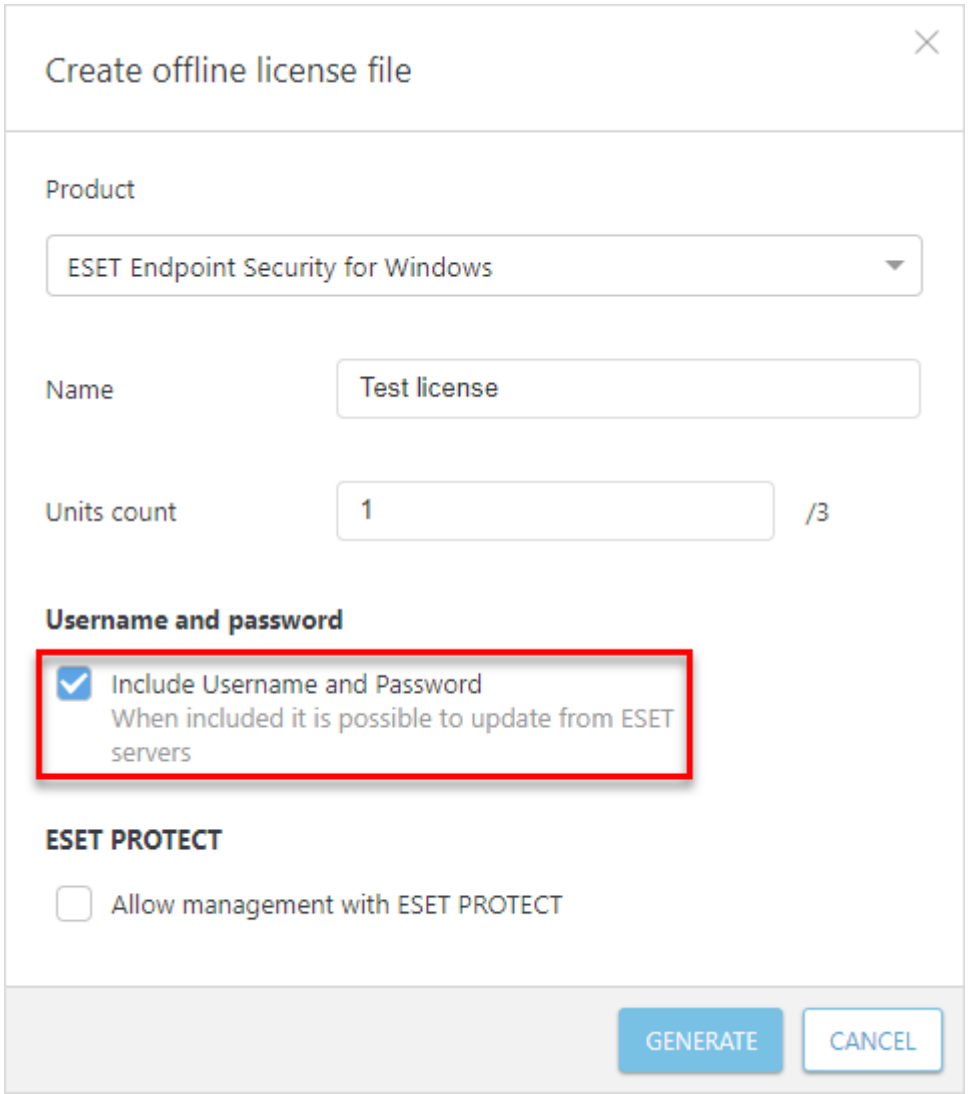
La herramienta de replicación no es compatible con Windows XP ni Windows Server 2003.

- La carpeta de destino debe estar disponible para el uso compartido, servicio Samba/Windows o HTTP/FTP, según cómo desea tener accesibles las actualizaciones.

  - Productos de seguridad de ESET para Windows: puede actualizarlos de forma remota con 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 fuera de línea válido que incluye el nombre de usuario y la contraseña. Cuando genere un archivo de licencia, asegúrese de seleccionar la casilla de verificación junto a **Incluir nombre de usuario y contraseña**. Además, debe ingresar un **nombre** de licencia. Se necesita un archivo de licencia fuera de línea para la activación de la herramienta de replicación y la generación de la replicación de la actualización.



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

Como usar la herramienta de replicación

1.Descargue la herramienta de replicación de la página de descarga de ESET (sección **Instaladores independientes**).

2.Descomprima el archivo descargado.

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

4.Ejecute el siguiente comando para ver todos los parámetros disponibles para la herramienta de replicación 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 diferencian entre mayúsculas y minúsculas.

Parámetro	Descripción
`--updateServer`	Cuando lo usa, debe especificar el URL completo del servidor de actualización.
`--offlineLicenseFilename`	Debe especificar una ruta hacia su archivo de licencia fuera de línea (como se mencionó arriba).
`--mirrorOnlyLevelUpdates`	No se necesita ningún argumento. Si está configurado, se descargarán únicamente las actualizaciones de nivel (no se descargarán las actualizaciones nano). Obtenga más información sobre los tipos de actualización en nuestro artículo de la base de conocimiento.
`--mirrorFileFormat`	Antes de usar el parámetro `--mirrorFileFormat`, asegúrese de que el entorno no contenga ambas versiones del producto de seguridad de ESET, es decir, la anterior (6.5 y anteriores) y la más nueva (6.6 y posteriores). El uso incorrecto de este parámetro puede tener como resultado actualizaciones incorrectas en sus productos de seguridad ESET. Puede indicar qué tipo de archivos de actualización se descargarán. Valores posibles (distingue entre mayúsculas y minúsculas): • `dat`: use este valor si tiene un entorno solo con versiones del producto de seguridad ESET 6.5 y anteriores. • `dll`: use este valor si tiene un entorno solo con versiones del producto de seguridad ESET 6.6 y posteriores. El parámetro se ignora cuando se crea una replicación para los productos de legado (`ep4`, `ep5`).
`--compatibilityVersion`	Este parámetro opcional se aplica a la herramienta de replicación distribuida con ESET PROTECT 8.1 y versiones posteriores. La herramienta de replicación 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 de repositorio distribuidos con ESET PROTECT 9: `--filterFilePath` y `--dryRun`:
1.Cree un filtro en un formato *JSON* (ver `--filterFilePath` a continuación).
2.Ejecute una herramienta de replicación de prueba ejecutada con el parámetro `--dryRun` (ver a continuación) y ajuste el filtro según sea necesario.
3.Ejecute la herramienta de replicación con el parámetro `--filterFilePath` y el filtro de descarga definido, junto con los parámetros `--intermediateRepositoryDirectory` y `--outputRepositoryDirectory`.
4.Ejecute la herramienta de replicación periódicamente para utilizar siempre los instaladores más recientes.

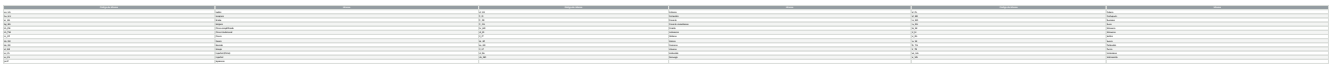
Parámetro	Descripción

`--filterFilePath`	Use este parámetro opcional para filtrar productos de seguridad de ESET en función de un archivo de texto en formato *JSON* situado en la misma carpeta que la herramienta de replicación, por ejemplo: `--filterFilePath filter.txt`)
	Descripción de 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 verdadero, se incluirán productos heredados.
	o`defaults` (objeto *JSON*, opcional): define las propiedades del filtro que se aplicará a todos los productos.
	■`languages` (lista): especifique los códigos de idioma de los idiomas ISO que desea incluir, por ejemplo, para el tipo francés `"fr_FR"`. La siguiente tabla contiene 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 incluirán (`["x64", "x86", "arm64"]`).
	⚠ Use el filtro `platforms` con cuidado. Por ejemplo, si la herramienta de replicación descarga solo instaladores de 64 bits y su infraestructura contiene equipos de 32 bits, los productos de seguridad de ESET de 64 bits no se instalarán en equipos de 32 bits.
	■`os_types` (lista): tipos de SO que se incluirán (`["windows"]`, `["linux"]`, `["mac"]`).
	o`products` (lista de objetos JSON, opcional): filtros que se aplican a productos específicos; anulación de `defaults` para productos especificados. Los objetos tienen las siguientes propiedades:
	■`app_id` (cadena): necesario si no se especifica `name`.
	■`name` (cadena), necesario si no se especifica `app_id`.
	■`version` (cadena): especifica la versión o el intervalo de versiones que se incluirán.
	■`languages` (lista): códigos de idioma ISO de los idiomas que se incluirán (consulte la tabla que aparece a continuación).
	■`platforms` (lista): plataformas que se incluirán (`["x64", "x86", "arm64"]`).
	■`os_types` (lista): tipos de SO que se incluirán (`["windows"]`, `["linux"]`, `["mac"]`).
	ℹ Para determinar los valores adecuados para los campos, ejecute la herramienta de replicación en el modo simulacro y busque el producto correspondiente en el archivo CSV creado.
	Descripciones de formato de la cadena de versiones
	Todos los números de versión están compuestos por cuatro números separados por puntos (por ejemplo, `7.1.0.0`). Puede especificar menos números al escribir filtros de versión (por ejemplo, `7.1`) y el resto de los números será cero (`7.1` es igual a `7.1.0.0`).
	La cadena de versiones puede tener uno de los dos formatos siguientes:
	• [>|<|>=|<=|=]<n>.(<n>.(<n>.(<n>)))
	oSelecciona las versiones posteriores/inferiores o iguales/inferiores, iguales/iguales que la versión especificada.
	• <n>.(<n>.(<n>.(<n>))) - <n>.(<n>.(<n>.(<n>)))
	oSelecciona las versiones que son posteriores o iguales que el límite inferior e inferior o igual que el límite superior.
	Las comparaciones se realizan de forma sencilla 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` reemplaza a los parámetros `--languageFilterForRepository`, `--productFilterForRepository` y `--downloadLegacyForRepository` utilizados en versiones anteriores de la herramienta de replicación (lanzados con ESET PROTECT 8.x).

Parámetro	Descripción
`--dryRun`	Si usa este parámetro opcional, la herramienta de replicación no descargará ningún archivo, pero generará un archivo *.csv* con una lista de todos los paquetes que se descargarán. Puede usar 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 de replicación los incluirá en el archivo *.csv* aunque especifique `idiomas` en `--filterFilePath`. Si usa el parámetro `--dryRun` y también los parámetros `--intermediateRepositoryDirectory` y `--outputRepositoryDirectory`, la herramienta de replicación no borra el *outputRepositoryDirectory*.
`--listUpdatableProducts`	Enumere 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 de Mirror Tool: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).

La herramienta de replicación crea una estructura de carpetas diferente de lo que hace la replicación de punto de conexión. Cada carpeta contiene archivos de actualización de productos. Debe especificar la ruta completa a la carpeta correcta en la configuración de la actualización del producto con la replicación. Por ejemplo, para actualizar ESET PROTECT 9 de la replicación, establezca el Actualizar servidor en (de acuerdo con la ubicación raíz de su servidor HTTP):
`http://your_server_address/mirror/eset_upd/era6`
Nota: La carpeta mirror `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 fuera de línea con productos seleccionados, idiomas y descarga habilitada de archivos anteriores, definidos en el archivo *filter.txt* (ver el ejemplo anterior de contenido del archivo en `--filterFilePath` detalle):

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

Configuración de herramienta de replicación y actualización

- Para automatizar las descargas para las actualizaciones de módulos, puede crear un programa para ejecutar la herramienta de replicación. Para ello, abra su consola web y vaya a **Tareas de clientes** > **Sistema operativo** > **Ejecutar comando. Seleccione Línea de comandos a ejecutar** (incluso una ruta a *MirrorTool.exe*) y un activador razonable (como CRON para cada hora 0 0 * * * ? *). Como alternativa, puede usar el programador de tareas de Windows o `Cron` en Linux.

- Para configurar las actualizaciones en un equipo del cliente, cree una nueva política y configure **Actualizar servidor** para apuntar a su dirección de replicación o carpeta compartida.

Si usa un servidor de replicación HTTPS, debe importar el certificado en el almacenamiento raíz de confianza en la máquina cliente. Consulte Cómo instalar un certificado raíz confiable en Windows.

Lea este artículo de la base de conocimiento para configurar el encadenamiento de la herramienta de replicación (configure la herramienta de replicación para descargar actualizaciones desde otra herramienta de replicación).

Instalación del Conector de dispositivo móvil – Windows

Se debe poder acceder al conector de dispositivo móvil desde Internet para que los dispositivos móviles se puedan administrar en todo momento sin importar su ubicación.

Le recomendamos que despliegue su componente MDM en un dispositivo host aparte de donde está alojado el Servidor de ESET PROTECT.

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

Asegúrese de cumplir con todos los requisitos previos de instalación.

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

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

3. Haga clic en **Examinar**, navegue hacia la ubicación de su certificado SSL para comunicarse por HTTPS, ingrese la contraseña para este certificado.

4. Especifique el **Nombre de host de MDM**: es el dominio público o dirección IP pública de su servidor MDM ya que se localiza mediante los dispositivos móviles desde Internet.

Debe introducir el nombre del host MDM en la misma forma que se especifica en su **certificado de servidor HTTPS**; de lo contrario, el dispositivo móvil iOS rechazará la instalación del Perfil MDM. Por ejemplo, si hay una dirección IP especificada en el certificado HTTPS, escriba esta dirección IP en el campo **nombre de host de MDM**. En el caso en que se especifica una FQDN (por ejemplo, `mdm.mycompany.com`) en el certificado de HTTPS, ingrese dicho FQDN en el campo **Nombre de host de MDM**. Además, si se usa un comodín * (por ejemplo, `*.mycompany.com`) en el certificado de HTTPS, puede usar `mdm.mycompany.com` en el campo **Nombre de host de MDM**.

5. Ahora el instalador necesita conectarse con una base de datos existente que usará el Conector de dispositivo móvil. Especifique los siguientes detalles de conexión:

- **Base de datos**: Servidor MySQL/Servidor MS SQL/Servidor MS SQL por medio de la autenticación de Windows

- **Controlador ODBC**: Controlador MySQL ODBC 5.1/Controlador unicode MySQL ODBC 5.2/Controlador unicode MySQL ODBC 5.3/Controlador unicode MySQL ODBC 8.0/Servidor SQL/Cliente nativo Servidor SQL 10.0/Controlador ODBC 11 para Servidor SQL/Controlador ODBC 13 para Servidor SQL/Controlador ODBC 17 para Servidor SQL/Controlador ODBC 18 para Servidor SQL

- **Nombre de la base de datos**: Se recomienda utilizar el nombre predefinido o cambiarlo si es necesario.

- **Nombre de host**: nombre de host o dirección de IP de su servidor de base de datos

- **Puerto**: usado para la conexión con el servidor de base de datos

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

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

Puede usar el mismo servidor de la base de datos que usa para la base de datos de ESET PROTECT, pero es recomendable usar un servidor de la BD diferente si planea registrar más de 80 dispositivos móviles.

6. Especifique el usuario para la base de datos del Conector de dispositivo móvil recién creada. Puede **Crear un nuevo usuario** o **Usar un usuario de la base de datos existente**. Ingrese la contraseña para el usuario de la base de datos.

7. Ingrese el **Host de servidor** (nombre o dirección de IP de su Servidor de ESET PROTECT) y **Puerto del servidor** (el puerto predeterminado del servidor es 2222, si está usando un puerto diferente, reemplace el puerto predeterminado por su número de puerto personalizado).

8. Conecte el Conector de MDM al Servidor de ESET PROTECT. Complete el **Host del servidor** y el **Puerto de servidor** requeridos para la conexión con el Servidor de ESET PROTECT y seleccione **Instalación asistida del servidor** o **Instalación fuera de línea** para proceder:

- **Instalación asistida del Servidor**: provee credenciales de administrador de Consola Web ESET PROTECT y

el instalador descargará los certificados necesarios automáticamente. Verifique también los permisos necesarios para la instalación asistida por servidor.

1.Ingrese el **Host del servidor**: nombre o dirección IP de su Servidor y **Puerto de Consola web** de ESET PROTECT (deje el puerto predeterminado 2223 si no está usando un puerto personalizado). También, ofrezca credenciales de cuenta de administrador de la consola web: **Nombre de usuario/Contraseña**.

2.Cuando se pida que acepte el certificado, haga clic en **Sí**. Continúe en el paso 10.

- **Instalación fuera de línea**: proporciona un **Certificado de Proxy** y una **Autoridad de certificación** que se puede exportar desde ESET PROTECT. Como alternativa, puede usar su certificado personalizadoy una Autoridad de certificación apropiada.

1.Haga clic en **Examinar**, junto a Certificado de pares, y navegue hasta la ubicación del **Certificado de pares** (este es el certificado de proxy que exportó desde ESET PROTECT). Deje en blanco el área de **Contraseña del certificado** porque este certificado no necesita una contraseña.

2.Repita el procedimiento para la Autoridad de certificado y continúe en el paso 10.

> Si usa certificados personalizados con ESET PROTECT (en lugar de los predeterminados que se generaron automáticamente durante la instalación de ESET PROTECT), debe usarse estos mismos cuando se le solicite proveer un certificado Proxy.

9. Especifique la carpeta de destino para el Conector de dispositivo móvil (recomendamos usar la predeterminada), haga clic en **Siguiente**, luego **Instalar**.

10. Una vez finalizada la instalación, verifique si Mobile Device Connector funciona correctamente al abrir *https://your-mdm-hostname:enrollment-port* (por ejemplo *https://mdm.company.com:9980*) en su navegador web o desde un dispositivo móvil. Si la instalación fue exitosa, verá el siguiente mensaje: ¡Servidor MDM activo y en funcionamiento!

11. Ahora puede activar MDM desde el administrador remoto ERA ESET PROTECT.

Requisitos previos del conector de dispositivo móvil

> Si el puerto o el nombre de host para el servidor MDM cambió, todos los dispositivos móviles deben volver a inscribirse.
> Por este motivo, se recomienda que configure un nombre de host dedicado para el servidor MDM de modo que si alguna vez necesita cambiar el dispositivo host del servidor MDM, pueda hacerlo mediante la reasignación de la dirección IP del nuevo dispositivo host al nombre de host MDM en su configuración de DNS.

Los siguientes prerrequisitos se deben cumplir para poder instalar el Conector de dispositivo móvil en Windows:

- Dirección IP pública / dominio público accesible desde Internet.

> Si necesita cambiar el nombre de host de su Servidor de MDM, deberá ejecutar una instalación de reparación de su componente de MDC. Si cambia el nombre de host en su servidor MDM, necesitará importar un nuevo **certificado del servidor HTTPS** que incluya este nuevo nombre de host para que el MDM continúe trabajando correctamente.

- Puertos abiertos y disponibles: consulte la lista completa de puertos aquí. Recomendamos usar los números de puerto predeterminados 9981 y 9980, pero también se pueden cambiar en la Política de su Servidor de MDM si fuera necesario. Asegúrese de que los dispositivos móviles se pueden conectar por puertos específicos. Modifique su configuración de firewall y/o red (de ser necesario) para permitirlo. Obtenga más información sobre la arquitectura MDM.

- Configuración del Firewall: al instalar un conector de dispositivo móvil en un SO que no es servidor como Windows 7 (a fines de evaluación), asegúrese de permitir la comunicación de los puertos a través 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

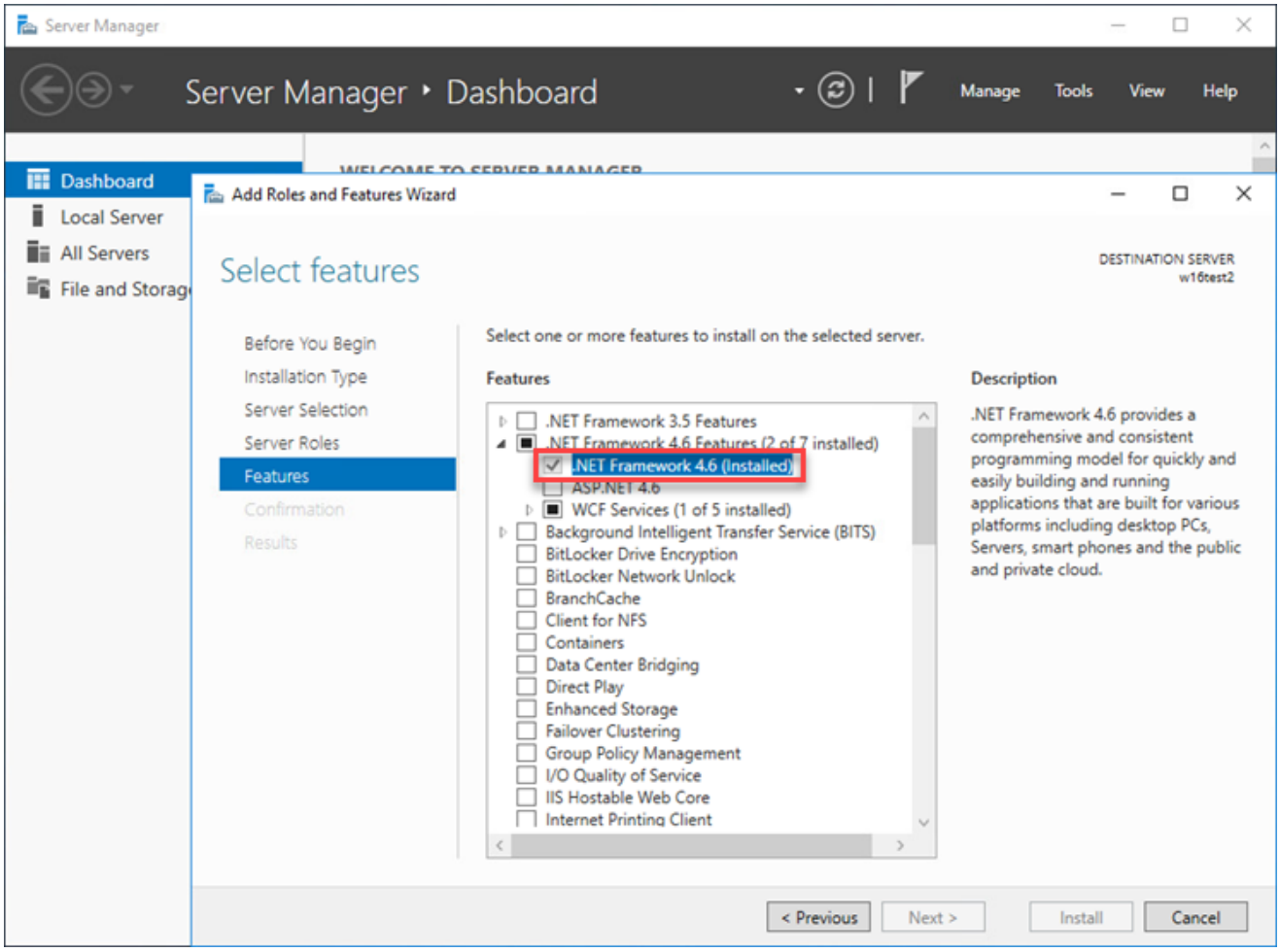
C:\Program Files\ESET\RemoteAdministrator\Server\ERAServer.exe, puerto TCP 2222

> Las rutas reales a los archivos *.exe* pueden variar, de acuerdo al lugar de instalación de cada uno de los componentes ESET PROTECT en su sistema operativo cliente.

- Un servidor de la base de datos ya instalado y configurado. Asegúrese de cumplir con los requisitos de Microsoft SQL o MySQL.

- El uso de RAM del conector MDM está optimizado para tener como máximo 48 procesos "ESET PROTECT MDMCore Module" ejecutándose de manera simultánea, y si el usuario conecta más dispositivos, los procesos cambiarán periódicamente para cada dispositivo que en la actualidad necesite usar 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 de los certificados

• Necesitará un **certificado SSL** en formato *.pfx*para garantizar la comunicación en HTTPS. Le recomendamos que utilice un certificado provisto por una Autoridad de certificación de terceros. No se recomiendan los certificados autofirmados (incluso los certificados firmados por la autoridad de certificación de ESET PROTECT) porque no todos los dispositivos móviles permiten a sus usuarios aceptar certificados autofirmados.

• Necesitará tener un certificado firmado por la AC y la clave privada correspondiente y usar los procedimientos estándar (tradicionalmente, mediante OpenSSL) para fusionarlos en un archivo *.pfx*:
`openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out httpsCredentials.pfx`
Es un procedimiento estándar para la mayoría de los servidores que usan certificados SSL.

• Para la instalación fuera de línea, además necesitará un certificado de pares (el **certificado del agente** exportado desde ESET PROTECT). Como alternativa, puede usar su certificado personalizado con ESET PROTECT.

Activación del conector de dispositivo móvil

Luego de haber instalado el Conector de dispositivo móvil, necesitará activarlo con una licencia ESET Endpoint, Business u Office:

1. Agregue la licencia ESET Endpoint, Business u Office al administrador de licencias de ESET PROTECT.

2.Activar Mobile Device Connector mediante una tarea del cliente de Activación del producto. Este procedimiento es el mismo que el que se usa al activar cualquier producto de ESET en un equipo cliente; en este caso, el Conector de dispositivo móvil es el equipo cliente.

Funcionalidad de licencias MDM iOS

Dado que ESET no ofrece una aplicación en Apple App Store, el Conector de dispositivo móvil ESET almacena todos los detalles de licencias para los dispositivos iOS.

Las licencias se ofrecen por dispositivo y se pueden activar mediante una Tarea de activación del producto (igual que Android).

Se pueden desactivar las licencias iOS de las siguientes maneras:

- Eliminación del dispositivo de la administración mediante una tarea Detener administración
- Desinstalación de MSC mediante la opción **Eliminar base de datos**
- Desactivación por otros medios (ESET PROTECT o desactivación EBA)

Debido a que MDC se comunica con los servidores de licencia de ESET en nombre de los dispositivos iOS, el portal EBA refleja el estado de MDC y no el estado de los dispositivos individuales. La información actual del dispositivo está siempre disponible en la Consola web de ESET PROTECT.

Los dispositivos no activados o los dispositivos con licencias vencidas mostrarán un estado de protección rojo y el mensaje “El producto no está activado”. Estos dispositivos se rehusarán a manejar tareas, definir políticas y proporcionar registros no críticos.

Durante la desinstalación de MDM, si la opción **No quitar la base de datos** está seleccionada, las licencias que se usen no se desactivarán. Estas licencias pueden reutilizarse si se reinstala MDM en esta base de datos, si se quita mediante ESET PROTECT o si se desactiva en EBA. Cuando se traslada a otro servidor MDM, deberá realizar la Tarea de activación del producto nuevamente.

Requisitos del certificado HTTPS

Para inscribir un dispositivo móvil en el Conector de dispositivo móvil ESET, asegúrese de que el servidor HTTPS devuelve la cadena completa de certificados.

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

- El certificado HTTPS (contenedor pkcs#12/pfx) debe contener la cadena completa de certificados, incluida la raíz de AC.
- El certificado debe ser válido durante el tiempo requerido (válido desde / válido hasta).
- El **NombreComún** o **temaAltNombre** debe coincidir con el nombre de host de MDM.

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

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

Básicamente, el " * " no se puede usar para reemplazar el "punto". iOS confirma este comportamiento al aceptar los certificados de MDM.

Observe que algunos dispositivos tienen en cuenta su zona horaria cuando verifican la validez del certificado y otros dispositivos no. Brinde la validez del certificado uno o dos días antes de la fecha actual para evitar posibles problemas.

Instalación y caché del proxy Apache HTTP

Acerca de Apache HTTP Proxy

Apache HTTP Proxy puede cumplir con diversos propósitos:

Función	La solución proxy que proporciona esta función
Almacenamiento en caché de descargas y actualizaciones	Apache HTTP Proxy u otras soluciones proxy
Resultados del almacenamiento en caché de ESET LiveGuard Advanced	Únicamente Apache HTTP Proxyconfigurado
Replicación de la comunicación de los Agentes ESET Management con el Servidor ESET PROTECT	Apache HTTP Proxy u otras soluciones proxy

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

Función de almacenamiento en caché de Apache HTTP Proxy

Apache HTTP Proxydescargas y cachés:

- Actualizaciones del módulo ESET
- Paquetes de instalación de los servidores de depósito
- Actualizaciones de componentes del producto

Los datos en caché se distribuyen a los clientes de extremo en su red. El almacenamiento en caché puede disminuir significativamente el tráfico de Internet en su red

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

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

- Instalación desde el instalador todo en uno

- Instalación desde el instalador independiente

Instalación desde el instalador independiente

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

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

> Si desea instalar el Proxy Apache HTTP en un disco duro diferente, debe reemplazar *C:\Program Files* por la ruta correspondiente en las instrucciones a continuación y en el archivo *httpd.conf* ubicado en el directorio *Apache HTTP Proxy\conf*. Por ejemplo, si extrae el contenido de *ApacheHttp.zip* hacia *D:\Apache Http Proxy*, entonces *C:\Program Files* se debe reemplazar con *D:\Apache Http Proxy*.

3. Abra un símbolo del sistema administrativo 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 proxy con el siguiente comando **ApacheHttpProxy**:

```
sc start ApacheHttpProxy
```

6. Puede verificar si el servicio Proxy HTTP Apache se está ejecutando en la extensión `services.msc` (busque **ApacheHttpProxy**). En forma predeterminada, el servicio está configurado para iniciar automáticamente.

Después de la instalación, configure Apache HTTP Proxy para la funcionalidad deseada.

Configuración del Apache HTTP Proxy

El instalador de Apache HTTP Proxy que proporciona ESET está preconfigurado. Sin embargo, deberá realizar una configuración personalizada adicional para que el servicio funcione correctamente.

Configuración de Apache HTTP Proxy para replicación (Agente-Servidor)

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

a.En forma predeterminada, el puerto 2222 se usa para la comunicación con el Agente ESET Management. Si cambió el puerto durante la instalación, use el número de puerto modificado. Cambie 2222 en la línea: `AllowCONNECT 443 563 2222 8883 53535` para su número de puerto.

b.Agregue un segmento `ProxyMatch` aparte:

I.La dirección usada por sus Agentes para conectarse con el Servidor de ESET PROTECT.

II.Todas las direcciones posibles del Servidor ESET PROTECT(IP, FQDN)
(agregue el siguiente código completo; la dirección IP 10.1.1.10 y el nombre de host `hostname.example` son solo ejemplos que debe sustituir por sus direcciones. También puede generar la expresión `ProxyMatch` 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 del Agente correcta para asegurarse de que sus agentes usen el proxy para replicación.

Configuración de Apache HTTP Proxy para caché

1. Inicie el servicio de proxy con el siguiente comando **ApacheHttpProxy**:

```
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 de Apache.

```
sc start ApacheHttpProxy
```

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

Configuración de Apache HTTP Proxy para nombre de usuario y

contraseña

La configuración del nombre de usuario y la contraseña solo puede usarse para caché. La autenticación no es compatible con el protocolo de replicación que se usa en la comunicación Agente-Servidor.

1. Detenga el servicio **ApacheHttpProxy** y, para ello, abra un símbolo del sistema elevado y ejecute 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. Agregue 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. Use el comando `htpasswd` para crear un archivo que se llame `password.file` en la carpeta *Apache HTTP Proxy\bin* (se le solicitará una contraseña):

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

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

```
usergroup:username
```

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

```
sc start ApacheHttpProxy
```

7. Pruebe la conexión al Proxy HTTP accediendo a la siguiente URL en su navegador:

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

Tras finalizar con éxito la instalación del Proxy Apache HTTP, puede elegir entre permitir solo las comunicaciones de ESET (y bloquear el tráfico restante de manera predeterminada) o permitir todo el tráfico. Realice los cambios de configuración necesarios descritos aquí:

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

Mostrar una lista de contenido que se encuentre actualmente en la caché

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

Use la herramienta htcacheclean para limpiar el caché del disco. Consulte el comando recomendado a continuación (configuración de tamaño de caché de 20 GB y límite de archivos en caché ~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 caché, debe limpiar las ejecuciones a 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 ^ justo después del final de la línea en los comandos anteriores es esencial, ya que estos no se ejecutarán correctamente si no se incluye.

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

Squid instalación en Windows y caché de proxy HTTP

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

1. Descargue el instalador MSI Squid e instale Squid.

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

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

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

Esto crea los directorios intercambiables para almacenamiento.

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

5. Reemplace `http_access deny all` con `http_access allow all`.

6. Permita el almacenamiento del disco al agregar la siguiente línea:

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

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

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

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

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

Repositorio fuera de línea: Windows

Puede usar la herramienta de replicación para crear un repositorio sin conexión (en Windows). Esto suele ser necesario en redes cerradas de equipos o en redes con acceso limitado a internet. La herramienta de replicación se puede usar para crear un clon del repositorio ESET en una carpeta local. Este repositorio clonado luego se puede mover (por ejemplo, a un disco externo) a una ubicación en la red cerrada. Puede copiar el repositorio a una ubicación segura en la red local y hacer que esté disponible a través de un servidor HTTP.

Para actualizar el repositorio fuera de línea, ejecute el mismo comando con los mismos parámetros que para la creación del repositorio fuera de línea. Los datos existentes en la carpeta intermediaria se volverán a usar y solo los archivos obsoletos se reemplazarán.

Tenga en cuenta que el tamaño del repositorio está aumentando y el directorio intermediario tendrá el mismo tamaño. Asegúrese de tener al menos **1,2 TB** de espacio libre antes de comenzar 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.

Escenario de ejemplo para Windows

I. Crear un clon del repositorio

1. Descargar la herramienta de replicación.

2. Extraer la herramienta de replicación del archivo *.zip* descargado.

3. Preparar (crear) carpetas para:

   - archivos intermediarios
   - repositorio final

4. Abrir el símbolo del sistema y cambiar el directorio a la carpeta donde se extrajo la herramienta de replicación (comando `cd`).

5. Ejecutar el siguiente comando (cambiar los directorios de repositorio intermedio y de salida a las carpetas del paso 3):

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

6. Luego de copiado el repositorio a la carpeta `outputRepositoryDirectory`, mover la carpeta y sus contenidos a otro equipo donde se pueda acceder a su red cerrada.

II. Configurar el servidor HTTP

7. Necesita de un servidor HTTP en ejecución en el equipo dentro de la red cerrada. Puede usar:

   - Apache HTTP Proxy del sitio de descargas de ESET (este escenario)
   - un servidor HTTP diferente

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

9. Abra un símbolo del sistema administrativo 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. En un editor de texto simple, abra el archivo *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf* y agregue las siguientes líneas en la parte inferior 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 proxy con el siguiente comando **ApacheHttpProxy**:

```
sc start ApacheHttpProxy
```

13. Compruebe que el servicio esté en funcionando; ingrese *http://YourIPaddress:80/index.html* en su navegador (reemplace *YourIPaddress* con la dirección IP de su equipo).

III. Ejecutar el repositorio fuera de línea

14. Crear nueva carpeta para el repositorio fuera de línea, por ejemplo: *C:\Repository.*

15. En el archivo *httpd.conf* reemplace 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">
```

con la dirección de la carpeta del repositorio, de la siguiente manera:

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

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

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

```
sc restart ApacheHttpProxy
```

18. Ahora, su repositorio fuera de línea está funcionando en la dirección *http://YourIPaddress* (por ejemplo, *http://10.1.1.10*).

19. Configure la nueva dirección del repositorio con la consola web ESET PROTECT:

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

b.Agentes ESET Management: haga clic en **Políticas**, haga clic en la política del agente > **Editar** > **Configuración** > **Configuración avanzada** > **Repositorio** > ingrese 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 de **ESET Endpoint para Windows** > **Editar** > **Configuración** > **Actualizar** > **Perfiles** > **Actualizaciones** > **Actualizaciones de módulos** > anule la selección de **Elegir automáticamente** e ingrese la dirección del repositorio sin conexión en el campo **Servidor personalizado**.

Clúster de conmutación por error: Windows

A continuación, se encuentran los pasos de nivel alto que se requieren para instalar ESET PROTECT en un entorno de clúster de conmutación por error.

Vea también este Artículo de base de conocimiento acerca de la instalación de clúster del servidor de ESET PROTECT.

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

   - Instrucciones para crear un clúster de conmutación por error en el Servidor de Windows 2016 e 2019
   - Instrucciones para crear un clúster de conmutación por error en el Servidor de Windows 2012 e 2012 R2

2. En el **Asistente crear clúster**, ingrese el nombre del host que desee (invente uno) y la dirección IP.

3. Obtenga el disco compartido del clúster en línea en el nodo 1 e instale el Servidor ESET PROTECT mediante el instalador independiente. Asegúrese de que **Esta es una instalación de clústeres** esté seleccionada durante la instalación y seleccione el disco compartido como almacenamiento de datos de la aplicación. Invente un nombre de host e ingréselo para el certificado del servidor de ESET PROTECT Server junto a los nombres del host completados anteriormente. Recuerde este nombre de host y úselo en el paso 6 al crear el rol del Servidor ESET PROTECT en el administrador de clústeres.

4. Detenga el ESET PROTECT Server en el nodo 1, traiga el disco compartido del clúster en línea en el nodo 2 e instale el Servidor ESET PROTECT mediante el instalador independiente. Asegúrese de que **Esta es una instalación de clústeres** esté seleccionada durante la instalación. Elija el disco compartido como la aplicación de almacenamiento de datos. Mantenga la información de conexión y certificado de la base de datos intacta, se configuraron durante la instalación de ESET PROTECT Server en el nodo 1.

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

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

7. Instale el Agente ESET Management en todos los nodos de clústeres mediante el instalador independiente. En las pantallas **Configuración del agente** y **Conexión a las pantallas del Servidor ESET PROTECT**, use el nombre de host que usó en el paso número 6. Almacene los datos del agente en el nodo local (no el disco del clúster).

8. El servidor web (Apache Tomcat) no es compatible en un clúster y, por lo tanto, se debe instalar en un disco sin clúster o en un equipo diferente:

   a. Instale la consola web en un equipo separado y configúrela correctamente para conectarse con el rol del clúster del servidor de ESET PROTECT.

   b. Después de instalar la consola web, ubique el 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 cualquier otro editor de textos simple. En la línea `server_address=localhost`, reemplace localhost con la dirección IP o el nombre de host del rol del clúster del servidor ESET PROTECT.

Instalación de componentes en Linux

En la mayoría de los escenarios de instalación, necesita instalar diferentes componentes de ESET PROTECT en distintas máquinas para admitir las diferentes arquitecturas de red, cumplir con los requisitos de rendimiento, o por otros motivos.

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

Instalación de componentes principales

- Servidor ESET PROTECT
- Consola web ESET PROTECT – Puede instalar la consola web de ESET PROTECT en un equipo diferente a donde se ejecuta el servidor de ESET PROTECT.
- Agente ESET Management
- un servidor de base de datos

Instalación de componentes opcionales

- RD Sensor
- Conector de dispositivo móvil
- Apache HTTP Proxy
- Herramienta de replicación

Para actualizar ESET PROTECT para Linux a la versión más reciente, consulte el capítulo Tarea de actualización de componentes en nuestro Artículo de la base de conocimiento.

Instalación del ESET PROTECT en Windows paso a paso

En este escenario de instalación vamos a simular la instalación paso a paso del Servidor ESET PROTECT y de la Consola Web ESET PROTECT. Vamos a simular la instalación usando MySQL.

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

Antes de la instalación

1. Verifique la presencia del servidor de la base de datos en su red y asegúrese de que puede acceder a él desde su servidor local o remoto. Si no hay un servidor de base de datos instalado, instale y configure uno nuevo.

2. Descargar ESET PROTECT Componentes Linux independientes (Agente, Servidor, Consola web). Puede encontrar estos archivos de instalación en la categoría Instaladores independientes ESET PROTECT disponible en el sitio web de ESET.

Proceso de instalación

Debe poder usar el comando `sudo` o instalarlo en privilegios `root` para finalizar la instalación.

1. Instale los paquetes necesarios para el Servidor ESET PROTECT .

2. Configure la conexión al servidor MySQL, tal como se muestra en el tema configuración de MySQL.

3. Verifique la configuración del controlador de MySQL ODBC. Consulte Instalación y configuración de ODBC para más información.

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

5. Instale los paquetes Java y Tomcat necesarios e instale la Consola web ESET PROTECT. Si tiene problemas con la conexión HTTPS a la Consola web ESET PROTECT, consulte laConfiguración de la conexión HTTPS/SSL.

6. Instale el Agente ESET Management en el equipo servidor.

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

Instalación y configuración de MySQL

Instalación

Asegúrese de instalar una versión compatible de MySQL Server y ODBC Connector.

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 seleccionar las opciones predeterminadas: Consulte también Agregar el repositorio MySQL APT.

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

2. Actualice la memoria caché de su 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 variará según la distribución y versión de Linux usada:

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 la fuente 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 para una instalación manual.

Configuración

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

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

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

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

> i
> - 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 su versión 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`	Como alternativa, puede deshabilitar la creación de registros binarios: `log_bin=0`	Versiones 8.x compatibles
`innodb_log_file_size=100M`	La multiplicación de los valores de estos dos parámetros debe ser como mínimo **200**. El valor mínimo para `innodb_log_files_in_group` es **2**, y el máximo es **100**;; además, el valor debe ser entero.	Versiones 8x compatibles 5.7 5.6.22 (y versiones posteriores 5.6.x)
`innodb_log_files_in_group=2`		
`innodb_log_file_size=200M`	Configure un valor mínimo de**200M**, pero no mayor de **3000M**.	5.6.20 y 5.6.21

3. Presione **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 para algunas distribuciones de 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 siguiendo una de las siguientes opciones:

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

- 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` con 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 ODBC Connector.

ℹ Puede instalar el controlador de MS ODBC (versión 13 o posterior) para conectar el servidor de ESET PROTECT en Linux con el Servidor MS SQL en Windows. Para obtener más información, visite este artículo de la base de conocimiento.

Instale el controlador MySQL ODBC utilizando el terminal. Siga los pasos de su distribución Linux:

- Debian, Ubuntu

- CentOS 7
- Otras distribuciones de Linux compatibles

Debian, Ubuntu

1. Instalando controladores unixODBC:

```
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`

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

3. Descomprima el archivo del controlador ODBC (el nombre del paquete cambia en función del enlace 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 enlace 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 enlace 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 para ODBC.

- Para nuevas versiones de Linux, como Ubuntu 20.x, recomendamos usar el controlador Unicode:

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0 Driver" -t
"Driver=/usr/local/lib/libmyodbc8w.so"
```

- Para 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. Enumerar los controladores instalados:

```
sudo myodbc-installer -d -l
```

Para más información, consulte:
https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-tarball.html.

CentOS 7

1. Instalando controladores unixODBC:

```
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 utilizando YUM, ya que instalaría la versión más reciente que no es compatible.
- Asegúrese de seleccionar y descargar la versión compatible con su distribución y versión de Linux.
- Puede descargar el conector ODBC para MySQL desde el sitio oficial de MySQL.

3. Instalar el controlador ODBC:

```
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. Enumerar los controladores instalados:

```
sudo myodbc-installer -d -l
```

Otras distribuciones de Linux compatibles

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

1. Siga estas instrucciones para instalar el controlador ODBC:

- **OpenSuse, SUSE Linux Enterprise Server**: `sudo zypper install unixODBC`. Consulte además 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 textos:

```
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 hacia el **Driver** y la **Setup** sean correctas), luego 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
```

Es posible que el controlador se encuentre en una ubicación diferente para algunas distribuciones. Puede encontrar el archivo con el siguiente comando:

```
sudo find /usr -iname "*libmyodbc*"
```

4. Actualice los archivos de configuración que controlan el acceso de ODBC a los servidores de la base 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 seleccionadas**
> Puede seguir los artículos de nuestra base de conocimiento con instrucciones específicas de la distribución:
> - CentOS 7
> - Debian 10
> - SUSE Linux Enterprise Server (SLES)

Instalación

Siga los pasos indicados a continuación para instalar el componente del Servidor de ESET PROTECT en Linux mediante un comando de terminal:

> Asegúrese de cumplir con todos los requisitos previos de instalación.

1. Descargue el componente del servidor ESET PROTECT:

```
wget https://download.eset.com/com/eset/apps/business/era/server/linux/latest/server
-linux-x86_64.sh
```

2. Convierta al archivo descargado en ejecutable:

```
chmod +x server-linux-x86_64.sh
```

3. Puede preparar un script de instalación y, luego, ejecutarlo con `sudo`.

Ejecute el script de instalación basado en el ejemplo de abajo (las nuevas líneas se dividen con "\" para copiar todo el comando a la 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`	No se eliminará la base de datos durante la desinstalación.	-
`--locale`	El identificador local (LCID) del servidor instalado (el valor predeterminado es `en_US`). Consulte losidiomas compatibles para ver las opciones disponibles. Si no especifica la `configuración regional`, el servidor de ESET PROTECT se instalará en inglés. Luego de la instalación de ESET PROTECT, puede configurar un idioma para cada sesión de la consola web de ESET PROTECT. No todos los elementos de la consola web se cambiarán luego 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 le solicitará al usuario la confirmación del acuerdo de licencia.	-
`--skip-cert`	Omita la generación de certificados (úsela junto con el parámetro `--server-cert-path`).	-
`--license-key`	Clave de licencia de ESET. Puede facilitar la clave de licencia más tarde.	-
`--server-port`	ESET PROTECT puerto del servidor (el valor predeterminado es `2222`).	-
`--console-port`	ESET PROTECT puerto de consola (el valor predeterminado es `2223`)	-
`--server-root-password`	La contraseña para el inicio de sesión de la Consola web del usuario “Administrador” debe tener al menos 8 caracteres.	Sí
`--db-type`	Tipo de base de datos que se usará (posibles valores: `"MySQL Server"`, `"MS SQL Server"`) MS SQL Server en Linux no es compatible. Sin embargo, puede conectar el servidor de ESET PROTECT en Linux con el Servidor MS SQL en Windows.	-
`--db-driver`	Controlador ODBC usado para conectarse a la base de datos especificada en el archivo *odbcinst.ini* (el comando `odbcinst -q -d` brinda una lista de controladores disponibles; use uno de estos controladores, por ejemplo: `--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 equipo o dirección IP del servidor de la base de datos. La instancia de la base de datos nombrada no es compatible.	Sí

Atributo	Descripción	Requerido
`--db-port`	Puerto del servidor de la base de datos (el valor predeterminado es `3306`).	Sí
`--db-name`	Nombre de la base de datos del Servidor ESET PROTECT (el valor predeterminado es `era_db`).	-
`--db-admin-username`	Nombre de usuario del administrador de la base de datos (usado por la instalación para crear y modificar la base de datos). Se puede omitir este parámetro si ya hay un usuario de la base de datos previamente creado definido en `--db-user-username` y `--db-user-password`	Sí
`--db-admin-password`	Contraseña del administrador de la base de datos. Se puede omitir este parámetro si ya hay un usuario de la base de datos previamente creado definido por `--db-user-username` y `--db-user-password`	Sí
`--db-user-username`	Nombre del usuario de la base de datos del Servidor ESET PROTECT (usado por el Servidor ESET PROTECT 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 del Servidor ESET PROTECT	Sí
`--cert-hostname`	Contiene todos los posibles nombres o direcciones IP del equipo del Servidor de ESET PROTECT. El valor tendrá que coincidir con el nombre del servidor especificado en el certificado del Agente que intenta conectarse al servidor.	Sí
`--server-cert-path`	Ruta al certificado de pares del servidor (use esta opción si especificó `--skip-cert` también)	-
`--server-cert-password`	Contraseña del certificado de pares del servidor	-
`--agent-cert-password`	Contraseña del certificado de pares del agente	-
`--cert-auth-password`	Contraseña de la autoridad de certificado	-
`--cert-auth-path`	Ruta al archivo de la autoridad de certificación del servidor	-
`--cert-auth-common-name`	Nombre común de la autoridad de certificación (use “”)	-
`--cert-organizational-unit`	-	-
`--cert-organization`	-	-
`--cert-locality`	-	-
`--cert-state`	-	-
`--cert-country`	-	-
`--cert-validity`	Validez del certificado en días o años (especifique en argumento `--cert-validity-unit`)	-
`--cert-validity-unit`	Unidad para la validez del certificado; los posibles valores son “años” o “días” (el valor predeterminado es `Years`)	-
`--ad-server`	Servidor de Active Directory	-
`--ad-user-name`	Nombre del usuario que tiene derechos para buscar la red de AD	-
`--ad-user-password`	Contraseña del usuario de Active Directory	-
`--ad-cdn-include`	Ruta del árbol de Active Directory que se sincronizará. Use paréntesis vacíos “” para sincronizar un árbol entero	-
`--enable-imp-program`	Active el Programa de mejora del producto.	-
`--disable-imp-program`	Desactive el Programa de mejora del producto.	-

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

4. La instalación le solicita si desea participar en el programa de mejora del producto. Presione **Y** si acepta enviar informes de errores y datos de telemetría a ESET o presione **N** para no enviar datos.

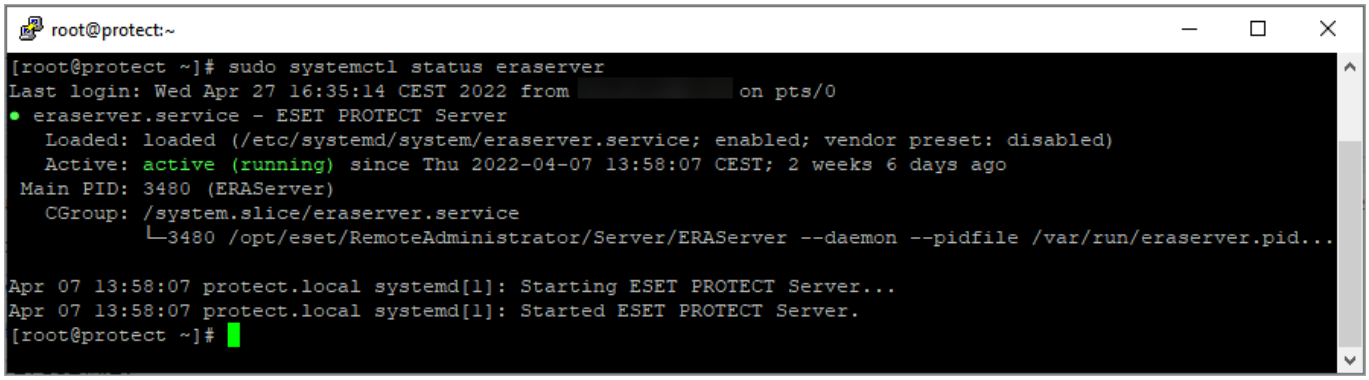
5. El Servidor ESET PROTECT y el servicio`eraserver` se instalarán en la siguiente ubicación:

/opt/eset/RemoteAdministrator/Server

La instalación puede terminar con **SELinux policy... failure**. Puede ignorarlo si no utiliza SELinux.

6. Después de la instalación, verifique que el servicio del Servidor ESET PROTECT se encuentra activo mediante el comando que se muestra 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 el Servidor de ESET PROTECT en Linux, debe cumplir con los siguientes requisitos previos:

- Debe tener 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 tener un servidor de la base de datos debe estar instalado y configurado con una cuenta raíz. No tiene que crear una cuenta de usuario antes de la instalación. El instalador puede crear la cuenta. MS SQL Server en Linux no es compatible. Sin embargo, puede conectar el servidor de ESET PROTECT en Linux con el Servidor MS SQL en Windows.

El servidor de ESET PROTECT almacena grandes blobs de datos en la base de datos. Configure MySQL para aceptar paquetes grandes para que ESET PROTECT se ejecute correctamente.

- **Controlador ODBC**: el controlador ODBC se usa para establecer la conexión con el servidor de base de datos (MySQL).

- Configure el archivo de instalación del servidor como un ejecutable utilizando el comando de terminal:

```
chmod +x server-linux-x86_64.sh
```

- Le recomendamos **usar la versión más reciente de OpenSSL 1.1.1**. OpenSSL 3.x no es compatible. La versión compatible mínima de OpenSSL para Linux es openssl-1.0.1e-30. Puede haber más versiones de OpenSSL instaladas en un sistema de forma simultánea. Debe haber al menos una versión compatible presente en su sistema.

    - Use el comando `openssl version` para mostrar la versión predeterminada actual.

    - Puede mostrar una lista de 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 verificar si el cliente de Linux es compatible mediante el siguiente comando: `openssl s_client -connect google.com:443 -tls1_2`

- **Xvfb** - Necesario para una adecuada impresión de informes (Generar informe) en los sistemas Linux Server sin una interfaz gráfica.

- **Xauth:** el paquete se instala junto con **xvfb**. Debe instalar **xauth** si no instala **xvfb**.

- **cifs-utils**: se requiere para una implementación adecuada del agente en un sistema operativo Windows.

- **Bibliotecas Qt4 WebKit** - se usan para imprimir informes en formato PDF y PS (deben ser versión 4.8, no 5). Todas las demás dependencias Qt4 se instalarán automáticamente. Si el paquete no está disponible en el repositorio de su 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 de CentOS 7, instrucciones de Ubuntu 20.04.

- **kinit + klist**: Kerberos se usa para autenticar un usuario de dominio al iniciar sesión y la tarea de sincronización con Active Directory. Asegúrese de configurar Kerberos correctamente (*/etc/krb5.conf*). ESET PROTECT 9.1 es compatible con la sincronización con varios dominios.

- **ldapsearch**: se usa en la tarea de sincronización de AD y para autorización.

- **snmptrap**: opcional, se usa para enviar capturas SNMP. SNMP también necesita una configuración.

- **Paquete SELinux devel** - usado durante la instalación del producto para desarrollar módulos de políticas SELinux. Solo es obligatorio en sistemas con SELinux habilitado (CentOS, RHEL). SELinux puede generar problemas con otras aplicaciones. En el caso del Servidor ESET PROTECT, no es necesario.

- **lshw** - Instale el paquete `lshw` en el equipo cliente/servidor Linux para que el agente ESET Management informe correctamente del inventario de hardware.

La tabla a continuación contiene los comandos de terminal adecuados para cada paquete descrito anteriormente para diversas distribuciones de Linux (ejecute los comandos como `sudo` o `root`):

Paquete	Distribuciones Debian y Ubuntu	Distribuciones CentOS y Red Hat	Distribución OpenSUSE
Controlador 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 estándar de CentOS. Instale estos 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 de SELinux devel (opcional: no es necesario para el servidor de ESET PROTECT; SELinux puede causar problemas con otras aplicaciones.)	`apt-get install selinux-policy-dev`	`yum install policycoreutils-devel`	`zypper install selinux-policy-devel`
samba (opcional, necesario únicamente 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

- Le recomendamos **usar la versión más reciente de OpenSSL 1.1.1**. OpenSSL 3.x no es compatible. La versión compatible mínima de OpenSSL para Linux es openssl-1.0.1e-30. Puede haber más versiones de OpenSSL instaladas en un sistema de forma simultánea. Debe haber al menos una versión compatible presente en su sistema.
  - Use el comando `openssl version` para mostrar la versión predeterminada actual.
  - Puede mostrar una lista de 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 verificar si el cliente de Linux es compatible mediante el siguiente comando: `openssl s_client -connect google.com:443 -tls1_2`
- Instale el paquete `lshw` en el equipo cliente/servidor Linux para que el agente ESET Management informe correctamente del inventario de hardware.

Distribución Linux	Comando de terminales
Debian, Ubuntu	`sudo apt-get install -y lshw`
Red Hat, CentOS, RHEL	`sudo yum install -y lshw`
OpenSUSE	`sudo zypper install lshw`

- En Linux CentOS, se recomienda instalar el paquete `policycoreutils-devel`. Ejecute el comando para instalar el paquete:

```
yum install policycoreutils-devel
```

- Instalación del agente asistida por servidor:
  - Debe poder acceder al equipo servidor desde la red y tener el ESET PROTECTservidor y la ESET PROTECTConsola web instalados
- Instalación del agente fuera de línea:
  - Debe poder acceder al equipo servidor desde la red y tener el ESET PROTECTServidor instalado.
  - Es necesario contar con un Certificado para el Agente.
  - Debe haber un archivo de clave pública de la autoridad de certificación de servidor.

Instalación

Siga los pasos indicados a continuación para instalar el componente del Agente de ESET Management en Linux mediante un comando de terminal:

Asegúrese de cumplir con todos los requisitos previos de 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. Convierta al archivo en ejecutable:

```
chmod +x agent-linux-x86_64.sh
```

3. Ejecute el script de instalación basado en el ejemplo de abajo (las nuevas líneas se dividen con "\" para copiar todo el comando a la terminal):

Para obtener más información, consulte los Parámetros a continuación.

Instalación asistida por 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 quitar los comandos que contienen datos confidenciales (por ejemplo, una contraseña) del historial de la línea de comandos:
1.Ejecute `history` para ver la lista de todos los comandos del historial.
2.Ejecute `history -d line_number` (especifique el número de línea del comando). Como alternativa, ejecute `history -c` para quitar todo el historial de la línea de comandos.

4. Cuando se le solicite, presione **y** para aceptar el certificado. Puede ignorar cualquier error sobre SELinux devueltos por el instalador.

5. Tras la instalación, compruebe que el servicio del Agente de ESET Management se está ejecutando:

```
sudo systemctl status eraagent
```

6. Configurar el servicio **eraagent** para que se inicie al arrancar: `sudo systemctl enable eraagent`

> **Registro del instalador**
> El registro del instalador puede ser útil para solucionar problemas. Puede encontrarlo en Archivos de registro.

Parámetros

La conexión al Servidor ESET PROTECT se resuelve con el uso de los parámetros --hostname y --port (el puerto no se usa cuando se proporciona un registro SRV). Formatos posibles de conexión.

- **Nombre del host** y **puerto**
- **Dirección IPv4** y **puerto**
- **Dirección IPv6** y **puerto**
- Registro de servicio (registro SRV): para configurar el registro de recurso DNS en Linux, el equipo debe estar en un dominio con un servidor DNS que funcione. Consulte el Registro de recurso DNS. El registro SRV debe comenzar con el prefijo "_NAME._tcp", en el cual 'NAME' representa un nombre personalizado (por ejemplo, “era”).

Atributo	Descripción	Requerido
`--hostname`	Nombre de host o dirección IP para conectarse al Servidor ESET PROTECT.	Sí
`--port`	ESET PROTECT () puerto del servidor (el valor predeterminado es `2222`).	Sí
`--cert-path`	Ruta de acceso local al archivo de certificación del Agente (más información sobre el certificado)	Sí (fuera de línea)
`--cert-auth-path`	Ruta al archivo de la autoridad de certificación del servidor (más información sobre autoridad)	Sí (fuera de línea)
`--cert-password`	Contraseña del certificado del agente.	Sí (fuera de línea)
`--cert-auth-password`	Contraseña de la autoridad de certificado.	Sí (si la usa)
`--skip-license`	La instalación no le solicitará al usuario la confirmación del acuerdo de licencia.	No
`--cert-content`	El contenido encriptado Base64 del certificado de clave pública encriptado PKCS12 más las claves privadas se usan para configurar canales de comunicación seguros entre el Servidor y los Agentes. Use solo una de las opciones de `--cert-path` o `--cert-content`.	No
`--cert-auth-content`	Contenido encriptado Base64 del certificado de clave privada encriptado DER usado para verificar pares remotos (proxy o servidor). Use solo una de las opciones de `--cert-auth-path` o `--cert-auth-content`.	No
`--webconsole-hostname`	Nombre del host o dirección IP usado por la Consola web para conectarse al servidor (si se deja en blanco, el instalador copiará el valor de “nombre del host”).	No
`--webconsole-port`	Puerto usado por la Consola web para conectarse al servidor (el valor predeterminado es `2223`).	No
`--webconsole-user`	Nombre de usuario usado por la Consola web para conectarse al servidor (el valor predeterminado es `Administrator`) No puede usar un usuario con autenticación de dos factores para instalaciones asistidas por el servidor.	No

Atributo	Descripción	Requerido
`--webconsole-password`	Contraseña usada por la Consola web para conectarse al servidor.	Sí (asistida por servidor)
`--proxy-hostname`	Nombre de host del proxy HTTP. Use este parámetro para habilitar el uso de HTTP Proxy (que ya está instalado en su red) para la replicación entre el agente ESET Management y el servidor de ESET PROTECT (no para el almacenamiento en caché de actualizaciones).	Si usa el proxy
`--proxy-port`	Puerto de HTTP Proxy para conectarse con el servidor.	Si usa el proxy
`--enable-imp-program`	Active el Programa de mejora del producto.	No
`--disable-imp-program`	Desactive el Programa de mejora del producto.	No

Conexión y certificados

- Se debe proveer una **Conexión al Servidor ESET PROTECT** : `--hostname`, `--port` (no se necesitará un puerto si se proporciona un registro de servicio, el valor del puerto predeterminado es `2222`)

- Provea la siguiente información de conexión para la **Instalación asistida por servidor**: `--webconsole-port, --webconsole-user, --webconsole-password`

- Provea la información de certificado para la **Instalación fuera de línea**: `--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 consola web. (Lea cómo exportar el archivo .pfx y el archivo .der.)

Parámetros de los tipo de contraseñas

Los parámetros del tipo de contraseña pueden se pueden proporcionar como variables de entorno, archivos, leído desde `stdin` o provisto como texto plano. Esto es:

`--password=env:SECRET_PASSWORD` donde `SECRET_PASSWORD` es una variable de entorno con una contraseña

`--password=file:/opt/secret` donde la primera línea del archivo estándar `/opt/secret` contiene su contraseña

`--password=stdin` le dice al instalador que lea la contraseña desde un ingreso estándar

`--password="pass:PASSWORD"` es igual a `--password="PASSWORD"` y es obligatorio si la contraseña actual es `"stdin"` (ingreso estándar) o si una cadena comienza con `"env:"`, `"file:"` o `"pass:"`

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

Conexión HTTP Proxy

Si está usando el proxy HTTP para la replicación entre el agente de ESET Management y el servidor de ESET PROTECT (y no para almacenar en caché las actualizaciones), puede especificar los parámetros de conexión en `--proxy-hostname` y `--proxy-port`.

```
EJEMPLO - instalación del agente fuera de línea con Conexión HTTP Proxy
./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 el Agente y el servidor ESET PROTECT no es compatible con la autenticación. Cualquier solución proxy que se use para reenviar la comunicación del agente hacia el servidor ESET PROTECT que requiera autenticación no funcionará.
Si elige usar un puerto no predeterminado para la consola web o el agente, puede requerir un ajuste del firewall. De lo contrario, la instalación puede fallar.

Actualizar y reparar la instalación del Agente en Linux

Si instala el Agente en forma manual en un sistema donde el Agente ha sido instalado previamente, pueden ocurrir los siguiente escenarios:

- **Actualizar**: ejecuta una versión posterior del instalador.
  - Instalación asistida por servidor - actualiza la aplicación, pero usará los certificados anteriores.
  - Instalación fuera de línea - actualiza la aplicación con nuevos certificados.
- **Reparar**: ejecuta la misma versión del instalador. Puede utilizar esta opción para migrar el Agente a un Servidor de ESET PROTECT diferente.
  - Instalación asistida por servidor - la aplicación se vuelve a instalar y obtendrá certificados actuales del Servidor ESET PROTECT (definidos por el parámetro `hostname`).
  - Instalación fuera de línea - la aplicación se vuelve a instalar con nuevos certificados.

Si migra el agente de un Servidor anterior a un Servidor ESET PROTECT nuevo en forma manual, y usa una instalación asistida por servidor, ejecute el comando dos veces. El primero actualizará el Agente, y el segundo obtendrá los nuevos certificados para que el Agente pueda conectarse con el Servidor de ESET PROTECT.

Instalación de la consola web: Linux

Siga estos pasos para instalar la consola web ESET PROTECT:

Puede instalar la consola web de ESET PROTECT en un equipo diferente a donde se ejecuta el servidor de ESET PROTECT. Este procedimiento requiere pasos adicionales.

1. Instale los paquetes Apache Tomcat y Java. Los nombres de paquetes de ejemplo que se muestran a continuación pueden diferir de sus paquetes del repositorio de distribución de 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 la consola web (*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 e implemente 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 *era* esté presente en la carpeta Tomcat:

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 aspecto: `era era.war`

6. Configure el servicio Tomcat para que se inicie al arrancar (`sudo systemctl enable tomcat` o `tomcat9` en función del nombre del servicio)

7. Si instaló la Consola Web de ESET PROTECT en un equipo diferente al del Servidor de ESET PROTECT, realice estos pasos adicionales para permitir la comunicación entre la Consola Web de ESET PROTECT y el Servidor de ESET PROTECT:

a)Detenga el servicio de Tomcat:`sudo systemctl stop tomcat`

b)Edite 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 usar el siguiente comando para encontrar el archivo en su sistema:

```
find / -iname "EraWebServerConfig.properties"
```

c)Busque`server_address=localhost`

d)Sustituya `localhost` por la dirección IP de su Servidor de ESET PROTECT 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` en función del nombre del servicio)

8. Abra la consola web de ESET PROTECT en un navegador web compatible para ver una pantalla de inicio de sesión:

• Desde el equipo en el que se aloja la consola web ESET PROTECT: *http://localhost:8080/era*

• Desde cualquier equipo con acceso a Internet a la consola web ESET PROTECT (sustituya *IP_ADDRESS_OR_HOSTNAME* con la dirección IP o el nombre de host de su consola webESET PROTECT): *http://IP_ADDRESS_OR_HOSTNAME:8080/era*

9. Configure la consola web después de la instalación:

• El puerto HTTP predeterminado se define en 8080 durante la instalación manual de Apache Tomcat. Le recomendamos que configure una conexión HTTPS para Apache Tomcat.

• Consulte también la Configuración adicional de la consola web para soluciones empresariales o sistemas de bajo rendimiento.

Instalación del rogue detection sensor – Linux

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

Requisitos previos

• Se puede realizar búsquedas en la red (los puertos están abiertos, el firewall no bloquea la comunicación entrante, etc.).

• Se puede acceder al equipo del Servidor.

• El Agente ESET Management debe estar instalado en el equipo local para que sea compatible con todas las características del programa

- El terminal está abierto.
- Configure el archivo de instalación del RD Sensor como ejecutable:

```
chmod +x rdsensor-linux-x86_64.sh
```

Instalación

Siga los pasos indicados a continuación para instalar el componente RD Sensor en Linux mediante un comando de terminal:

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

1. Use el siguiente comando para ejecutar el archivo de instalación como sudo:

```
sudo ./rdsensor-linux-x86_64.sh
```

2. Lea el Contrato de licencia de usuario final. Use **la barra espaciadora** para pasar a la página siguiente de EULA.
El instalador le preguntará si acepta el acuerdo. Presione **S** en el teclado si está de acuerdo. De lo contrario, presione **N**.

3. Presione **Y** si acepta participar en el programa de mejora del producto. De lo contrario, presione **N**.

4. ESET Rogue Detection Sensor se iniciará después de que se complete la instalación.

5. Para controlar si se instaló correctamente, verifique que el servicio esté funcionando al ejecutar el siguiente comando:

```
sudo systemctl status rdsensor
```

6. Puede encontrar 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 diferente al que ejecuta su Servidor ESET PROTECT. Por ejemplo, puede utilizar este escenario de instalación para que pueda accederse a 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 mediante un comando de terminal:

Asegúrese de cumplir con todos los requisitos previos de 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 basado en el ejemplo de abajo (las nuevas líneas se dividen con "\" para copiar todo el comando a la terminal):

```
sudo ./mdmcore-linux-x86_64.sh \
--https-cert-path="full_path/proxycert.pfx" \
--https-cert-password="I23456789" \
--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
```

Para obtener una lista completa de los parámetros disponibles (imprima mensaje de ayuda), use:

```
--help
```

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

Parámetros necesarios del comando de instalación

Hay muchos parámetros de instalación opcionales, pero algunos de ellos son obligatorios:

- Certificado de pares: existen dos métodos para obtener el certificado de pares de ESET PROTECT:
  - **Instalación asistida por servidor**: necesitará credenciales de administrador de la consola web ESET PROTECT (el instalador descargará automáticamente los certificados necesarios).
  - **Instalación fuera de línea**: necesitará proporcionar un Certificado de pares (certificado de proxy exportado desde ESET PROTECT). Como alternativa, puede usar su certificado personalizado.
    - Para el caso de **Instalación asistida del Servidor** incluya como mínimo:

```
--webconsole-password=
```

    - Para el caso de **Instalación fuera de línea** incluya:

```
--cert-path=
--cert-password=
```

(El certificado de agente predeterminado creado durante la instalación del servidor ESET PROTECT 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 al Servidor ESET PROTECT (nombre o dirección de 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 lo siguiente:

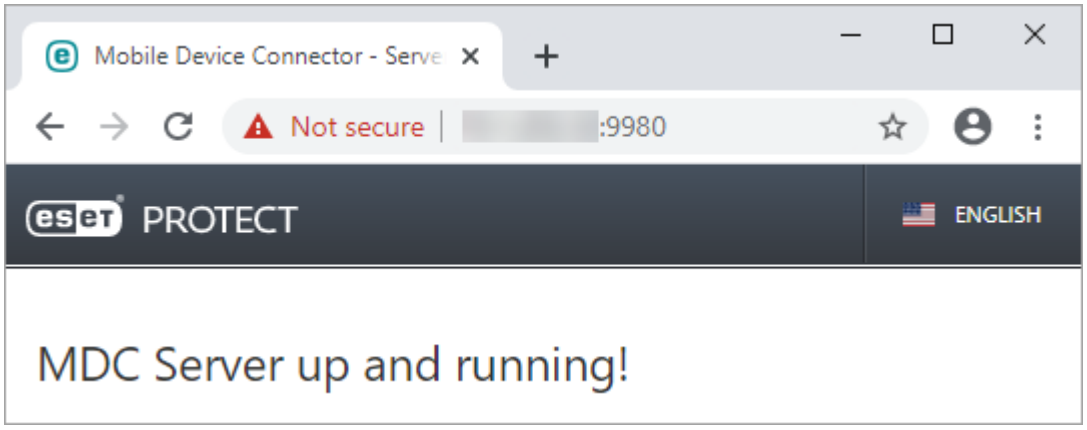
```
--db-type="Microsoft SQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

Registro del instalador

El registro del instalador puede resultar útil para solucionar problemas y puede encontrarlo en Archivos de registro.

Después de completar la instalación, verifique si el Conector de dispositivo móvil se ejecuta correctamente abriendo *https://your-mdm-hostname:enrollment-port* (por ejemplo *https://eramdm:9980*) en su navegador

web. Si la instalación fue exitosa, verá el siguiente mensaje:



También puede usar esta URL para verificar la disponibilidad del servidor del Conector de dispositivo móvil desde Internet (si está configurado de esa manera) ingresando desde un dispositivo móvil. Si no puede conectarse con la página, revise su firewall y la configuración en la infraestructura de su red.

Prerrequisitos para el Conector de dispositivo móvil - Linux

Los siguientes prerrequisitos se deben cumplir para poder instalar el Conector de dispositivo móvil en Linux:

- Un servidor de la 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 crear la cuenta).
- Un controlador ODBC para la conexión con el servidor de la base de datos (MySQL/MS SQL) instalado en el equipo. Consulte el capítulo Instalación y configuración de ODBC.

> Debería usar el paquete `unixODBC_23` (no el `unixODBC`predeterminado) para que el MDC se conecte a la base de datos MySQL sin inconvenientes. Esto es particularmente correcto para SUSE Linux.

> Le recomendamos que despliegue su componente MDM en un dispositivo host aparte de donde está alojado el Servidor de ESET PROTECT.

- Archivo de instalación de MDMCore configurado como ejecutable.

```
chmod +x mdmcore-linux-x86_64.sh
```

- Luego de la instalación, verifique que el servicio MDMCore se encuentre activo.

```
sudo systemctl status eramdmcore
```

- Le recomendamos **usar la versión más reciente de OpenSSL 1.1.1**. OpenSSL 3.x no es compatible. La versión compatible mínima de OpenSSL para Linux es openssl-1.0.1e-30. Puede haber más versiones de OpenSSL instaladas en un sistema de forma simultánea. Debe haber al menos una versión compatible presente en su sistema.
  - Use el comando `openssl version` para mostrar la versión predeterminada actual.
  - Puede mostrar una lista de 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 verificar si el cliente de Linux es compatible mediante el siguiente comando: `openssl s_client -connect google.com:443 -tls1_2`

> **i** Si su base de datos MDM en MySQL es muy grande (miles de dispositivos), el valor de `innodb_buffer_pool_size` predeterminado es 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 de los certificados

- Necesitará un **certificado SSL** en formato *.pfx* para garantizar la comunicación en HTTPS. Le recomendamos que utilice un certificado provisto por una Autoridad de certificación de terceros. No se recomiendan los certificados autofirmados (incluso los certificados firmados por la autoridad de certificación de ESET PROTECT) porque no todos los dispositivos móviles permiten a sus usuarios aceptar certificados autofirmados.

- Necesitará tener un certificado firmado por la AC y la clave privada correspondiente y usar los procedimientos estándar (tradicionalmente, mediante OpenSSL) para fusionarlos en un archivo *.pfx*: `openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out httpsCredentials.pfx`
Es un procedimiento estándar para la mayoría de los servidores que usan certificados SSL.

- Para la instalación fuera de línea, además necesitará un certificado de pares (el **certificado del agente** exportado desde ESET PROTECT). Como alternativa, puede usar su certificado personalizado con ESET PROTECT.

Instalación de Proxy HTTP Apache: Linux

Los agentes ESET Management pueden conectarse con el Servidor ESET PROTECT mediante Apache HTTP Proxy. Obtenga más información sobre cómo funciona el proxy para Agentes ESET Management.

Normalmente Apache HTTP Proxy se distribuye como un paquete `apache2` o `httpd`.

Elija los pasos de instalación del Proxy Apache HTTP según la distribución de Linux que use en su servidor: Si desea usar Apache para almacenar en caché los resultados de ESET LiveGuard Advanced, consulte también la documentación relacionada.

Instalación en Linux (distribución genérica) del Proxy Apache HTTP

1. Instalar servidor HTTP Apache (al menos la versión 2.4.10).

2. Verifique que se carguen 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. Agregar la configuración de 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 es directorio */var/cache/apache2/mod_cache_disk* no existe, créelo y asígnele privilegios de Apache (r,w,x).

5. Agregar configuración 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. En forma predeterminada, el puerto 2222 se usa para la comunicación con el Agente ESET Management. Si cambió el puerto durante la instalación, use el número de puerto modificado. Cambie 2222 en la línea: `AllowCONNECT 443 563 2222 8883 53535` para su número de puerto.

7. Habilite el proxy de caché añadido y la configuración (si la configuración se encuentra en el archivo de configuración principal de Apache, podrá omitir este paso).

8. De ser necesario, cambie al puerto que desee (el predeterminado es el puerto 3128).

9. Autenticación básica opcional:

- Agregar configuración de autenticación al directorio 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 un archivo de forma manual denominado group.file con `usergroup:username`

10. Reinicie el Servidor Apache HTTP.

Ubuntu Server y otra instalación de distribuciones Linux basada en Debian del Servidor Apache HTTP

1. Instale la versión más reciente del Servidor Apache HTTP desde el repositorio apt:

```
sudo apt-get install apache2
```

2. Ejecute el siguiente comando para cargar los módulos de Apache que necesite:

```
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 de almacenamiento de caché de Apache:

```
sudo vim /etc/apache2/conf-available/cache_disk.conf
```

y copie / 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. Ese paso no debería ser necesario, pero si no existe un directorio de 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 de proxy de Apache:

```
sudo vim /etc/apache2/conf-available/proxy.conf
```

y copie / 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. En forma predeterminada, el puerto 2222 se usa para la comunicación con el Agente ESET Management. Si cambió el puerto durante la instalación, use el número de puerto modificado. Cambie 2222 en la línea: `AllowCONNECT 443 563 2222 8883 53535` para su número de puerto.

7. Habilite los archivos de configuración que editó en los pasos anteriores:

```
sudo a2enconf cache_disk.conf proxy.conf
```

8. Cambie el puerto de escucha del Servidor Apache HTTP a 3128. Edite el archivo */etc/apache2/ports.conf* y reemplace `Listen 80` por `Listen 3128`.

9. Autenticación básica opcional:

```
sudo vim /etc/apache2/mods-enabled/proxy.conf
```

oCopiar/pegar 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


oInstale apache2-
utils y cree un nuevo archivo de contraseñas (por ejemplo, nombre de usuario: user,
grupo: usergroup):

sudo apt-get install apache2-utils
sudo htpasswd -c /etc/apache2/password.file user

oCree un archivo llamado grupo:

sudo vim /etc/apache2/group.file

y copie / pegue la siguiente línea:
```

```
usergroup:user
```

10. Reinicie el Servidor Apache HTTP con el siguiente comando:

```
sudo systemctl restart apache2
```

Reenvío solo para la comunicación de ESETPara permitir el reenvío solo para la comunicación de ESET, elimine lo siguiente:

```
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

Y agregue 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>
```

Reenviando para todas las comunicaciones

Para permitir el reenvío de todas las comunicaciones, agregue lo siguiente:

```
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

y elimine 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>
```

Encadenamiento proxy (todo el tráfico)

ESET PROTECT no admite el encadenamiento de proxy cuando estos requieren autenticación. Puede usar su propia solución proxy de red transparente; sin embargo, es posible que se requieran configuraciones adicionales además de las mencionadas aquí. Agregue lo siguiente a la configuración proxy (la contraseña funciona solamente en proxy secundario):

```
<VirtualHost *:3128>
ProxyRequests On
ProxyRemote * http://IP_ADDRESS:3128
</VirtualHost>
```

Cuando se use el encadenamiento proxy en el aparto virtual ESET PROTECT , debe especificar la política SELinux. Abra el terminal en el AV ESET PROTECT y ejecute el siguiente comando:

```
/usr/sbin/setsebool -P httpd_can_network_connect 1
```

Configurar el proxy HTTP para una gran cantidad de clientes

Si usa un Apache HTTP Proxy de 64 bits, puede aumentar el límite de subprocesos para su Apache HTTP Proxy. Edite el archivo de configuración de *httpd.conf*, dentro de la carpeta Apache HTTP Proxy. Encuentre los siguientes ajustes en el archivo y actualice los valores para que coincidan con la cantidad de clientes.

Substituya el valor de ejemplo de `5000` con su cantidad. El valor máximo es `32000`.

```
ThreadLimit 5000
ThreadsPerChild 5000
```

No cambie el resto del archivo.

Configure el proxy Apache HTTP para enviar las conexiones entre agentes y servidores

1.Abra el archivo en el equipo del proxy

i.Distribuciones Debian
`/etc/apache2/mods-available/proxy.conf`

ii.Distribuciones de Red Hat
`/etc/httpd/conf/httpd.conf`

2.Agregue las siguientes líneas al final del archivo:
`AllowCONNECT 443 563 2222 8883 53535`

3.Abra el archivo en el equipo del proxy

i.Distribuciones Debian
`/etc/apache2/apache2.conf`

ii.Distribuciones de Red Hat

```
/etc/httpd/conf/httpd.conf
```

4.Busque la línea:
`Listen 80`
y cámbiela a
`Listen 3128`

5.Si agregó restricciones para las direcciones en la configuración de proxy (paso 1), debe permitir el acceso al Servidor ESET PROTECT:

Agregue un segmento `ProxyMatch` aparte:

I.La dirección usada por sus Agentes para conectarse con el Servidor de ESET PROTECT.

II.Todas las direcciones posibles del Servidor ESET PROTECT(IP, FQDN)
(agregue el siguiente código completo; la dirección IP 10.1.1.10 y el nombre de host `hostname.example` son solo ejemplos que debe sustituir por sus direcciones. También puede generar la expresión `ProxyMatch` 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 memoria caché

Puede utilizar htcachceclean para configurar el tamaño de la memoria caché y la limpieza de la memoria caché de Apache HTTP Proxy. Consulte las instrucciones de configuración de la memoria caché para un aparato virtual de ESET PROTECT.

Configuración de SELinux

Cuando usa Proxy en el Aparato virtual ESET PROTECT, debe modificar la política SELinux (otras distribuciones de Linux pueden tener el mismo requisito). Abra el terminal en el AV 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 Servidor Ubuntu

Podrá usar el proxy Squid en lugar del Apache en el Servidor Ubuntu. Para instalar y configurar Squid en el Servidor Ubuntu (y en distribuciones de Linux similares basadas en Debian), siga los siguientes pasos:

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
```

con:

```
cache_dir ufs /var/spool/squid3 3000 16 256 max-size=200000000
```

- Además, puede cambiar el tamaño de caché total (3000 MB en el ejemplo) y el número de subdirectorios de primer nivel (16 en el ejemplo) y de segundo nivel (256 en el ejemplo) en el directorio de caché.
- El parámetro `max-size` define el tamaño máximo del archivo almacenado en caché 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 tengan acceso al proxy.

5. Reinicie el servicio squid3:

```
sudo systemctl restart squid3
```

Herramienta de replicación: Linux

¿Es usuario de Windows?

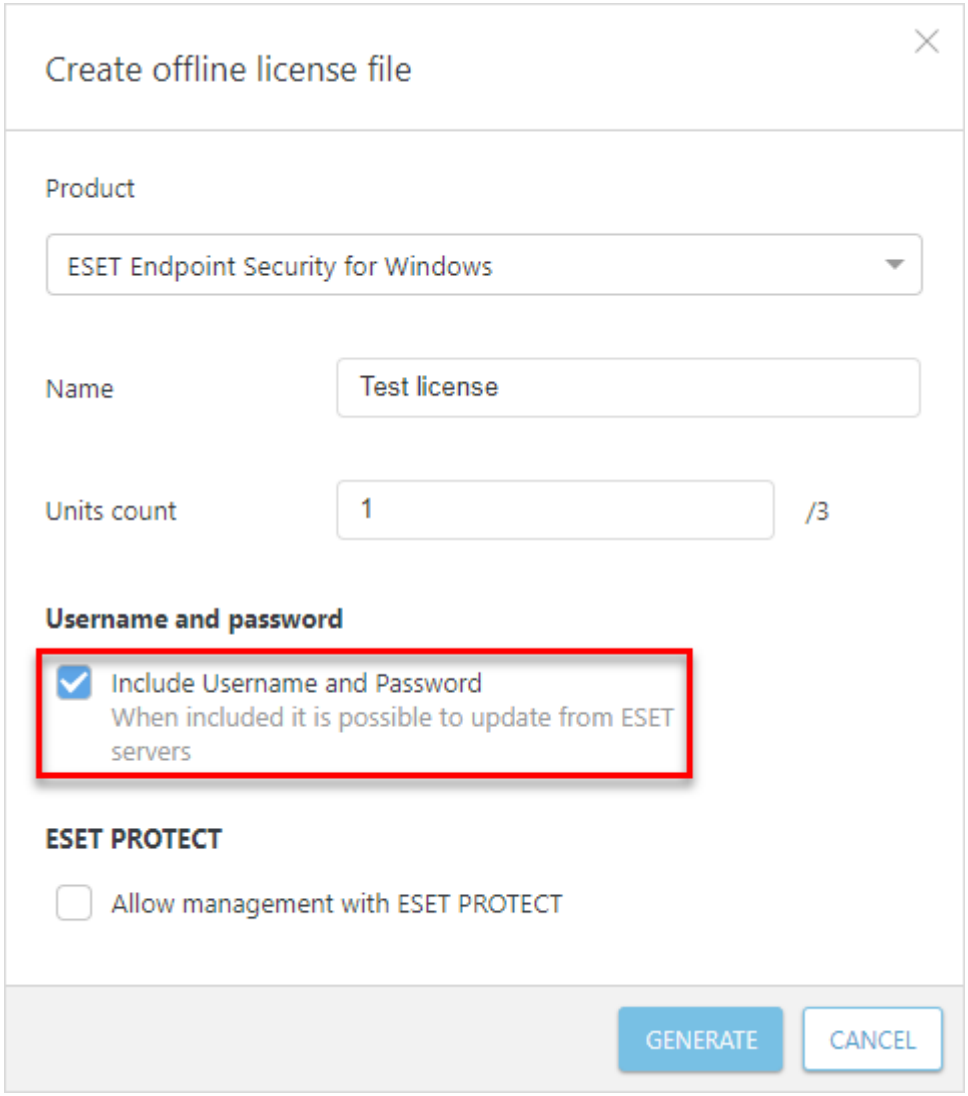
La herramienta de replicación es necesaria para la actualizaciones del motor de detección fuera de línea. Si los equipos de su cliente no tienen conexión a Internet y necesitan actualizaciones del motor de detección, puede usar la herramienta de replicación para descargar los archivos de actualización de los servidores ESET y almacenarlos localmente.

La Herramienta de replicación descarga solamente actualizaciones del motor de detección y otros módulos del programa; no descarga PCU (Actualizaciones de componentes del programa) ni datos de ESET LiveGrid®. Además, puede crear un repositorio fuera de línea completo. Alternativamente, puede actualizar individualmente los productos.

Requisitos previos

- La carpeta de destino debe estar disponible para el uso compartido, servicio Samba/Windows o HTTP/FTP, según cómo desea tener accesibles las actualizaciones.
  - Productos de seguridad de ESET para Windows: puede actualizarlos de forma remota con 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 fuera de línea válido que incluye el nombre de usuario y la contraseña. Cuando genere un archivo de licencia, asegúrese de seleccionar la casilla de verificación junto a **Incluir nombre de usuario y contraseña**. Además, debe ingresar un **nombre** de licencia. Se necesita un archivo de licencia fuera de línea para la activación de la herramienta de replicación y la generación de la replicación de la actualización.



Como usar la herramienta de replicación

1.Descargue la herramienta de replicación de la página de descarga de ESET (sección **Instaladores independientes**).

2.Descomprima el archivo descargado.

3.Abra el terminal en la carpeta con el archivo *MirrorTool* y convierta al archivo en ejecutable:

```
chmod +x MirrorTool
```

4.Ejecute el siguiente comando para ver todos los parámetros disponibles para la herramienta de replicación 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 diferencian entre mayúsculas y minúsculas.

Parámetro	Descripción
`--updateServer`	Cuando lo usa, debe especificar el URL completo del servidor de actualización.
`--offlineLicenseFilename`	Debe especificar una ruta hacia su archivo de licencia fuera de línea (como se mencionó arriba).
`--mirrorOnlyLevelUpdates`	No se necesita ningún argumento. Si está configurado, se descargarán únicamente las actualizaciones de nivel (no se descargarán las actualizaciones nano). Obtenga más información sobre los tipos de actualización en nuestro artículo de la base de conocimiento.
`--mirrorFileFormat`	⚠ Antes de usar el parámetro `--mirrorFileFormat`, asegúrese de que el entorno no contenga ambas versiones del producto de seguridad de ESET, es decir, la anterior (6.5 y anteriores) y la más nueva (6.6 y posteriores). El uso incorrecto de este parámetro puede tener como resultado actualizaciones incorrectas en sus productos de seguridad ESET. Puede indicar qué tipo de archivos de actualización se descargarán. Valores posibles (distingue entre mayúsculas y minúsculas): • `dat`: use este valor si tiene un entorno solo con versiones del producto de seguridad ESET 6.5 y anteriores. • `dll`: use este valor si tiene un entorno solo con versiones del producto de seguridad ESET 6.6 y posteriores. El parámetro se ignora cuando se crea una replicación para los productos de legado (`ep4`, `ep5`).
`--compatibilityVersion`	Este parámetro opcional se aplica a la herramienta de replicación distribuida con ESET PROTECT 8.1 y versiones posteriores. La herramienta de replicación 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 de repositorio distribuidos con ESET PROTECT 9: `--filterFilePath` y `--dryRun`:
1.Cree un filtro en un formato *JSON* (ver `--filterFilePath` a continuación).
2.Ejecute una herramienta de replicación de prueba ejecutada con el parámetro `--dryRun` (ver a continuación) y ajuste el filtro según sea necesario.
3.Ejecute la herramienta de replicación con el parámetro `--filterFilePath` y el filtro de descarga definido, junto con los parámetros `--intermediateRepositoryDirectory` y `--outputRepositoryDirectory`.
4.Ejecute la herramienta de replicación periódicamente para utilizar siempre los instaladores más recientes.

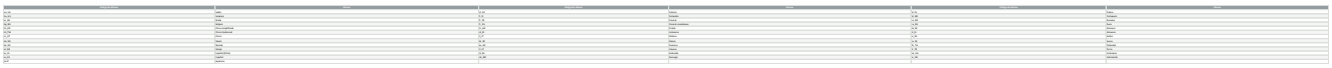
Parámetro	Descripción

`--filterFilePath`	Use este parámetro opcional para filtrar productos de seguridad de ESET en función de un archivo de texto en formato *JSON* situado en la misma carpeta que la herramienta de replicación, por ejemplo: `--filterFilePath filter.txt`)
	Descripción de 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 verdadero, se incluirán productos heredados.
	o`defaults` (objeto *JSON*, opcional): define las propiedades del filtro que se aplicará a todos los productos.
	■`languages` (lista): especifique los códigos de idioma de los idiomas ISO que desea incluir, por ejemplo, para el tipo francés `"fr_FR"`. La siguiente tabla contiene 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 incluirán (`["x64", "x86", "arm64"]`).
	Use el filtro `platforms` con cuidado. Por ejemplo, si la herramienta de replicación descarga solo instaladores de 64 bits y su infraestructura contiene equipos de 32 bits, los productos de seguridad de ESET de 64 bits no se instalarán en equipos de 32 bits.
	■`os_types` (lista): tipos de SO que se incluirán (`["windows"]`, `["linux"]`, `["mac"]`).
	o`products` (lista de objetos JSON, opcional): filtros que se aplican a productos específicos; anulación de `defaults` para productos especificados. Los objetos tienen las siguientes propiedades:
	■`app_id` (cadena): necesario si no se especifica `name`.
	■`name` (cadena), necesario si no se especifica `app_id`.
	■`version` (cadena): especifica la versión o el intervalo de versiones que se incluirán.
	■`languages` (lista): códigos de idioma ISO de los idiomas que se incluirán (consulte la tabla que aparece a continuación).
	■`platforms` (lista): plataformas que se incluirán (`["x64", "x86", "arm64"]`).
	■`os_types` (lista): tipos de SO que se incluirán (`["windows"]`, `["linux"]`, `["mac"]`).
	Para determinar los valores adecuados para los campos, ejecute la herramienta de replicación en el modo simulacro y busque el producto correspondiente en el archivo CSV creado.
	Descripciones de formato de la cadena de versiones
	Todos los números de versión están compuestos por cuatro números separados por puntos (por ejemplo, `7.1.0.0`). Puede especificar menos números al escribir filtros de versión (por ejemplo, `7.1`) y el resto de los números será cero (`7.1` es igual a `7.1.0.0`).
	La cadena de versiones puede tener uno de los dos formatos siguientes:
	• [>|<|>=|<=|=]<n>.(<n>.(<n>.(<n>)))
	oSelecciona las versiones posteriores/inferiores o iguales/inferiores, iguales/iguales que la versión especificada.
	• <n>.(<n>.(<n>.(<n>))) - <n>.(<n>.(<n>.(<n>)))
	oSelecciona las versiones que son posteriores o iguales que el límite inferior e inferior o igual que el límite superior.
	Las comparaciones se realizan de forma sencilla 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` reemplaza a los parámetros `--languageFilterForRepository`, `--productFilterForRepository` y `--downloadLegacyForRepository` utilizados en versiones anteriores de la herramienta de replicación (lanzados con ESET PROTECT 8.x).

Parámetro	Descripción
`--dryRun`	Si usa este parámetro opcional, la herramienta de replicación no descargará ningún archivo, pero generará un archivo *.csv* con una lista de todos los paquetes que se descargarán. Puede usar 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 de replicación los incluirá en el archivo *.csv* aunque especifique `idiomas` en `--filterFilePath`. Si usa el parámetro `--dryRun` y también los parámetros `--intermediateRepositoryDirectory` y `--outputRepositoryDirectory`, la herramienta de replicación no borra el *outputRepositoryDirectory*.
`--listUpdatableProducts`	Enumere 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 de Mirror Tool: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).

La herramienta de replicación crea una estructura de carpetas diferente de lo que hace la replicación de punto de conexión. Cada carpeta contiene archivos de actualización de productos. Debe especificar la ruta completa a la carpeta correcta en la configuración de la actualización del producto con la replicación. Por ejemplo, para actualizar ESET PROTECT 9 de la replicación, establezca el Actualizar servidor en (de acuerdo con la ubicación raíz de su servidor HTTP):
`http://your_server_address/mirror/eset_upd/era6`
Nota: La carpeta mirror `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 fuera de línea con productos seleccionados, idiomas y descarga habilitada de archivos anteriores, definidos en el archivo *filter.txt* (ver el ejemplo anterior de contenido del archivo en `--filterFilePath` detalle):

```
sudo ./MirrorTool --repositoryServer AUTOSELECT \
--intermediateRepositoryDirectory /tmp/repoTemp \
--outputRepositoryDirectory /var/lib/tomcat9/webapps/mirrorRepo \
--filterFilePath filter.txt
```

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

Configuración de herramienta de replicación y actualización

- Para automatizar las descargas para las actualizaciones de módulos, puede crear un programa para ejecutar la herramienta de replicación. Para ello, abra su consola web y vaya a **Tareas de clientes** > **Sistema operativo** > **Ejecutar comando. Seleccione Línea de comandos a ejecutar** (incluso una ruta a *MirrorTool.exe*) y un activador razonable (como CRON para cada hora 0 0 * * * ? *). Como alternativa, puede usar el programador de tareas de Windows o `Cron` en Linux.

- Para configurar las actualizaciones en un equipo del cliente, cree una nueva política y configure **Actualizar servidor** para apuntar a su dirección de replicación o carpeta compartida.

Instalación de componentes en macOS

En la mayoría de los escenarios de instalación, necesita instalar diferentes componentes de ESET PROTECT en distintas máquinas para admitir las diferentes arquitecturas de red, cumplir con los requisitos de rendimiento, o por otros motivos.

MacOS solo es compatible como cliente. El Agente ESET Management y los productos ESET para macOS se pueden instalar en macOS. Sin embargo, no se puede instalar el servidor ESET PROTECT en macOS.

Instalación del agente: macOS

Puede instalar el Agente de ESET Management en macOS de dos maneras:

- De forma remota: mediante la tarea del Servidor **Instalación del agente**. Si tiene problemas para implementar el agente ESET Management de manera remota (la tarea del servidor **Implementación del agente** finaliza con un estado de Error) consulte Resolución de problemas en la implementación de agentes.

- Localmente: consulte las instrucciones que se indican a continuación.

Requisitos previos

- ESET PROTECTSe instalan el Servidor y la Consola web ESET PROTECT (en un equipo servidor).

- Se creó un certificado de agente y se preparó en su disco local.

- Se preparó una Autoridad de certificación en su disco local (solo es necesario para certificados sin firmar).

Instalación

Siga los pasos indicados a continuación para instalar el componente del Agente de ESET Management de forma

local en macOS:

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

1. Obtenga el archivo de instalación (instalador de agente independiente *.dmg*) desde el sitio de descargas de ESET o su administrador de sistema.

2. Haga doble clic en el archivo *Agent-MacOSX-x86_64.dmg* y, luego, haga doble clic en el archivo *.pkg* para iniciar la instalación.

3. Proceda con la instalación. Cuando se le pregunte, escriba los datos de **conexión del Servidor**:

- **Nombre de host del servidor**: nombre de host o dirección IP del servidor de ESET PROTECT
- **Puerto de servidor**: puerto para la comunicación entre el Agente y el servidor, predeterminado en 2222.
- **Usar Proxy**: haga clic si desea usar el Proxy HTTP par la conexión entre el agente y el servidor.

Esta configuración de proxy sólo se usa para (replicación) entre el Agente de ESET Management y el Servidor de ESET PROTECT, no para almacenar actualizaciones en caché.
- **Nombre de host del proxy**: nombre de host o dirección IP de la máquina del Proxy HTTP.
- **Puerto del Proxy**: el valor predeterminado es 3128.
- **Nombre de usuario**, **Contraseña**: ingrese las credenciales que usa su proxy si usa autenticación.

Puede cambiar la configuración de proxy más adelante en su política. El Proxy debe instalarse antes de que pueda configurar la conexión entre el Agente y el Servidor vía Proxy.

4. Seleccione un certificado de pares y una contraseña para dicho certificado. Opcionalmente, puede agregar una Autoridad de certificación.

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

5. Revise la ubicación de la instalación y haga clic en **Instalar**. El Agente se instalará en su equipo.

6. El archivo de registro del Agente ESET Management se puede encontrar aquí:

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/
/Users/%user%/Library/Logs/EraAgentInstaller.log

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

Imagen ISO

Un archivo de imagen ISO es uno de los formatos en los que puede descargar los instaladores (en la categoría de instaladores todo en uno) de ESET PROTECT. La imagen ISO contiene lo siguiente:

- Paquete del instalador ESET PROTECT

- Instaladores independientes para cada componente

La imagen ISO es útil cuando desea mantener todos los instaladores de ESET PROTECT en un solo lugar. También elimina la necesidad de descargar los instaladores del sitio web de ESET cada vez que necesita ejecutar la instalación. La imagen ISO también es útil cuando desea instalar ESET PROTECT en un equipo virtual.

Registro de servicio DNS

Para configurar un registro de recursos DNS:

1.En su servidor DNS (servidor DNS en su controlador de dominio), ingrese a **Panel de control** > **Herramientas de administración**.

2.Seleccione el valor de DNS.

3.En el administrador de DNS, seleccione _tcp desde el árbol y cree un nuevo registro de **Ubicación de servicio (SRV**).

4.Ingrese el nombre del servicio en el campo **Servicio** de acuerdo a las reglas DNS estándar, escriba el símbolo de guion bajo (**_**) adelante del nombre del servicio (use su propio nombre de servicio, por ejemplo **_era**).

5.Ingrese el protocolo tcp en el campo **Protocolo** con el siguiente formato:_tcp.

6.Ingrese el puerto 2222 en el campo **Número de puerto.**

7.Ingrese el nombre de dominio completamente calificado del Servidor ESET PROTECT en el campo **Host que ofrece este servicio**.

8.Haga clic en **Aceptar** > **Listo** para guardar el registro. El registro se mostrará en la lista.

Para verificar el registro DNS:

1.Inicie sesión en su dominio en cualquier equipo y abra un símbolo del sistema (cmd.exe).

2.Escriba `nslookup` en el símbolo del sistema y presione **Intro**.

3.Escriba `set querytype=srv` y presione **Intro**.

4.Escriba `_era._tcp.domain.name` y presione **Intro**. La ubicación del servicio se visualiza correctamente.

No olvide modificar el valor de “Host que ofrece este servicio:” en el FQDN de su servidor nuevo cuando instale el servidor de ESET PROTECT en un equipo distinto.

Escenario de instalación fuera de línea para 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 equipo 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 de JDK compatible (necesario para la consola web).
   - Instalador del agente de ESET Management
   - Instaladores de productos de seguridad de ESET (por ejemplo, ESET Endpoint Security)

En un equipo Windows sin conexión en la misma red local

1. Copie los instaladores de la carpeta compartida de red en un equipo Windows sin conexión en el que desee instalar ESET PROTECT.

2. Instale el paquete de 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 el Agente ESET Management en equipos de su entorno sin conexión mediante Script del instalador de agentes. Modifique el script de instalación para usar la nueva URL y así acceder al paquete de instalación del agente desde la carpeta de red compartida.

6. Implemente productos de seguridad de ESET en estaciones de trabajo mediante una Tarea de instalación de software. Seleccione **<Choose package>** y proporcione una URL personalizada para el paquete de instalación del repositorio local.

7. Active los puntos de conexión administrados con una licencia sin conexión.

8. Deshabilite ESET LiveGrid®.

Le recomendamos que mantenga actualizada la infraestructura de ESET sin conexión mediante el uso de un repositorio de actualizaciones local. Actualice los módulos de los productos de seguridad de ESET con regularidad. Si los módulos no se actualizan, la consola web de ESET PROTECT marca los equipos como **No actualizados**. Para silenciar esta advertencia de la consola web, haga clic en el equipo de la lista y seleccione **Silenciar** en el menú contextual.

Para obtener instrucciones sobre la actualización de ESET PROTECT, consulte Actualizar componentes de ESET

PROTECT en entornos fuera de línea.

Procedimientos de actualización

Existen diferentes maneras de actualizar su Servidor de ESET PROTECT y otros componentes de ESET PROTECT. Consulte también los procedimientos de migración y reinstalación.

⚠ Asegúrese de tener un sistema operativo compatible antes de realizar la actualización a ESET PROTECT 9.1. Si tiene una base de datos no compatible instalada (MySQL 5.5 o MS SQL 2008/2012), actualice su base de datos a una base de datos compatible antes de actualizar el servidor de ESET PROTECT.

Actualización de ERA 5 o 6.5

La actualización directa no es compatible. Consulte Migración desde ERA 5.x o actualización desde ERA 6.x.

Actualización de ESMC 7.2 a ESET PROTECT versión 9.1

Seleccione uno de los procedimientos de actualización:

Procedimiento de actualización	Sistema operativo	Comentario
Tarea Actualización de componentes en la consola web	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 a través del 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.
Actualice el aparato virtual de ESET PROTECT	Aparato virtual de Linux	

ℹ Para buscar qué versión de cada componente ESET PROTECT está ejecutando, verifique cuál es la versión de su Servidor ESET PROTECT. Vaya a la página Acerca de en la consola web de ESET PROTECT y consulte la lista de todas las versiones de componentes de ESET PROTECT.

Tarea de actualización de componentes ESET PROTECT

Recomendaciones antes de actualizar

Recomendamos usar la tarea ESET PROTECTActualización de componentes disponible en la consola web de ESET PROTECT para actualizar la infraestructura de ESET PROTECT. Revise con precaución las instrucciones proporcionadas aquí antes de realizar la actualización.

Si se produce un error en la actualización de componentes en un equipo que ejecuta la consola web o el servidor de ESET PROTECT, es posible que no pueda iniciar sesión en la consola web de forma remota. Se recomienda configurar el acceso físico a la máquina del servidor antes de realizar esta actualización. Si no puede disponer del acceso físico a la máquina, asegúrese de que pueda iniciar sesión en ella con privilegios de administración usando un escritorio remoto. Se recomienda realizar una copia de seguridad de las bases de datos del Servidor ESET PROTECT y del conector de dispositivo móvil antes de realizar esta operación. Para realizar copias de seguridad de su Dispositivo virtual, cree una instantánea o clone su equipo virtual.

¿Está actualizando desde el aparato virtual ESMC?

¿La instancia del servidor de ESET PROTECT está instalada en un clúster de conmutación por error?

Si la copia del Servidor ESET PROTECT se instala en un clúster de conmutación por error, deberá actualizar el componente del Servidor ESET PROTECT en cada clúster de forma manual. Después de actualizar el servidor de ESET PROTECT, ejecute la tarea Actualización de componentes para actualizar el resto de su infraestructura (por ejemplo, los Agentes ESET Management en los equipos cliente).

Instrucciones importantes antes de actualizar el proxy Apache HTTP en Microsoft Windows

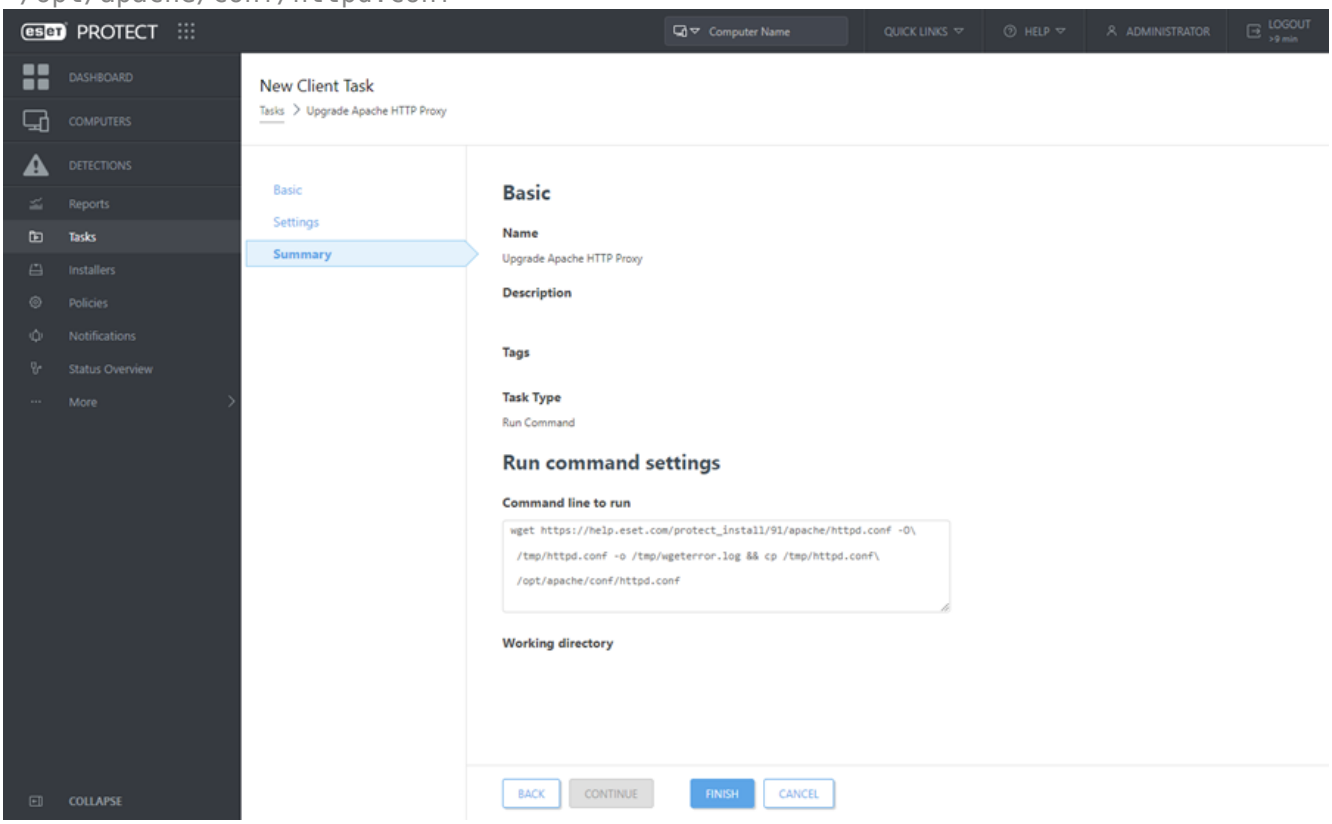
Si usa el Proxy Apache HTTP y tiene configuración predeterminada en su archivo *httpd.conf* (como nombre de usuario y contraseña), debe realizar una copia de seguridad del archivo original *httpd.conf* (ubicado en *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf*). Si no usa la configuración personalizada, no es necesario realizar una copia de seguridad del archivo *httpd.conf*. Realice una actualización a la última versión del Proxy Apache HTTP mediante alguno de los métodos a los que se hace referencia en Actualización del Proxy Apache HTTP.

Si ha actualizado con éxito Apache HTTP Proxy en Windows y completó una configuración personalizada en su archivos original *httpd.conf* (como nombre de usuario y contraseña), copie la configuración del archivo de copias de seguridad *httpd.conf* y aplique las configuraciones personalizadas solo al nuevo archivo *httpd.conf*. No use el archivo original *httpd.conf* con la nueva versión actualizada de Apache HTTP Proxy, no funcionará correctamente. Copie solo la configuración personalizada y use el archivo *httpd.conf* nuevo. Como alternativa, puede personalizar su nuevo archivo *httpd.conf* manualmente, la configuración se describe en Instalación de Proxy HTTP Apache: Windows.

Instrucciones importantes antes de actualizar el proxy Apache HTTP en el aparato virtual

Si usa **Apache HTTP Proxy** y tiene una configuración personalizada en su archivo *httpd.conf* (como su nombre de usuario y contraseña), realice una copia de seguridad de su archivo *httpd.conf* original (ubicado en */opt/apache/conf/*) y luego ejecute la **tarea de actualización de componentes de ESET PROTECT** para actualizar **Apache HTTP Proxy**. Si no usa configuración personalizada, no será necesario crear una copia de seguridad de *httpd.conf*.
Después de finalizar correctamente la tarea de actualización de componentes, ejecute el siguiente comando. Debe asignarlo a la máquina con Apache HTTP Proxy instalado. Después de finalizar correctamente la tarea de actualización de componentes, actualice el archivo *httpd.conf* (es necesario para la correcta ejecución de la versión actualizada de Apache HTTP Proxy):

```
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 Apache HTTP Proxy se ejecuta en su máquina AV, puede ejecutar el mismo comando directamente desde la consola del dispositivo virtual ESET PROTECT. Otra opción es reemplazar el archivo de configuración proxy de Apache HTTP httpd.conf manualmente.

Si tiene una configuración personalizada en su archivo original *httpd.conf* (como nombre de usuario y contraseña), copie la configuración desde el archivo de copia de seguridad *httpd.conf* y agregue solo la configuración personalizada al nuevo archivo *httpd.conf*. No use el archivo original *httpd.conf* con la nueva versión actualizada del proxy Apache HTTP, no funcionará correctamente. Copie solo la configuración personalizada y use el archivo original *httpd.conf*. Como alternativa, puede personalizar manualmente el nuevo archivo *httpd.conf*. Consulte la configuración detallada en Instalación de proxy HTTP Apache: Linux.

Puede actualizar a ESET PROTECT 9.1 únicamente desde la versión 7.2 y versiones posteriores de ESMC.
ESET PROTECT 9 le notifica automáticamente cuando hay una nueva versión del servidor de ESET PROTECT disponible.
Realice una copia de seguridad de los siguientes datos antes de ejecutar la actualización:
• Todos los certificados (Certificado de autoridad, Certificado del servidor y Certificado del agente)
• Exporte sus certificados de la autoridad de certificación desde un servidor de ESET PROTECT anterior en un archivo *.der* y guárdelo en un almacenamiento externo.
• Exporte sus certificados de pares (para el agente ESET Management, el servidor de ESET PROTECT) y el archivo de clave privada *.pfx* desde un servidor de ESET PROTECT anterior y guárdelo en un almacenamiento externo.
• Su base de datos ESMC/ESET PROTECT. Si tiene una base de datos no compatible instalada (MySQL 5.5 o MS SQL 2008/2012), actualice su base de datos a una base de datos compatible antes de actualizar el servidor de ESET PROTECT.

Asegúrese de tener un sistema operativo compatible antes de realizar la actualización a ESET PROTECT 9.1. Para actualizar los productos de seguridad ESET, ejecute la Tarea de instalación de software con el último paquete instalador para instalar la versión más reciente de su producto actual.

Procedimiento de actualización recomendado

1. Actualizar el servidor de ESET PROTECT: seleccione solo la máquina con el servidor de ESET PROTECT como destino para la tarea de **Actualización de los componentes de ESET PROTECT** .

2. Seleccione unos pocos equipos cliente (como ejemplo de prueba, al menos un cliente de cada sistema operativo y valor de bits) y ejecute la tarea **ESET PROTECTActualización de componentes** en ellos.

Se recomienda usar Apache HTTP Proxy (u otro proxy web transparente con almacenamiento en caché habilitado) para limitar la carga de la red. Los equipos cliente para prueba activarán la descarga/el almacenamiento en caché de los instaladores. Cuando la tarea se ejecute otra vez, se distribuirán los instaladores a los equipos cliente directamente desde caché.

3. Una vez que los equipos con el agente ESET Management actualizado se conectan correctamente al servidor ESET PROTECT, continúe con la actualización del resto de los clientes.

Para actualizar los agentes de ESET Management en todos los equipos administrados en la red, seleccione el Grupo estático **Todo** como destino para la tarea de **ESET PROTECT Actualización de componentes** . La tarea omitirá los ordenadores que ya ejecuten el Agente ESET Management más reciente.
ESET PROTECT 9.1 admite la actualización automática del agente ESET Management en equipos administrados.

Componentes actualizados automáticamente:

- ESET PROTECTServidor
- Agente ESET Management
- Consola web de ESET PROTECT: solo se aplica cuando se instalóApache Tomcat en su carpeta de instalación predeterminada en distribuciones Windows y Linux, incluido el aparato virtual ESET PROTECT (por ejemplo: */var/lib/tomcat8/webapps/*, */var/lib/tomcat7/webapps/*, */var/lib/tomcat/webapps/*).

Limitaciones de actualización de la consola web

- Apache Tomcat no se actualiza durante la actualización de la consola web de ESET PROTECT por medio de la tarea Actualización de componentes.
- ESET PROTECT La actualización de la consola web no funciona si Apache Tomcat se instaló en una ubicación personalizada.
- Si se instala una versión personalizada de Apache Tomcat (instalación manual del servicio Tomcat), la actualización posterior de la consola web de ESET PROTECT por medio del Instalador todo en uno o a través de la Tarea de actualización de componentes no será compatible.

- ESET PROTECT Conector de dispositivo móvil

Componentes que requieren una actualización manual:

Componentes de ESET

- ESET Rogue Detection Sensor: utilice la Tarea de instalación de 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 ESMC 7.2 y versiones posteriores, no necesita actualizarlo, ya que no hay nuevas versiones de RD Sensor.

Componentes de terceros

Además de los componentes de ESET, ESET PROTECT utiliza componentes de terceros que pueden estar desactualizados y requieren una actualización manual.

En la consola web de ESET PROTECT, haga clic en **Enlaces rápidos** > **Componentes desactualizados** para ver los componentes de terceros desactualizados.

El dispositivo virtual de ESET PROTECT no informa componentes de terceros obsoletos.

ESET PROTECT informa versiones anteriores a las indicadas a continuación como obsoletas:

Componente de terceros:	Versión:
Microsoft SQL Server	2019 (versión 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 del Motor de base de datos SQL Server e instale la actualización acumulativa más reciente.

2 ESET PROTECT no informa 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
- Apache HTTP Proxy

Solución de problemas

- Verifique si puede acceder al repositorio ESET PROTECT desde un equipo actualizado.
- No podrá volver a ejecutar la tarea Actualización de componentes de ESET PROTECT si ya existe al menos un componente actualizado a la nueva versión.
- Si no encuentra el motivo del error, puede actualizar los componentes manualmente. Consulte nuestras instrucciones para Windows o Linux.
- Consulte información general de solución de problemas para conocer más sugerencias para resolver los problemas de actualización.

Use el instalador todo en uno de ESET PROTECT 9.1 para la actualización

Use el instalador todo en uno de ESET PROTECT 9.1 para la actualización de ESMC 7.2 o una versión posterior de ESET PROTECT a la última versión de ESET PROTECT 9.1.

El instalador todo en uno es la opción de actualización recomendada si la instalación existente se realizó a través del 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 manera predeterminada.

- Si usa una edición anterior de Windows (servidor 2012 o SBS 2011), Microsoft SQL Server Express 2014 se instalará de manera 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 de cada base de datos relacionada. No recomendamos el uso de Microsoft SQL Server Express:
> - En entornos empresariales o redes de gran tamaño.
> - Si desea usar ESET PROTECT con ESET Inspect.

Puede actualizar a ESET PROTECT 9.1 únicamente desde la versión 7.2 y versiones posteriores de ESMC. Realice una copia de seguridad de los siguientes datos antes de ejecutar la actualización:

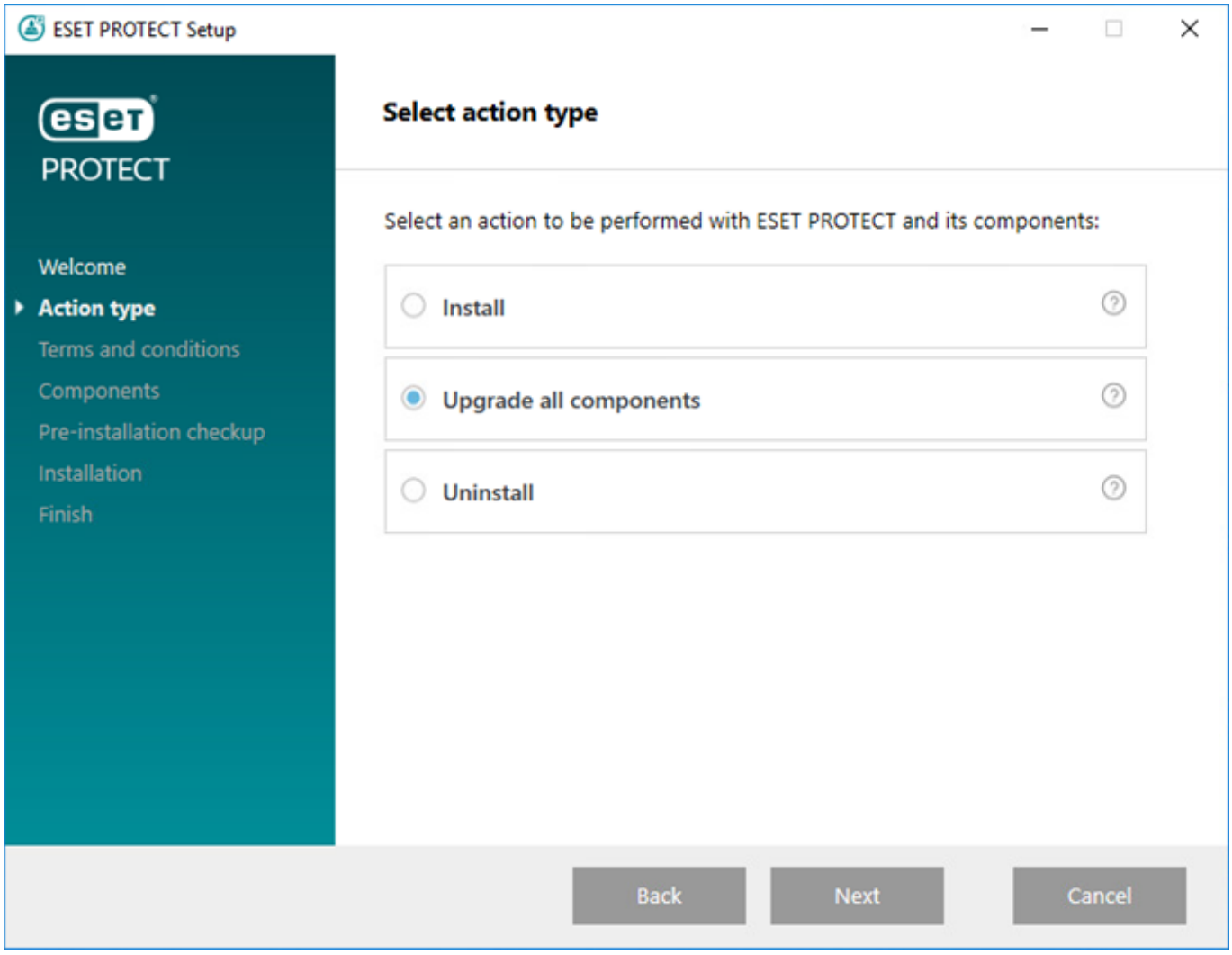
- Todos los certificados (Certificado de autoridad, Certificado del servidor y Certificado del agente)
- Exporte sus certificados de la autoridad de certificación desde un servidor de ESET PROTECT anterior en un archivo *.der* y guárdelo en un almacenamiento externo.
- Exporte sus certificados de pares (para el agente ESET Management, el servidor de ESET PROTECT) y el archivo de clave privada *.pfx* desde un servidor de ESET PROTECT anterior y guárdelo en un almacenamiento externo.
- Su base de datos ESMC/ESET PROTECT. Si tiene una base de datos no compatible instalada (MySQL 5.5 o MS SQL 2008/2012), actualice su base de datos a una base de datos compatible antes de actualizar el servidor de ESET PROTECT.

Asegúrese de tener un sistema operativo compatible antes de realizar la actualización 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 de usuario final**, acéptelo y haga clic en **Siguiente**.

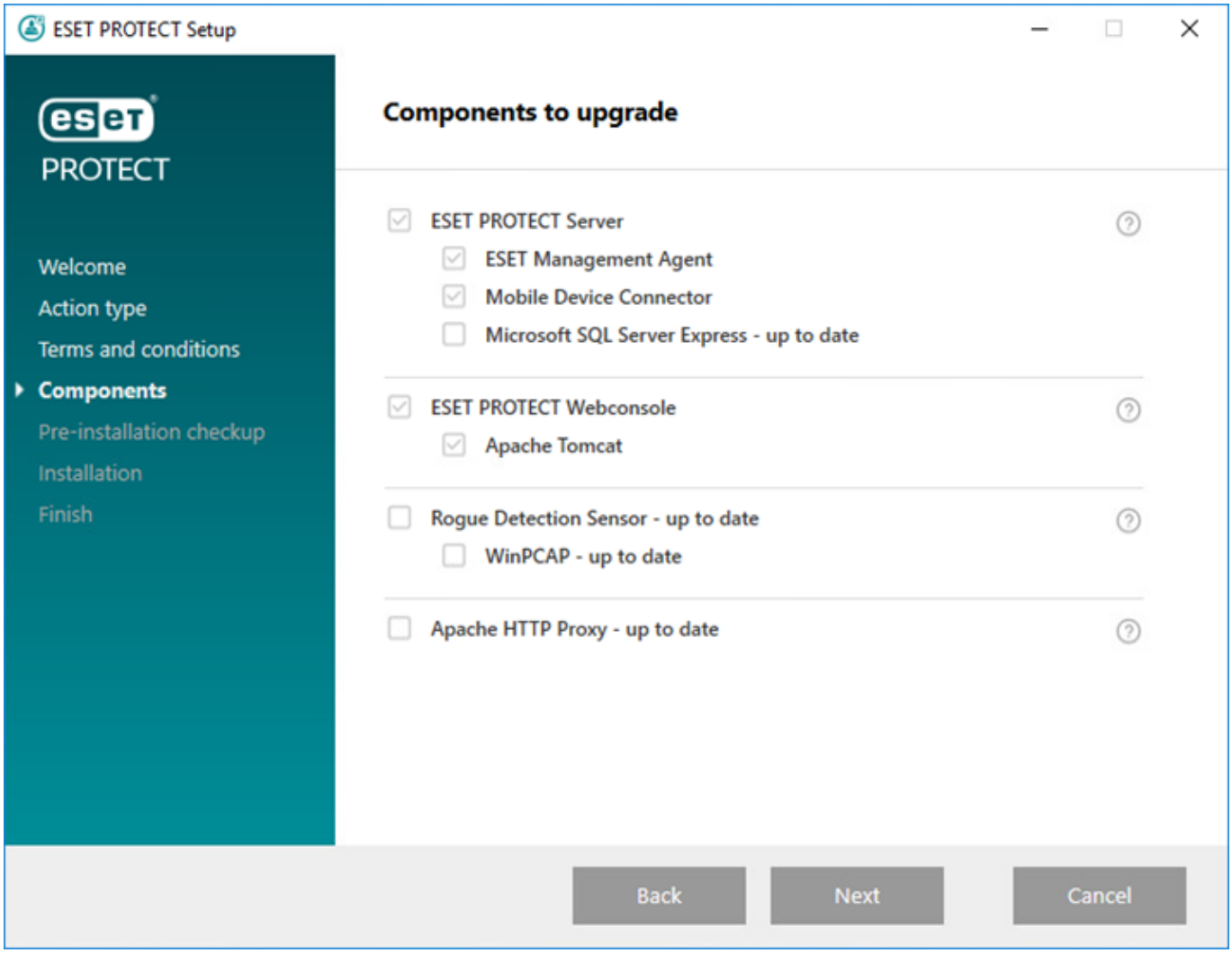
5.En **Componentes**, revise los componentes de ESET PROTECT que pueden actualizarse y haga clic en **Siguiente**.

Limitaciones de actualización de la consola web y Apache Tomcat

- Si se instala una versión personalizada de Apache Tomcat (instalación manual del servicio Tomcat), la actualización posterior de la consola web de ESET PROTECT por medio del Instalador todo en uno o a través de la Tarea de actualización de componentes no será compatible.
- La actualización de Apache Tomcat eliminará la carpeta de *era* folder ubicada en *C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\webapps*. Si usa la carpeta de *era* para almacenar datos adicionales, asegúrese de hacer una copia de seguridad de los datos antes de realizar la actualización.
- Si *C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\webapps* contiene datos adicionales (diferentes a las carpetas de *era* y *ROOT*), la actualización de Apache Tomcat no tendrá lugar y solo se actualizará la consola web.
- La consola web y la actualización de Apache Tomcat limpian los archivos de ayuda sin conexión. Si utilizó la ayuda sin conexión con ESMC o una versión anterior de ESET PROTECT, vuelva a crearla para ESET PROTECT 9.1 luego de realizar la actualización para asegurarse de tener la versión más reciente de la ayuda sin conexión que coincida con su versión de ESET PROTECT.

Limitaciones de actualización de Apache HTTP Proxy

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 usarla.



6.Siga la **Revisión previa a la instalación** para asegurarse de que su sistema cumpla con todos los requisitos previos.

7.Haga clic en **Actualizar** para iniciar la actualización de ESET PROTECT. La instalación puede llevar algo de

tiempo, en función de su sistema y la configuración de la red.

8.Cuando la actualización esté completa, haga clic en **Finalizar**.

9.Tras la actualización de ESET PROTECT, actualice el Agente ESET Management en los equipos administrados con la tarea Actualización de componentes. ESET PROTECT 9.1 admite la actualización automática del agente ESET Management en equipos administrados.

Actualización de ERA 6.5

No puede actualizar directamente a ESET PROTECT 9.1.

Si tiene instalado ERA 6.5, realice estas acciones:

1.Actualización de ERA 6.5 a ESET PROTECT 8.1.

2.Actualizar ESET PROTECT 8.1 a ESET PROTECT 9.1.

Actualización o copia de seguridad del servidor de la base de datos

ESET PROTECT usa una base de datos para almacenar datos del cliente. Las siguientes secciones proporcionan detalles para la copia de seguridad y la actualización de la base de datos del Servidor de ESET PROTECT (servidor ESMC) o la base de datos de MDM:

- Si no tiene configurada una base de datos para usar con el Servidor ESET PROTECT, **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 manera predeterminada.

  oSi usa una edición anterior de Windows (servidor 2012 o SBS 2011), Microsoft SQL Server Express 2014 se instalará de manera predeterminada.

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

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

- Si tiene una base de datos no compatible instalada (MySQL 5.5 o MS SQL 2008/2012), actualice su base de datos a una base de datos compatible antes de actualizar el servidor de ESET PROTECT.

Consulte también la migración de la base de datos de ESET PROTECT.

Se debe cumplir con los siguientes requisitos para Microsoft SQL Server:

• Instale una versión de Microsoft SQL Server compatible. Seleccione autenticación de **Modo mixto** durante la instalación.

• Si ya tiene Microsoft SQL Server instalado, establezca la autenticación a **Modo mixto (autenticación de SQL Server y autenticación de Windows)**. Para hacerlo, 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 que se detallan en este artículo de la base de conocimiento.

• Permita las conexiones TCP/IP al SQL Server. Para hacerlo, siga las instrucciones de este artículo de la base de conocimiento desde la parte **II. Permita las conexiones TCP/IP a la base de datos SQL**.

• Para configurar, administrar y gestionar 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/Essentials). Recomendamos que instale ESET PROTECT en un servidor diferente o que no seleccione el componente SQL Server Express durante la instalación (esto requiere que use un SQL Server o un MySQL existente para ejecutar la base de datos ESET PROTECT).

Copia de seguridad y restauración del servidor de la base de datos

Toda la información y la configuración de ESET PROTECT se almacenan en la base de datos. Se recomienda que haga una copia de seguridad de su base de datos periódicamente para evitar la pérdida de datos. Puede utilizar la copia de seguridad más adelante cuando realice la migración de ESET PROTECT a un servidor nuevo. Consulte la sección correspondiente a su base de datos a continuación:

• Los nombres de las bases de datos y los archivos de registros son iguales incluso luego de cambiar el nombre del producto de ESET Security Management Center a ESET PROTECT.
• Si usa el aparato virtual ESET PROTECT, siga las instrucciones de copia de seguridad de la base de datos del aparato virtual.

Ejemplos de copias de seguridad de MS SQL

Para realizar una copia de seguridad de la base de datos de MS SQL a un archivo, siga los siguientes ejemplos:

Estos ejemplos están destinados al uso con las configuraciones predeterminadas (por ejemplo, nombre de la base de datos predeterminada o configuración de la conexión de la base de datos). El script de la copia de seguridad debe personalizarse para acomodarse a los cambios que realice a las configuraciones predeterminadas.
Debe tener suficientes derechos para ejecutar los siguientes comandos. Si no usa una cuenta de usuario de administrador local, debe cambiar la ruta de la copia de seguridad, por ejemplo *'C:\USERS\PUBLIC\BACKUPFILE'*.

Copia de seguridad de la base de datos por única vez

Ejecute este comando en un símbolo del sistema de Windows para crear una copia de seguridad dentro del archivo llamado **BACKUPFILE**:

```
SQLCMD -S HOST\ERASQL -
```

```
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'"
```

> En este ejemplo, **HOST** se refiere a la dirección IP o al nombre de host y **ERASQL** al nombre de la instancia del servidor MS SQL. Puede instalar el servidor ESET PROTECT en una instancia personalizada llamada SQL (cuando usa la base de datos MS SQL). Modifique los scripts de la copia de seguridad correspondiente en este escenario.

Copia de seguridad regular de la base de datos con el script SQL

Seleccione uno de los siguientes scripts SQL:

a)Crear copias de seguridad regulares y almacenarlas en base a la 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 la base de datos MS SQL desde un archivo, siga el siguiente ejemplo:

```
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 la base de datos de MySQL a un archivo, siga el siguiente ejemplo:

```
mysqldump --host HOST --disable-keys --extended-insert --routines -u ROOTLOGIN -
p DBNAME -r BACKUPFILE
```

> En este ejemplo **HOST** se refiere a la dirección IP o al nombre de host del servidor de MySQL, **ROOTLOGIN** a la cuenta raíz del servidor MySQL y **DBNAME** al nombre de la base de datos ESET PROTECT.

Restauración de MySQL

Para restaurar la base de datos de MySQL desde un archivo, siga el siguiente ejemplo:

```
mysql --host HOST -u ROOTLOGIN -p DBNAME < BACKUPFILE
```

> Para obtener más información sobre las copias de seguridad del servidor Microsoft SQL, visite el sitio web de Microsoft TechNet. Para obtener más información sobre las copias de seguridad del servidor Microsoft SQL, visite el sitio web de MySQL.

Actualización del servidor de bases de datos

Siga las instrucciones a continuación para actualizar una instancia del Servidor Microsoft SQL a una versión más reciente que pueda usarse con una base de datos del Servidor ESET PROTECT:

1. Detenga todos los servicios del Servidor ESMC/ESET PROTECT que se conecten al servidor de la base de datos que vaya a actualizar. Asimismo, detenga cualquier otra aplicación que pueda conectarse a su instancia de Microsoft SQL Server.

2. Realice una copia de seguridad de todas las bases de datos relevantes con seguridad antes de proseguir.

3. Realice la actualización del servidor de bases 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.

- Otra alternativa consiste en seguir las instrucciones del proveedor de la base de datos: https://msdn.microsoft.com/en-us/library/bb677622.aspx.

- MS SQL Server en Linux no es compatible. Sin embargo, puede conectar el servidor de ESET PROTECT en Linux con el Servidor MS SQL en Windows.

Actualizar MySQL Server (Windows y Linux):

- Actualizar de MySQL 5.6 a la versión 5.7

- Actualizar de MySQL 5.7 a la versión 8

4. Inicie el servicio del Servidor ESET PROTECT y controle el rastreo de los registros para verificar que la conexión de la base de datos funcione correctamente.

Actualización de ESMC/ESET PROTECT instalada en clúster de conmutación por error en Windows

Si tiene el servidor de ESMC/ESET PROTECT 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 el rol del clúster de Servidor ESMC/ESET PROTECT en el administrador de clústeres. Asegúrese de que el servicio (**ESET Security Management Center Server** o **ESET PROTECT Server**) se detenga en todos los nodos de clústeres.

2. Obtenga el disco compartido del clúster en línea en el nodo 1 y actualice el componente del servidor manualmente mediante la ejecución del instalador *.msi* más reciente como en el caso de una instalación de componentes.

3. Después de finalizar la instalación (actualización), asegúrese de que el servicio **ESET PROTECT Server** se ha detenido.

4. Obtenga el disco compartido del clúster en línea en el nodo 2 y actualice el componente del servidor de la misma manera que en el paso 2.

5. Después de actualizar el Servidor ESET PROTECT en todos los nodos de clústeres, inicie el **rol de Servidor ESET PROTECT** en el administrador de clústeres.

6. Actualice el Agente ESET Management manualmente mediante la ejecución del último instalador *.msi* en todos los nodos de clústeres.

7. En la Consola web ESET PROTECT verifique si las versiones del Agente y el Servidor de todos los nodos informan la última versión a la cual ha actualizado.

Actualizar Apache HTTP Proxy

Proxy Apache HTTP es un servicio que puede usarse junto con ESET PROTECT para distribuir las actualizaciones a equipos cliente y paquetes de instalación para los Agentes ESET Management.

Si anteriormente instaló el Proxy Apache HTTP en Windows y desea actualizarlo a la versión más reciente, tiene dos maneras de realizar la actualización, ya sea manualmente o mediante el instalador todo en uno.

Actualizar Apache HTTP Proxy con el instalador todo en uno (Windows)

Si descargó el instalador de ESET PROTECT todo en uno más reciente, puede usar este método para actualizar rápidamente Apache HTTP Proxy a la versión más reciente. Si no tiene descargado el instalador más reciente, use el método de actualización manual de Apache HTTP Proxy.

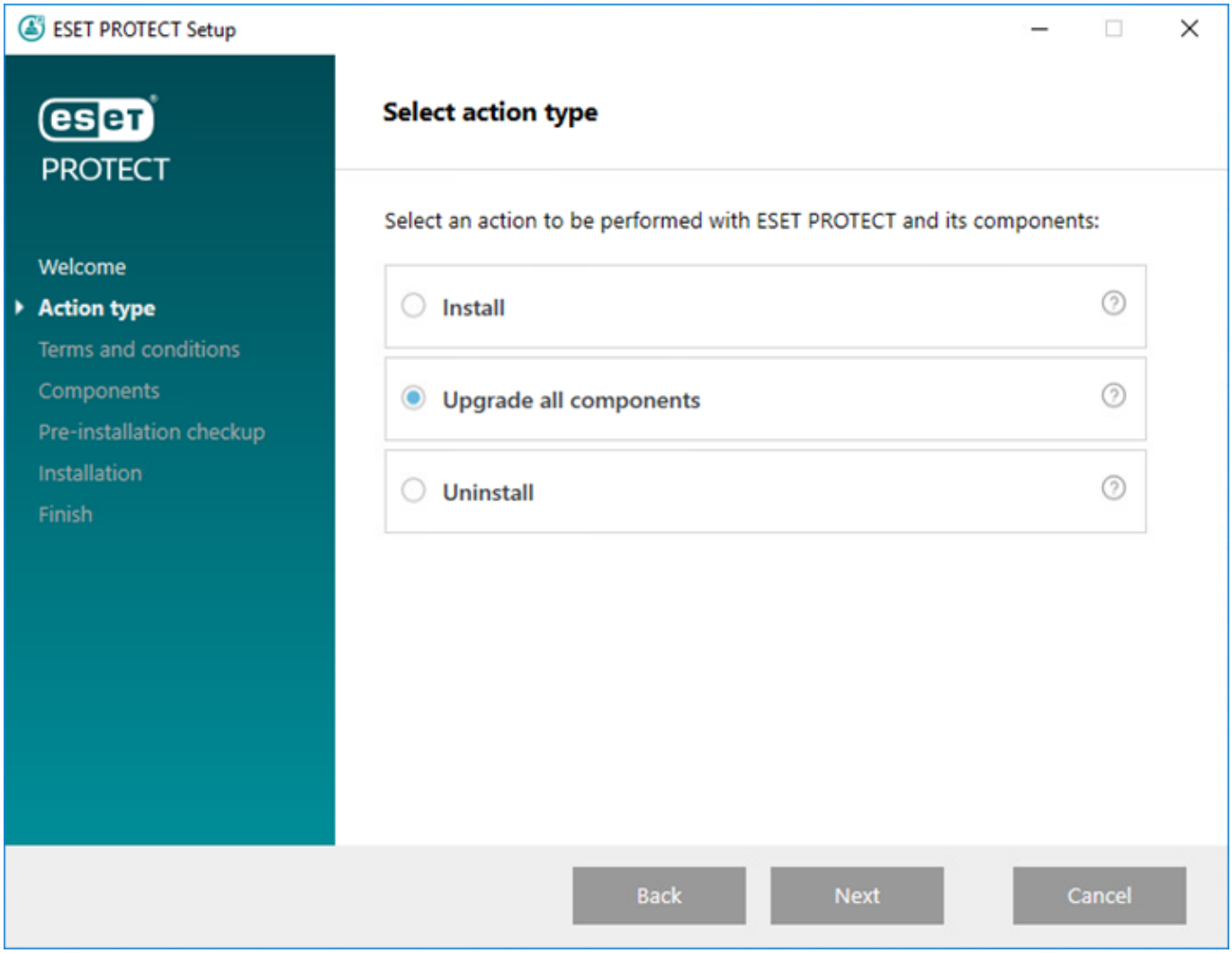
1. Realice copias de seguridad de los siguientes archivos:

   - *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. Ejecute el instalador todo en uno con un doble clic en el archivo *setup.exe* y en la pantalla de Bienvenida,

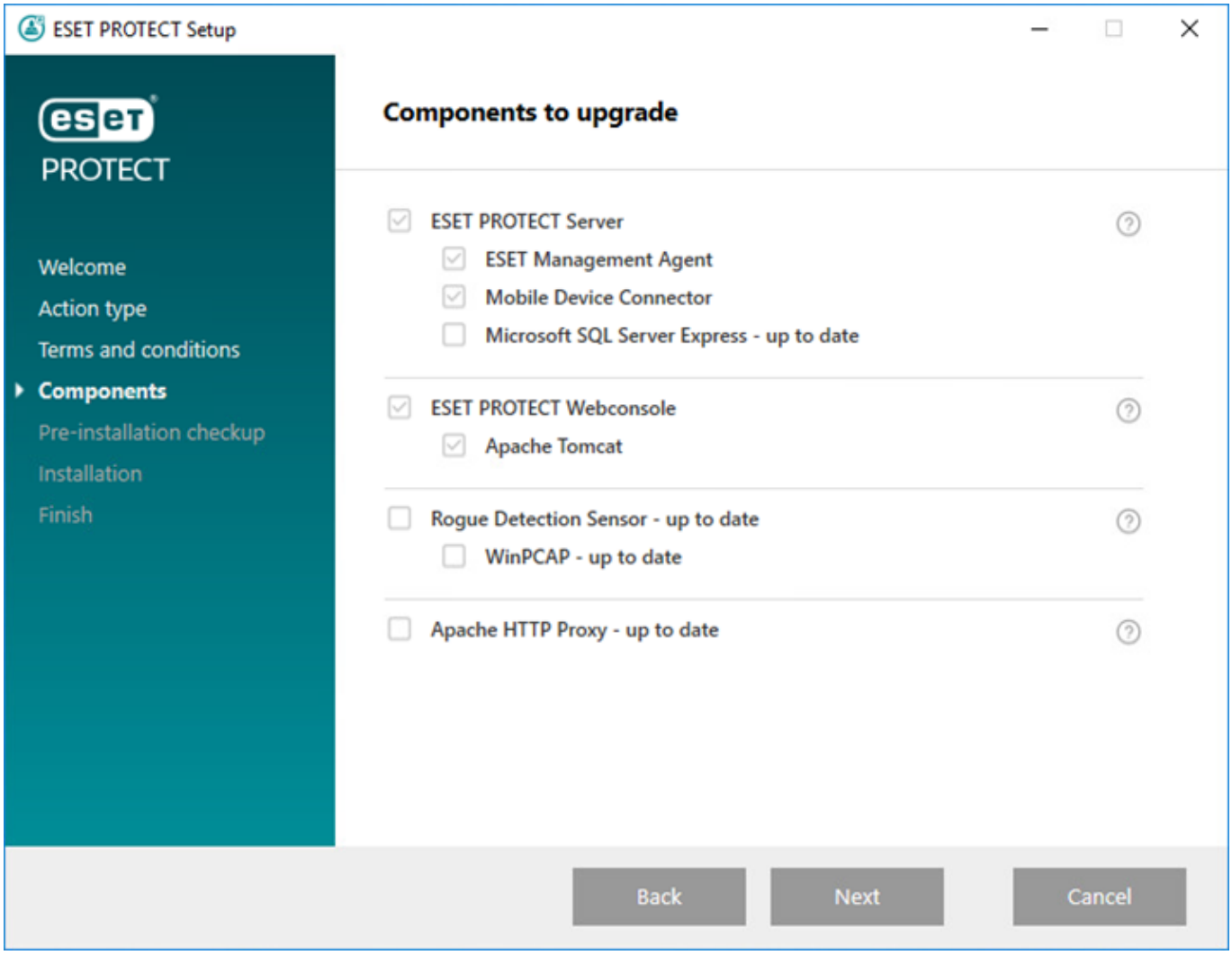
haga clic en **Siguiente**.

3. Seleccione **Actualizar todos los componentes** y haga clic en **Siguiente**.



4. Lea el **Acuerdo de licencia de usuario final**, acéptelo y haga clic en **Siguiente**.

5. En **Componentes**, revise los componentes de ESET PROTECT que pueden actualizarse y haga clic en **Siguiente**.



6. Siga la **Revisión previa a la instalación** para asegurarse de que su sistema cumpla con todos los requisitos previos.

7. Haga clic en **Actualizar** para iniciar la actualización de ESET PROTECT. La instalación puede llevar algo de tiempo, en función de su sistema y la configuración de la red.

8. Cuando la actualización esté completa, 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 usarla.

9. Pruebe la conexión a Apache HTTP Proxy accediendo a la siguiente URL en su navegador:

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

Solución de problemas

Para resolver un problema, consulte los archivos de registro de Apache HTTP Proxy.

Si se realizó una configuración personalizada en el archivo *httpd.conf* en la instalación anterior de Apache HTTP Proxy, siga estos pasos:

1. Detenga el servicio **ApacheHttpProxy** y, para ello, abra un símbolo del sistema administrativo y ejecute el

siguiente comando:

```
sc stop ApacheHttpProxy
```

2.Si utiliza un nombre de usuario y contraseña para acceder al proxy Apache HTTP (tema de instalación del proxy Apache HTTP), reemplace el siguiente bloque de código:

```
<Proxy *>
 Deny from all
</Proxy>
```

con el siguiente bloque de código (se encontró 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 realizó otras personalizaciones al archivo *httpd.conf* en lugar de su instalación anterior de Apache HTTP Proxy, copie manualmente esas modificaciones desde *httpd.conf.old* (o desde la copia de seguridad de *httpd.conf* del paso 1) al archivo *httpd.conf* nuevo (actualizado).

4.Guarde los cambios e inicie el servicio de **ApacheHttpProxy** mediante la ejecución del siguiente comando en un símbolo del sistema elevado:

```
sc start ApacheHttpProxy
```

Actualizar Apache HTTP Proxy manualmente (Windows)

Para actualizar el Apache HTTP Proxy a la versión más reciente, siga los pasos a continuación.

1. Realice copias 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** y, para ello, abra un símbolo del sistema administrativo y ejecute el siguiente comando:

```
sc stop ApacheHttpProxy
```

3. Descargue el archivo instalador del Apache HTTP Proxy desde el sitio de descarga de ESET y extraiga su contenido a *C:\Program Files\Apache HTTP Proxy 2.[x.xx]*\. Durante la extracción se sobrescribe los archivos

existentes.

4. Vaya a *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf*, haga clic con el botón derecho *httpd.conf*, desde el menú contextual y seleccione **Abrir con** > **Bloc de notas**.

5. Agregue el siguiente código en la parte inferior 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 y contraseña para acceder al proxy Apache HTTP (tema de instalación del proxy Apache HTTP), reemplace el siguiente bloque de código:

```
<Proxy *>
 Deny from all
</Proxy>
```

con este (que encontrará en el archivo *httpd.conf* de copia de seguridad al que le hizo copia de seguridad 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 realizaron otras personalizaciones al archivo *httpd.conf* en la instalación anterior de Apache HTTP Proxy, copie esas modificaciones desde la copia de seguridad del archivo *httpd.conf* en el archivo *httpd.conf* nuevo (actualizado).

7. Guarde los cambios e inicie el servicio de **ApacheHttpProxy** mediante la ejecución del siguiente comando en un símbolo del sistema administrativo:

```
sc start ApacheHttpProxy
```

8. Actualice la versión en la descripción del servicio.

```
sc description ApacheHttpProxy "Apache/2.4.43"
```

9. Pruebe la conexión al Proxy Apache HTTP accediendo a la siguiente URL en su navegador:

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

Si necesita resolver un problema, consulte los archivos de registro del Proxy Apache HTTP.

Actualizar Apache Tomcat

Apache Tomcat es un componente obligatorio necesario para ejecutar la consola web de ESET PROTECT.

Si está actualizando a la versión más reciente de ESET PROTECT, o si no ha actualizado Apache Tomcat durante un período prolongado de tiempo, debería considerar actualizar Apache Tomcat a la última versión. Si mantiene actualizados los servicios públicos, incluso Apache Tomcat y sus dependencias, reducirá los riesgos de seguridad del 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 existente de Apache Tomcat se realizó a través del instalador todo en uno.
- Instrucciones de Windows (instalación manual) – Actualice Apache Tomcat manualmente si realizó la instalación existente de Apache Tomcat manualmente o no tiene el instalador todo en uno más reciente de ESET PROTECT.
- Instrucciones de Linux

Actualizar Apache Tomcat con el instalador todo en uno (Windows)

Apache Tomcat es un componente obligatorio necesario para ejecutar la consola web de ESET PROTECT. Utilice este método para actualizar Apache Tomcat con el instalador todo en uno de ESET PROTECT9.1más reciente. Esta es la opción de actualización recomendada si la instalación existente de Apache Tomcat se realizó a través del instalador todo en uno. O puede actualizar Apache Tomcat manualmente.

Antes de actualizar

Realice copias 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 está usando un certificado SSL personalizado almacenado en la carpeta *Tomcat*, haga una copia de seguridad del certificado también.

Limitaciones de actualización de la consola web y Apache Tomcat

- Si se instala una versión personalizada de Apache Tomcat (instalación manual del servicio Tomcat), la actualización posterior de la consola web de ESET PROTECT por medio del Instalador todo en uno o a través de la Tarea de actualización de componentes no será compatible.
- La actualización de Apache Tomcat eliminará la carpeta de *era* folder ubicada en *C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\webapps*. Si usa la carpeta de *era* para almacenar datos adicionales, asegúrese de hacer una copia de seguridad de los datos antes de realizar la actualización.
- Si *C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\webapps* contiene datos adicionales (diferentes a las carpetas de *era* y *ROOT*), la actualización de Apache Tomcat no tendrá lugar y solo se actualizará la consola web.
- La consola web y la actualización de Apache Tomcat limpian los archivos de ayuda sin conexión. Si utilizó la ayuda sin conexión con ESMC o una versión anterior de ESET PROTECT, vuelva a crearla para ESET PROTECT 9.1 luego de realizar la actualización para asegurarse de tener la versión más reciente de la ayuda sin conexión que coincida con su versión de ESET PROTECT.

Procedimiento de actualización

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

2. Si quiere instalar la versión más reciente de Apache Tomcat y el instalador todo en uno contiene una versión anterior 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 vaya a la carpeta *installers*.

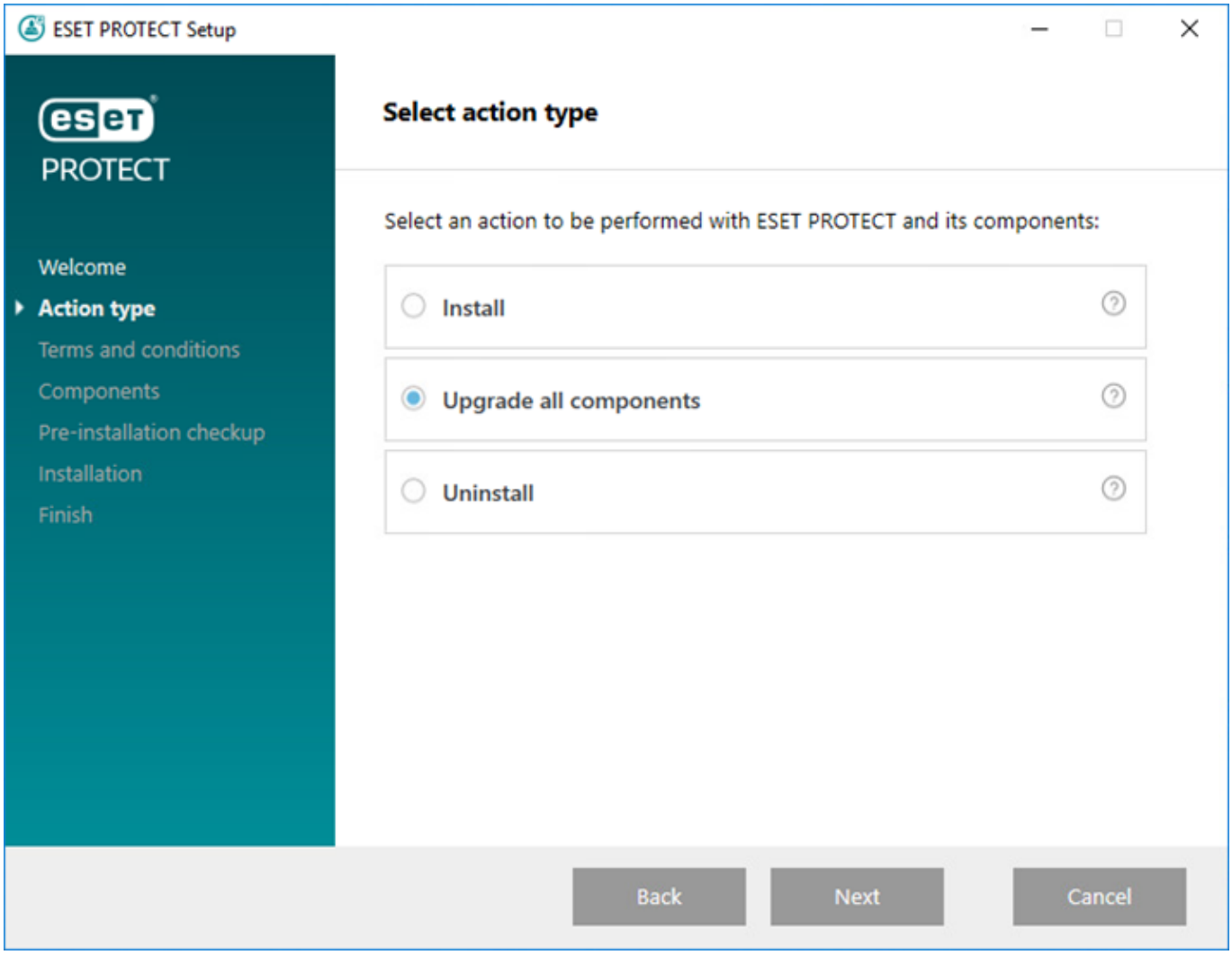
   b. Quite el archivo *apache-tomcat-9.0.x-windows-x64.zip* ubicado en la carpeta *installers*.

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

   d. Mueva el paquete con el archivo comprimido descargado a la carpeta *installers*.

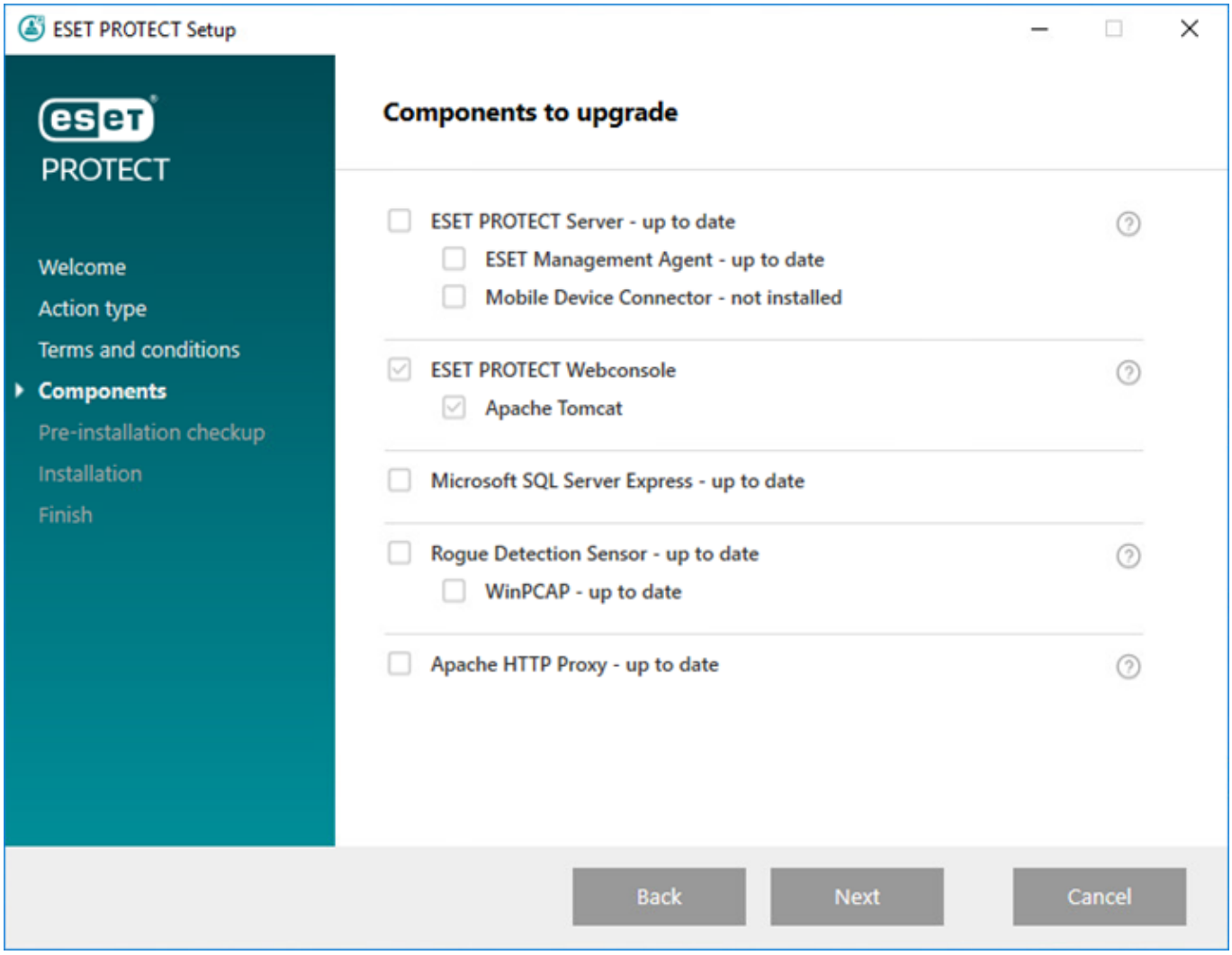
3. Para ejecutar el instalador todo en uno, haga doble clic en el archivo *Setup.exe* y, luego, en **Siguiente** en la pantalla de **Bienvenida**.

5. Seleccione **Actualizar todos los componentes** y haga clic en **Siguiente**.



6. Luego de aceptar el EULA, haga clic en **Siguiente**.

7. El instalador todo en uno detecta automáticamente si hay una actualización 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 equipo. Apache Tomcat requiere Java/OpenJDK de 64 bits. Si tiene muchas versiones de Java instaladas en su sistema, le recomendamos desinstalar las versiones anteriores de Java y solo dejar la última versión 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 pasar a una alternativa sin costo. Consulte las versiones compatibles de JDK.

9. Haga clic en **Actualizar** para completar la actualización y luego, en **Finalizar**.

10. Si instaló la consola web en un equipo diferente a donde está instalado el servidor de ESET PROTECT:

    a. Detenga el servicio de Apache Tomcat: Vaya a **Inicio** > **Servicios** > haga clic con el botón derecho en el servicio Apache Tomcat y seleccione **Detener**.

    b. Restaure el archivo *EraWebServerConfig.properties* (del paso 1) a su ubicación original.

    c. Inicie el servicioApache Tomcat. Vaya a **Inicio** > **Servicios** > haga clic con el botón derecho en el servicio Apache Tomcat y seleccione **Iniciar**.

11. Conéctese a la consola web de ESET PROTECT y asegúrese de que funcione correctamente.

ℹ Consulte también la Configuración adicional de la consola web para soluciones empresariales o sistemas de bajo rendimiento.

Solución de problemas

Si falla la actualización aApache Tomcat, instale su versión anterior y aplique la configuración del paso 1.

Actualizar Apache Tomcat manualmente (Windows)

Apache Tomcat es un componente obligatorio necesario para ejecutar la consola web de ESET PROTECT. Actualice Apache Tomcat manualmente si realizó la instalación existente de Apache Tomcat manualmente o no tiene el instalador todo en uno más reciente de ESET PROTECT.

Si se instala una versión personalizada de Apache Tomcat (instalación manual del servicio Tomcat), la actualización posterior de la consola web de ESET PROTECT por medio del Instalador todo en uno o a través de la Tarea de actualización de componentes no será compatible.

Antes de actualizar

- Apache Tomcat requiere Java/OpenJDK de 64 bits. Si tiene muchas versiones de Java instaladas en su sistema, le recomendamos desinstalar las versiones anteriores de Java y solo dejar la última versión 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 pasar a una alternativa sin costo. Consulte las versiones compatibles de JDK.

- Verifique la versión de Apache Tomcat que actualmente está en uso.

  a.Vaya a la carpeta de instalación Apache Tomcat:
  C:\Program Files\Apache Software Foundation\[Tomcat carpeta]

  b.Abra el archivo RELEASE-NOTES en un editor de texto y verifique el número de versión (por ejemplo 9.0.34).

  c.Si hay una versión compatible más reciente disponible, realice una actualización.

Procedimiento de actualización

1. Detenga el servicio de Apache Tomcat: Vaya a **Inicio** > **Servicios** > haga clic con el botón derecho en el servicio Apache Tomcat y seleccione **Detener**.

Cierre *Tomcat7w.exe* si se está ejecutando en la bandeja de su sistema.

2. Realice copias 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 está usando un certificado SSL personalizado almacenado en la carpeta *Tomcat*, haga una copia de seguridad del certificado también.

3. Desinstale la versión actual de Apache Tomcat.

4. Elimine la siguiente carpeta si todavía está presente en su sistema:

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

5. Descargue la última versión compatible del archivo instalador Apache Tomcat (32-bit/64-bit Windows Service Installer) `apache-tomcat-[versión].exe` de https://tomcat.apache.org.

6. Instale la última versión de Apache Tomcat que descargó:

- Si tiene instaladas más versiones de Java, seleccione la ruta de acceso a la versión más reciente de Java durante la instalación.

- Una vez que se complete la instalación, anule la selección de la casilla de verificación situada junto a **Ejecutar Apache Tomcat**.

7. Restaure *.keystore*, *server.xml* y los certificados personalizados a su ubicación original.

8. Abra el archivo *server.xml* y asegúrese de que la ruta *keystoreFile* sea correcta (actualice la ruta si cambió a una versión superior de Apache Tomcat):

keystoreFile="C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\.keystore"

9. Asegúrese de que se configure correctamente la conexión HTTPS para Apache Tomcat para la consola web de ESET PROTECT.

10. Implemente la consola web de ESET PROTECT (Instalación de la consola web: Windows).

11. Restaure *EraWebServerConfig.properties* a su ubicación original.

12. Ejecute Apache Tomcat y configure una máquina virtual de Java:

a.Vaya a la carpeta *C:\Program Files\Apache Software Foundation\[Tomcat carpeta]\bin* y ejecute *Tomcat9w.exe*.

b.En la pestaña **General**, configure el **Tipo de inicio** en **Automático** y presione **Iniciar**.

c.Haga clic en la pestaña **Java**, quite la selección de **Usar predeterminado** y asegúrese de que **Java Virtual Machine** incluya la ruta al archivo *jvm.dll* (consulte las instrucciones ilustradas de la base de conocimiento) y haga clic en **Aceptar**.

13. Conéctese a la consola web de ESET PROTECT y asegúrese de que funcione correctamente.

Consulte también la Configuración adicional de la consola web para soluciones empresariales o sistemas de bajo rendimiento.

Solución de problemas

- Si no puede configurar una conexión HTTPS para Apache Tomcat, puede omitir este paso y usar una conexión HTTP de manera temporal.

- Si falla la actualización aApache Tomcat, instale su versión original y aplique la configuración del paso 2.

- La consola web y la actualización de Apache Tomcat limpian los archivos de ayuda sin conexión. Si utilizó la ayuda sin conexión con ESMC o una versión anterior de ESET PROTECT, vuelva a crearla para ESET PROTECT 9.1 luego de realizar la actualización para asegurarse de tener la versión más reciente de la ayuda sin conexión que coincida con su versión de ESET PROTECT.

Actualizar Apache Tomcat (Linux)

Apache Tomcat es un componente obligatorio necesario para ejecutar la consola web de ESET PROTECT.

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 nueva disponible:

   a.Asegúrese de que la versión más reciente sea compatible.

   b.Realice una copia de seguridad del archivo de configuración de Tomcat */etc/tomcat7/server.xml*.

Procedimiento 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. Actualizar Apache Tomcat y Java. Los nombres de paquetes de ejemplo que se muestran a continuación pueden diferir de sus paquetes del repositorio de distribución de 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. Reemplace el archivo */etc/tomcat9/server.xml* con el archivo *server.xml* de su copia de seguridad.

4. Abra el archivo *server.xml* y asegúrese de que la ruta *keystoreFile* sea correcta.

5. Asegúrese de que la conexión HTTPS para Apache Tomcat esté configurada correctamente.

Consulte también la Configuración adicional de la consola web para soluciones empresariales o sistemas de bajo rendimiento.

Después de actualizar Apache Tomcat a una versión principal posterior (por ejemplo, Apache Tomcat versión 7.x a 9.x):
1.Implemente la consola web de ESET PROTECT nuevamente (consulte la 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 la configuración personalizada en la consola web de ESET PROTECT.
La consola web y la actualización de Apache Tomcat limpian los archivos de ayuda sin conexión. Si utilizó la ayuda sin conexión con ESMC o una versión anterior de ESET PROTECT, vuelva a crearla para ESET PROTECT 9.1 luego de realizar la actualización para asegurarse de tener la versión más reciente de la ayuda sin conexión que coincida con su versión de ESET PROTECT.

Procedimientos de migración y reinstalación

Existen diferentes maneras de migrar y reinstalar el Servidor ESET PROTECT y otros componentes ESET PROTECT.

- Migre o vuelva a instalar ESET PROTECT 9 de un servidor a otro.

Para migrar de un Servidor ESET PROTECT a un nuevo equipo de servidor, debe exportar/realizar copias de seguridad de todas las autoridades de certificados y del Certificado del servidor ESET PROTECT. De lo contrario, ninguno de los componentes ESET PROTECT podrán comunicar con su nuevo Servidor ESET PROTECT.

- migración de la base de datos de ESET PROTECT
- Migración de MDM
- Cambiar una dirección IP o nombre de host en un servidor de ESET PROTECT.
- Migración desde ERA 5.x

Consulte los procedimientos de actualización.

Migración de un servidor a otro

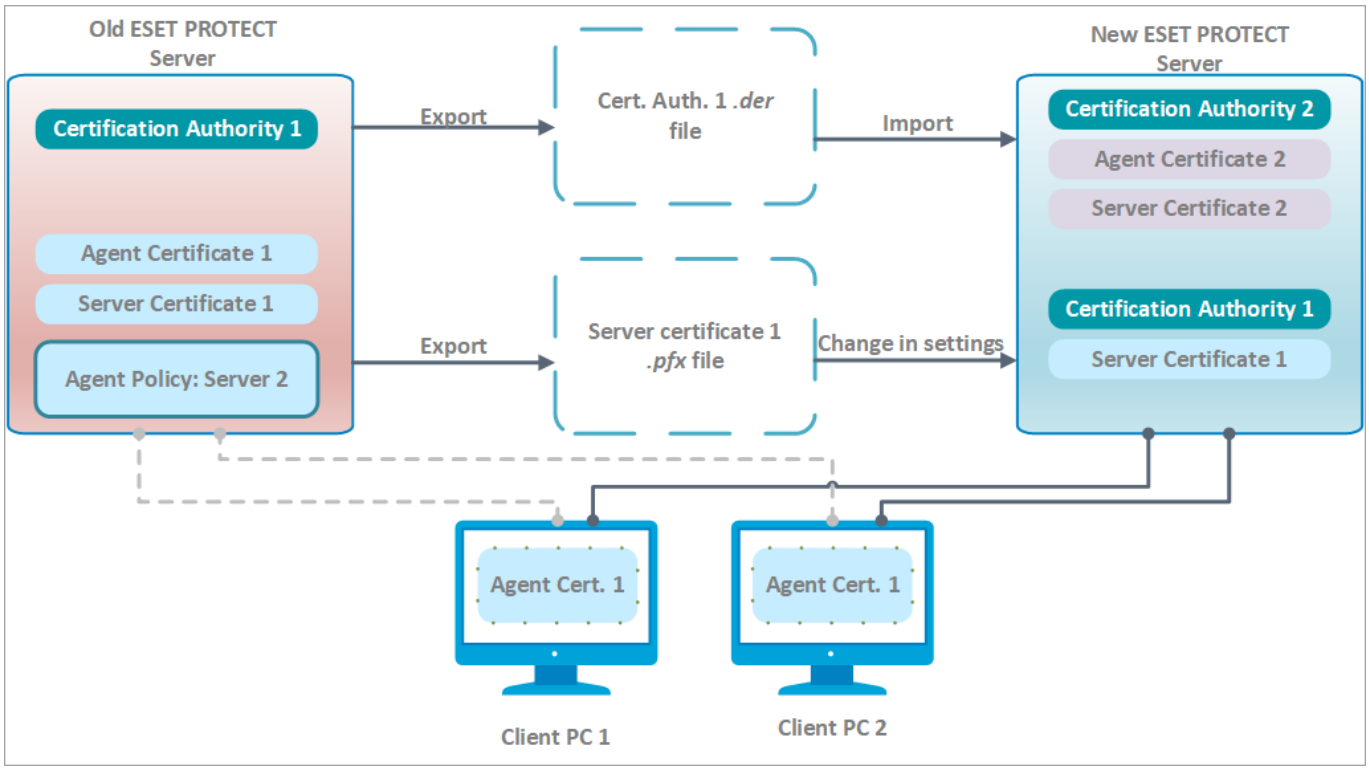
Existen varias maneras de migrar ESET PROTECT de un servidor a otro (estos escenarios se pueden usar al reinstalar su Servidor ESET PROTECT):

- Instalación limpia: misma dirección IP - La nueva instalación no usa la base de datos anterior del Servidor ESET PROTECT anterior y mantiene la dirección IP original.
- Instalación limpia: direcciónes IP diferente (artículo de base de conocimiento) - La instalación nueva no usa la base de datos previa del servidor de ESET PROTECT anterior y tiene otra dirección IP.
- Base de datos migrada: misma/distinta dirección IP: la migración de la base de datos se puede realizar entre dos tipos de bases de datos similares (desde MySQL hacia MySQL o desde MS SQL hacia MS SQL) y dos versiones similares de ESET PROTECT.

Instalación limpia: misma dirección IP

Este procedimiento tiene como objetivo instalar una instancia completamente nueva del Servidor ESET PROTECT que no usa la base de datos previa. El nuevo Servidor ESET PROTECT tendrá **la misma dirección IP**, que su servidor anterior, pero no usará la base de datos del Servidor ESET PROTECT anterior.

Las siguientes instrucciones requieren que se esté ejecutando su antiguo servidor de ESET PROTECT con una consola web accesible. Si no se puede acceder a su antiguo servidor de ESET PROTECT:
1. Instale el Servidor/MDM ESET PROTECT mediante el instalador de paquetes todo en uno (Windows) o elija otro método de instalación (instalación manual Windows, Linux o Aparato virtual).
2. Conéctese a la Consola web ESET PROTECT.
3. Agregue equipos cliente a la infraestructura de ESET PROTECT e implemente el agente ESET Management de forma local o remota.



Ver la imagen más grande

❑ **En su Servidor ESET PROTECT actual (anterior):**

Si administra dispositivos cifrados con ESET Full Disk Encryption, siga estos pasos para evitar perder los datos de recuperación.
1.Antes de la migración, diríjase a **Resumen del estado** > **Cifrado**. Aquí puede **Exportar** los **Datos de recuperación de ESET Full Disk Encryption** actuales.
2.Tras la migración: **importe** los **Datos de recuperación de ESET Full Disk Encryption** en su 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 la consola web de ESET PROTECT.

1. Exporte un certificado del Servidor ESET PROTECT actual y guárdelo en el almacenamiento externo.

• Exporte todos los Certificados de la autoridad de certificación de su Servidor ESET PROTECT y guarde cada certificado CA como un archivo *.der*.

• Exporte el Certificado del Servidor de su Servidor ESET PROTECT a un archivo *.pfx*. El *.pfx* exportado incluirá una clave privada también.

2. Detenga el servicio del Servidor ESET PROTECT.

3. Apague el equipo del Servidor ESET PROTECT.

No desinstale/quite su Servidor ESET PROTECT anterior.

❑ **En su Servidor ESET PROTECT nuevo:**

Para usar un nuevo Servidor ESET PROTECT con la misma dirección IP, asegúrese de que la configuración de red en el nuevo Servidor ESET PROTECT (**dirección IP, FQDN, nombre del equipo, registro DNS SRV**) coincida con el del Servidor ESET PROTECT anterior.

1. Instale el Servidor/MDM ESET PROTECT mediante el instalador de paquetes todo en uno (Windows) o elija otro método de instalación (instalación manual Windows, Linux o Aparato virtual).

2. Conéctese a la Consola web ESET PROTECT.

3. Importe todos los CAS que ha exportado desde su Servidor ESET PROTECT anterior. Para ello, siga las instrucciones para importar una clave pública.

4. Cambie el certificado de su Servidor ESET PROTECT en **Más** > Configuración para usar el certificado del servidor de su Servidor ESET PROTECT anterior.

5. Importe todas las licencias de ESET necesarias a ESET PROTECT.

6. Reinicie el servicio del Servidor ESET PROTECT, consulte nuestro artículo en la base de conocimiento para obtener más información.

Luego de uno o dos Intervalos de conexión del agente los equipos cliente se deben conectar a su nuevo servidor de ESET PROTECT con su certificado de Agente de ESET Management original, autenticado por el CA importado del servidor de ESET PROTECT anterior. Si los clientes no conectan, consulte Problemas después de la actualización/migración del Servidor ESET PROTECT .

Cuando agrega equipos de nuevos clientes, use una nueva autoridad de certificación para firmar los certificados de los agentes. Esto se hace porque el CA importado no se pueda usar para firmar nuevos certificados de pares, solo puede autenticar Agentes ESET Management de equipos de clientes migrados.

❑ **Desinstalación del Servidor/MDM ESET PROTECT anterior:**

Cuando tenga todo funcionando correctamente en el nuevo Servidor ESET PROTECT, desinstale con cuidado su Servidor/MDM ESET PROTECT anterior mediante las instrucciones paso a paso.

Base de datos migrada: misma/distinta dirección IP

El objetivo de este procedimiento es instalar una instancia completamente nueva del Servidor ESET PROTECT y **mantener su base de datos ESET PROTECT existente**, incluso los equipos cliente existentes. El nuevo Servidor ESET PROTECT tendrá la **misma dirección IP o una dirección IP distinta** y la base de datos del Servidor ESET PROTECT anterior se importará al equipo del nuevo servidor antes de la instalación.

- La migración de las bases de datos solo es compatible entre tipos de bases de datos idénticas (desde MySQL hacia MySQL o desde MS SQL hacia MS SQL).
- cuando migre una base de datos, debe migrar entre instancias de la misma versión de ESET PROTECT. Consulte nuestro artículo en la base de conocimiento para obtener instrucciones para determinar las versiones de los componentes ESET PROTECT. Después de finalizar la migración de la base de datos, podrá realizar una actualización, si fuera necesario, para obtener la última versión de ESET PROTECT.

❑ **En su Servidor ESET PROTECT actual (anterior):**

Recomendamos la migración a una dirección IP diferente solo para usuarios avanzados. Si su nuevo Servidor ESET PROTECT tiene **otra dirección IP**, siga estos pasos adicionales en su servidor actual (viejo) ESET PROTECT:
a)Genere un nuevo certificado del ServidorESET PROTECT con información de conexión para el nuevo Servidor ESET PROTECT. Deje el valor predeterminado (un asterisco) en el campo **Host** para permitir la distribución de este certificación sin asociación a un nombre de DNS específico o dirección IP.
b)Cree una política para definir una nueva dirección IP del Servidor ESET PROTECT y asígnela a todos los equipos. Espere que la política se distribuya a todos los equipos de los clientes (los equipos dejarán de enviar informes a medida que reciban la información del servidor nuevo).

1. Detenga el servicio del Servidor ESET PROTECT.
2. Exporte/Realice una copia de seguridad de la Base de datos ESET PROTECT.
3. Apague el equipo del Servidor ESET PROTECT actual (opcional si el nuevo servidor tiene otra dirección IP).

No desinstale/quite su Servidor ESET PROTECT anterior.

❑ **En su Servidor ESET PROTECT nuevo:**

Para usar un nuevo Servidor ESET PROTECT con la misma dirección IP, asegúrese de que la configuración de red en el nuevo Servidor ESET PROTECT (**dirección IP, FQDN, nombre del equipo, registro DNS SRV**) coincida con el del Servidor ESET PROTECT anterior.

1. Instale/Lance una base de datos ESET PROTECT compatible.
2. Importe/Restaure la base de datos ESET PROTECT desde su Servidor ESET PROTECT anterior.
3. Instale el Servidor/MDM ESET PROTECT mediante el instalador de paquetes todo en uno (Windows) o elija otro método de instalación (instalación manual Windows, Linux o Aparato virtual). Especifique la configuración de conexión de la base de datos durante la instalación del Servidor ESET PROTECT.
4. Conéctese a la Consola web ESET PROTECT.
5. Vaya a **Más** > **Configuración** > **Conexión**. Haga clic en **Cambiar certificado** > **Abrir lista de certificados**, seleccione el **Certificado del servidor** del antiguo Servidor ESET PROTECT y haga clic dos veces en **Aceptar**.
6. Reinicie el servicio del Servidor ESET PROTECT.
7. Inicie sesión en la Consola web ESET PROTECT y haga clic en **Ordenadores.**

Después de uno o dos Intervalos de conexión del agente, los equipos cliente deben conectarse a su nuevo servidor de ESET PROTECT mediante el certificado del agente de ESET Management original. Si los clientes no conectan, consulte Problemas después de la actualización/migración del Servidor ESET PROTECT .

❑ **Desinstalación del Servidor/MDM ESET PROTECT anterior:**

Cuando tenga todo funcionando correctamente en el nuevo Servidor ESET PROTECT, desinstale con cuidado su Servidor/MDM ESET PROTECT anterior mediante las instrucciones paso a paso.

migración de la base de datos de ESET PROTECT

Estas instrucciones se aplican a la migración de base de datos de ESET PROTECT entre instancias de SQL Server (también se aplica cuando se migra a una versión diferente de SQL Server o a un SQL Server alojado en un equipo diferente):

- Proceso de migración para el servidor MS SQL
- Proceso de migración para el servidor MySQL

Proceso de migración para el servidor MS SQL

Este proceso de migración es igual para **Microsoft SQL Server** y **Microsoft SQL Server Express**.

Para obtener más información, consulte el siguiente artículo de la base de conocimiento de Microsoft: https://msdn.microsoft.com/en-us/library/ms189624.aspx.

Requisitos previos

- Se deben instalar las instancias fuente y de destino del Servidor SQL. Es posible que se encuentren en diferentes equipos.
- La instancia de destino del Servidor SQL debe ser, al menos, de la misma versión que la instancia fuente. **¡No es posible restaurar a una versión anterior!**
- **SQL Server Management Studio** debe estar instalado. Si las instancias del Servidor SQL se encuentran en diferentes equipos, debe estar presente en ambos.

Migración con SQL Server Management Studio

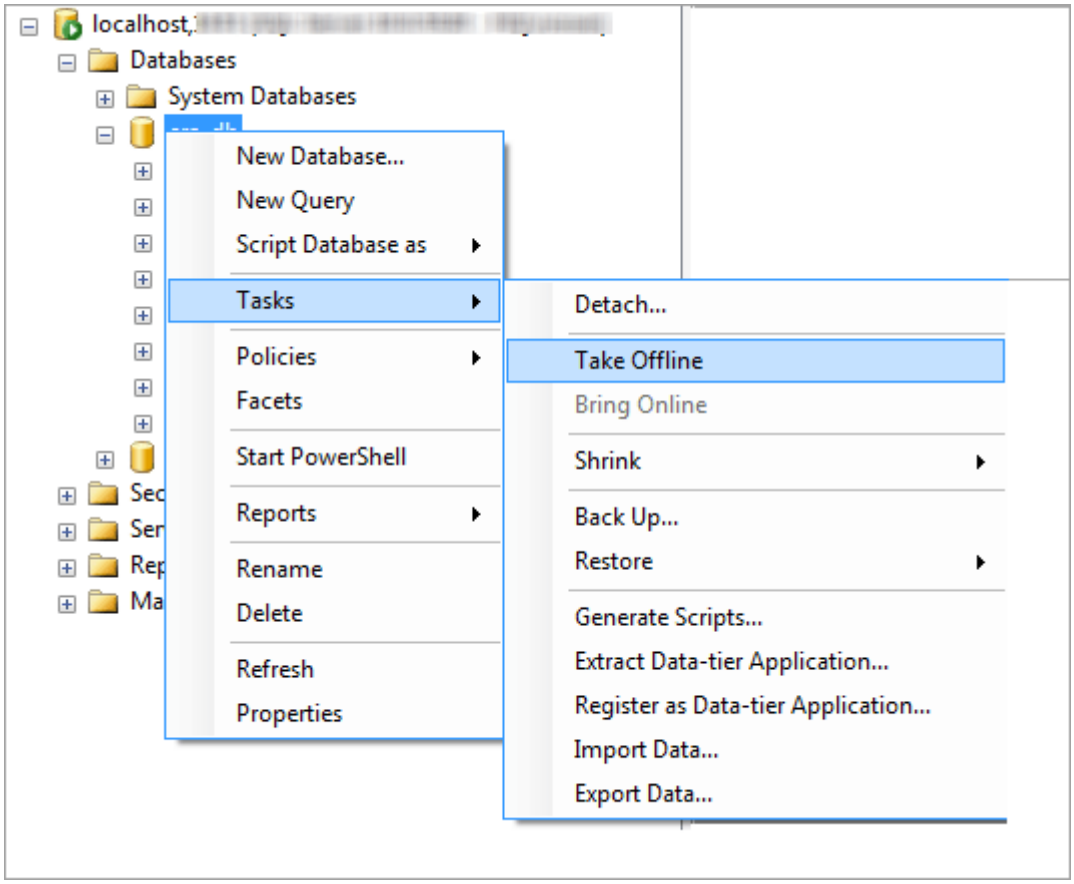
1. Detenga los servicios de servidor de ESET PROTECT (o el servicio de servidor de ESMC) o el servicio de MDM ESET PROTECT.

⚠ No inicie el servidor de ESET PROTECT ni MDM de ESET PROTECT antes de completar todos los pasos que se indican a continuación.

2. Ingrese a la instancia fuente del Servidor SQL mediante el SQL Server Management Studio.

3. Cree una copia de seguridad completa de base de datos de la base de datos a migrar. Recomendamos especificar un nuevo nombre para el conjunto de la copia de seguridad. De lo contrario, si ya se ha usado el conjunto de ala copia de seguridad, la nueva copia de seguridad se le anexará, lo que daría como resultado un archivo innecesariamente grande.

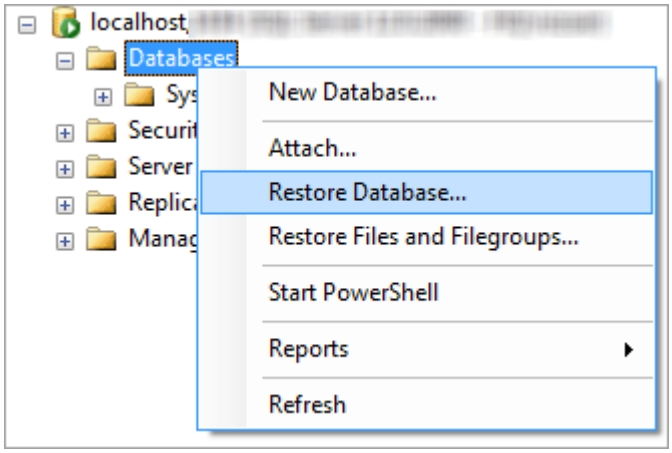
4. Desconecte la base de datos fuente, seleccione **Tareas** > **Desconectar**.



5. Copie el archivo de seguridad (*.bak*) que creó en el paso 3 a una ubicación que sea de fácil acceso desde la instancia del Servidor SQL. Es posible que necesite editar los derechos del acceso del archivo de copia de seguridad de la base de datos.

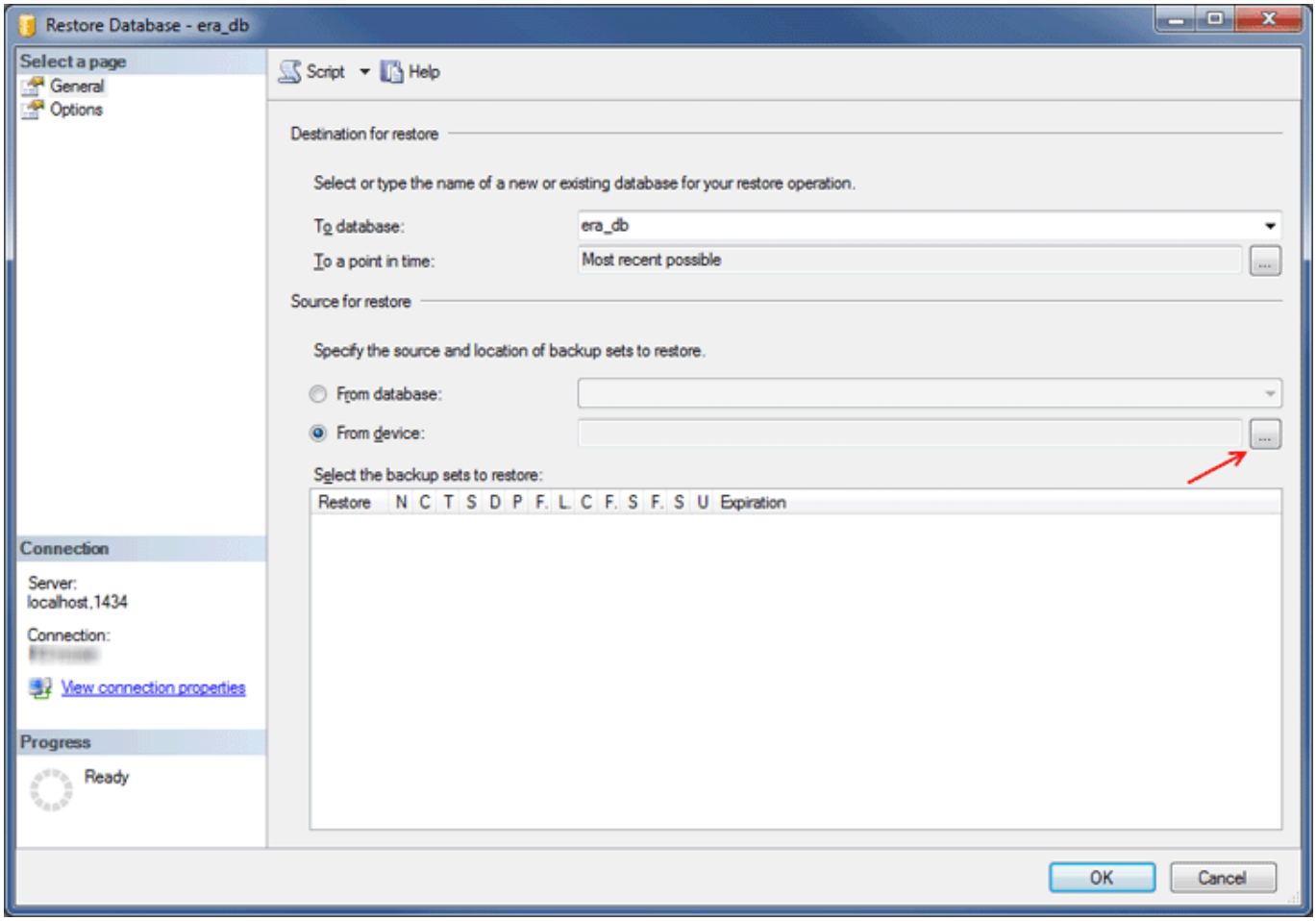
6. Ingrese a la instancia de destino del Servidor SQL mediante el SQL Server Management Studio.

7. Restaure su base de datos en la instancia del Servidor SQL de destino.



8. Ingrese un nombre para su nueva base de datos en el campo **A la base de datos**. Puede usar el mismo nombre de su base de datos anterior, si así lo prefiere.

9. Seleccione Desde dispositivo bajo **Especificar la fuente y ubicación de los conjuntos de copia de seguridad a restaurar** y luego haga clic en…

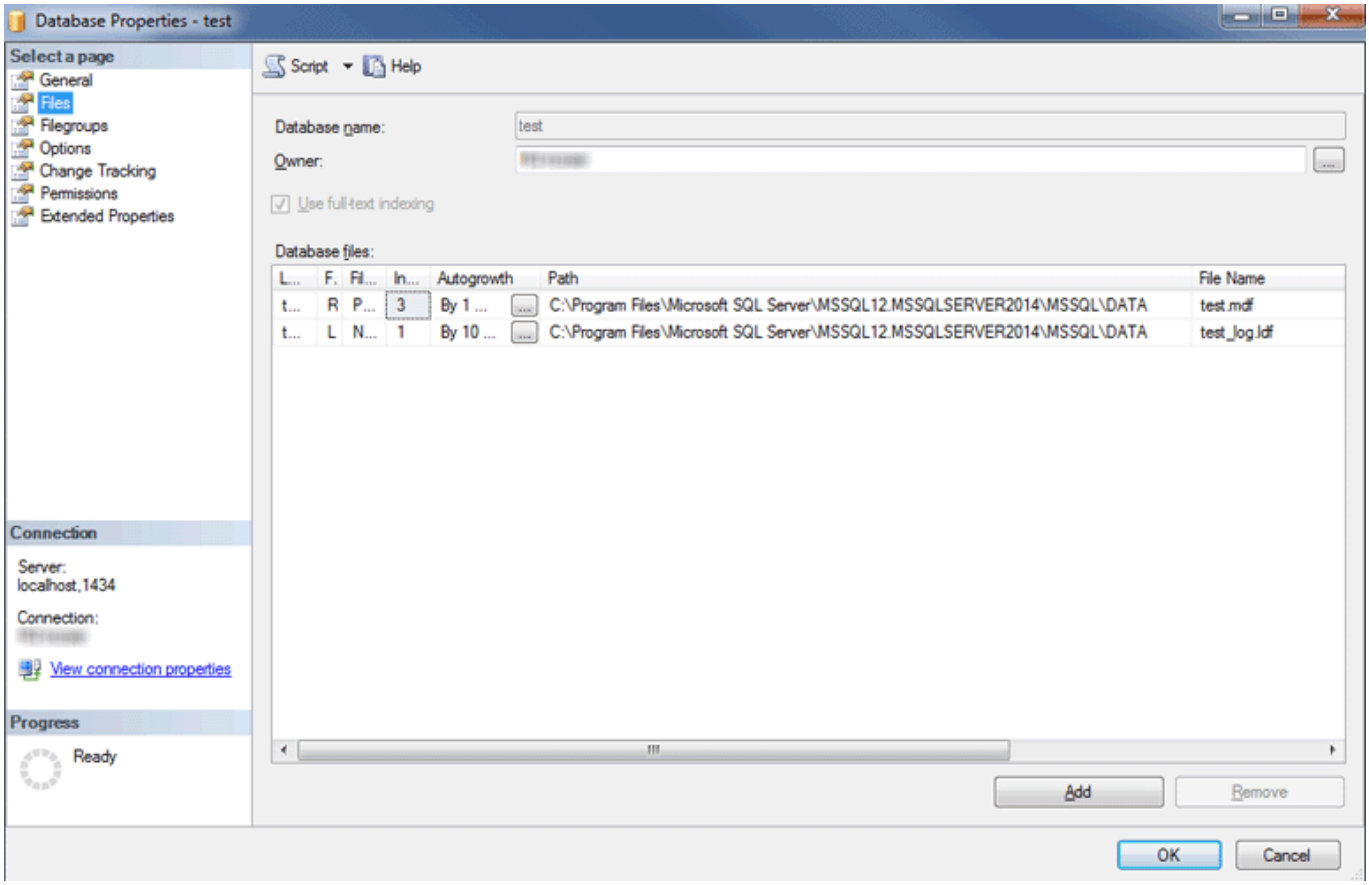


10. Haga clic en **Agregar, navegue hasta su archivo de copia de seguridad y ábralo**.

11. Seleccione la copia de seguridad más reciente posible para restaurar (el conjunto de copias de seguridad puede contener diferentes copias de seguridad).

12. Haga clic en la página **Opciones** del asistente de restauración. Opcionalmente, seleccione **Sobrescribir la base de datos existente** y asegúrese de que las ubicaciones de restauración de la base de datos (*.mdf*) y para el registro (*.ldf*) sean correctas. No modificar los valores predeterminados hará que se usen las rutas de su servidor SQL fuente, por lo que recomendamos verificar estos valores.

- Si no está seguro dónde se encuentran almacenados los archivos DB en la instancia del Servidor SQL de destino, haga clic en el botón secundario sobre una base de datos existente, seleccione **propiedades** y haga clic en la pestaña **Archivos**. El directorio donde se encuentra almacenada la base de datos se muestra en la columna **Ruta** de la tabla que se muestra a continuación.

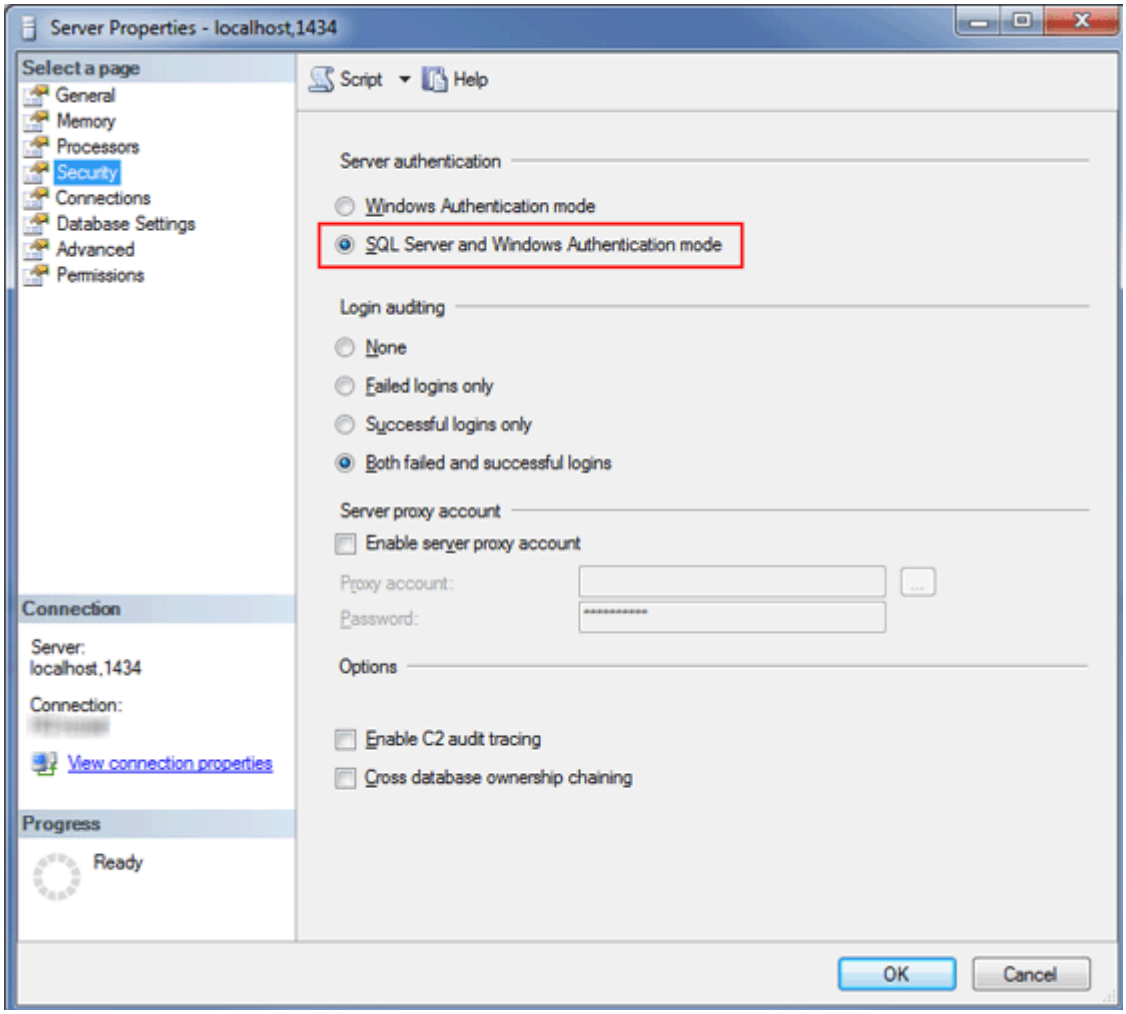


13. Haga clic en **Aceptar** en la ventana del asistente de restauración.

14. Haga clic con el botón derecho en la base de datos **era_db**, seleccione **Nueva consulta** y ejecute la siguiente consulta para eliminar los contenidos de la tabla **tbl_authentication_certificate** (de lo contrario, puede fallar la conexión de los agentes con el nuevo servidor):

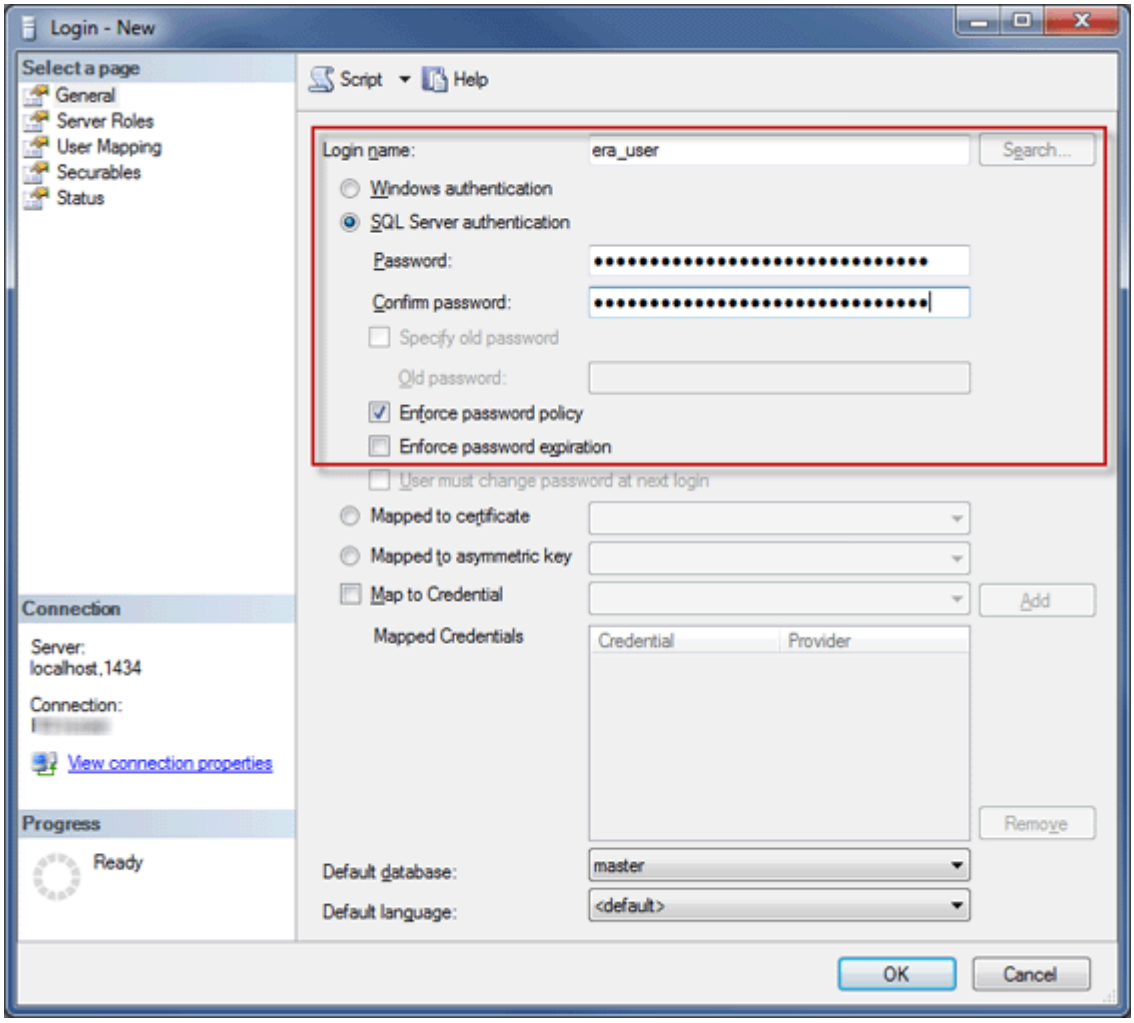
```
delete from era_db.dbo.tbl_authentication_certificate where certificate_id = 1;
```

15. Asegúrese de que el servidor de la nueva base de datos tenga **habilitada la Autenticación de Servidor SQL**. Haga clic con el botón secundario en el servidor y seleccione **Propiedades**. Navegue hasta **Seguridad** y verifique que el **Servidor SQL y el modo de Autenticación de Windows** se encuentren seleccionados.

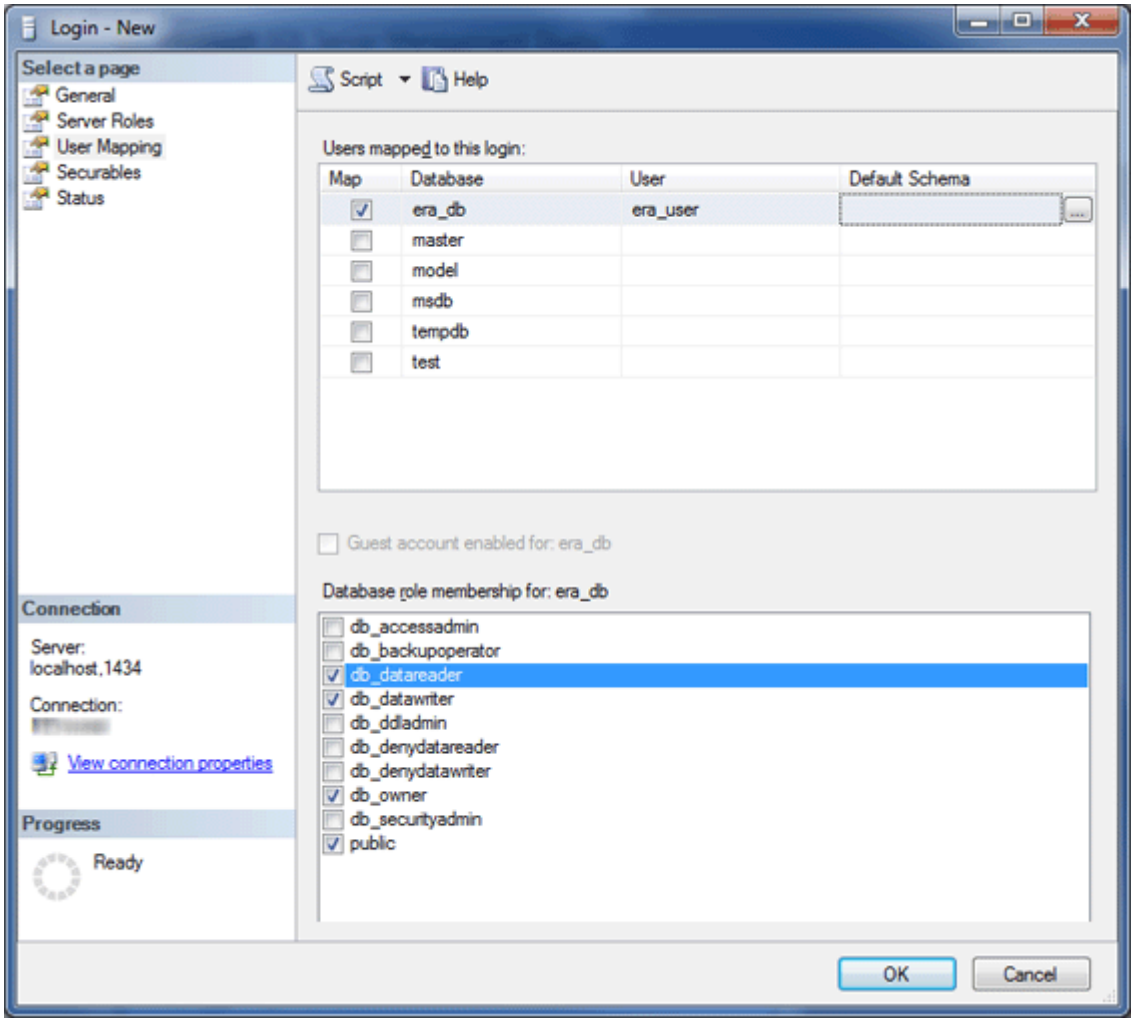


16. Cree un nuevo inicio de sesión del Servidor SQL (para Servidor de ESET PROTECT / MDM de ESET PROTECT) en el Servidor SQL de destino con **Autenticación de Servidor SQL** y vincule el inicio de sesión a un usuario en la base de datos restaurada.

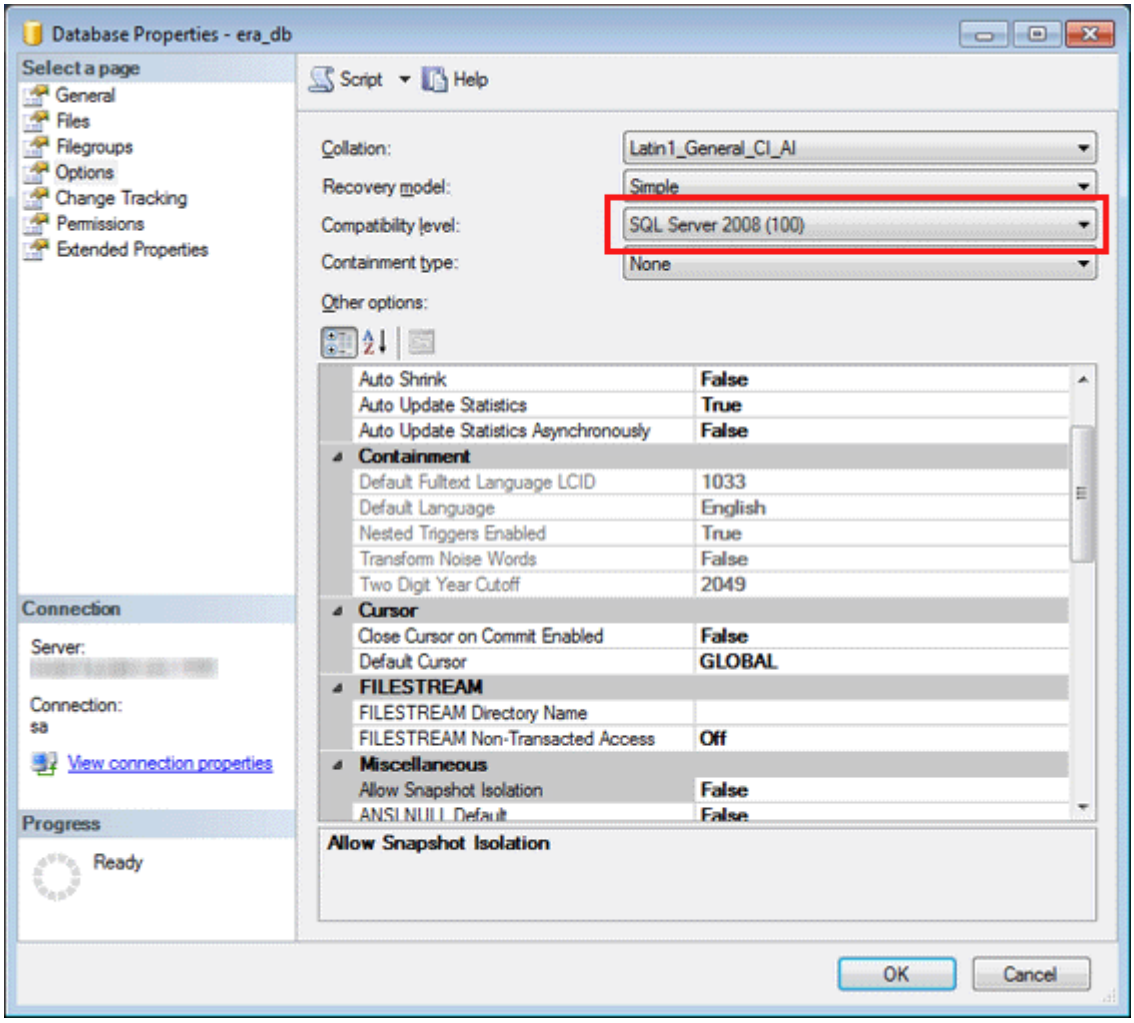
    - ¡No habilite el vencimiento de contraseña!
    - Caracteres recomendados para los nombres de usuario:
        - Letras ASCII minúsculas, números y guion bajo “_”
    - Caracteres recomendados para las contraseñas:
        - Solo caracteres ASCII, tanto en mayúscula como minúscula, números, espacios y caracteres especiales
    - No use caracteres que no sean ASCII, como llaves {} o @
    - Tenga en cuenta que si no sigue las recomendaciones de caracteres anteriores, puede tener problemas de conectividad de bases de datos o tendrá que evitar los caracteres especiales en los siguientes pasos durante la modificación de cadenas de conexión de la base de datos. No se incluyen en este documento las reglas de escape de caracteres.



17. Vincule el inicio de sesión a un usuario en la base de datos de destino. En la pestaña de **mapeos de usuario**, asegúrese de que el usuario de la base de datos tenga los siguientes roles: **db_datareader**, **db_datawriter**, **db_owner**.

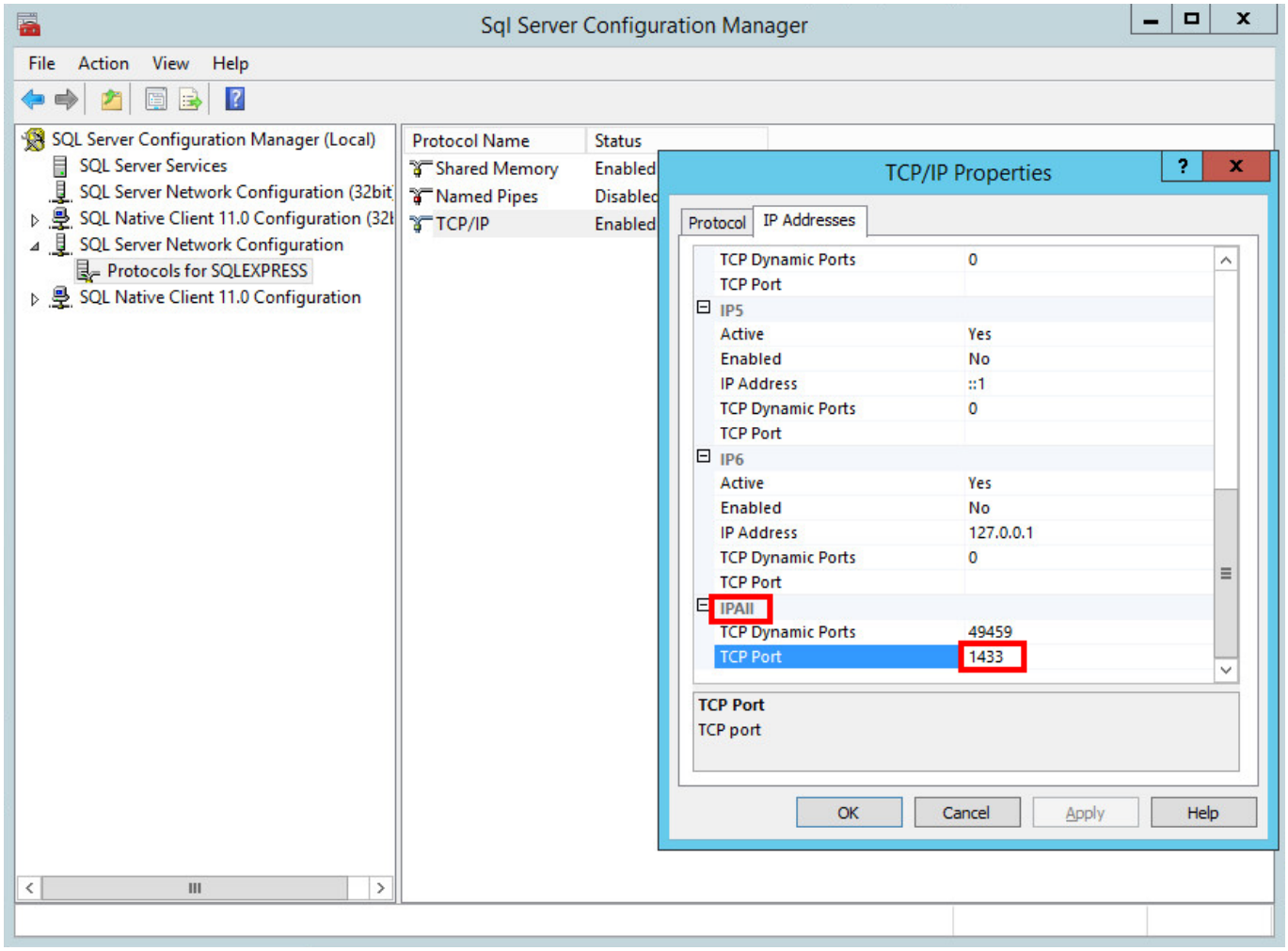


18. Para habilitar las características del servidor de la base de datos más recientes, cambie el **Nivel de compatibilidad** de la base de datos restaurada al más reciente. Haga clic con el botón secundario en la nueva base de datos y abra las **Propiedades** de la base de datos.



> SQL Server Management Studio no es capaz de definir niveles de compatibilidad superiores a la versión en uso. Por ejemplo, SQL Server Management Studio 2014 no puede establecer el nivel de compatibilidad para SQL Server 2019.

19. Asegúrese de que el protocolo de conexión **TCP/IP** esté **habilitado** para "db_instance_name» (ej., SQLEXPRESS o MSSQLSERVER) y el **puerto** TCP/IP **esté** configurado en 1433. Para ello, abra **Sql Server Configuration Manager**, navegue hasta **Configuración de la red del Servidor SQL** > **Protocolos para db_instance_name**, clic derecho **TCP/IP** y seleccione **Habilitado**. Haga doble clic en **TCP/IP**, cambie a la pestaña **Protocolos** desplácese hacia abajo hasta **IPAll** y en el campo **Puerto TCP** escriba 1433. Haga clic en **OK** y vuelva a iniciar el servicio del **Servidor SQL**.



20. Conecte el servidor de ESET PROTECT o MDM a la base de datos.

Proceso de migración para el servidor MySQL

Requisitos previos

• Se deben instalar las instancias fuente y de destino del Servidor SQL. Es posible que se encuentren en diferentes equipos.

• Las herramientas de MySQL deben estar disponibles en al menos uno de los equipos (`mysqldump` y el cliente mysql).

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 declaraciones SQL a continuación, siempre reemplace:
- **SRCHOST** con la dirección del servidor de base de datos fuente
- **SRCROOTLOGIN** con el inicio de sesión del usuario raíz del servidor MySQL fuente
- **SRCDBNAME** con el nombre de la base de datos ESET PROTECT fuente de la cual se debe hacer una copia de seguridad
- **BACKUPFILE** con la ruta al archivo donde se almacenará la copia de seguridad
- **TARGETROOTLOGIN** con el inicio de sesión del usuario raíz del servidor MySQL de destino
- **TARGETHOST** con la dirección del servidor de base de datos de destino
- **TARGETDBNAME** con el nombre de la base de datos ESET PROTECT de destino (luego de la migración)
- **TARGETLOGIN** con el nombre de inicio de sesión para el usuario de la nueva base de datos ESET PROTECT en el servidor de base de datos de destino
- **TARGETPASSWD** con la contraseña para el usuario de la nueva base de datos ESET PROTECT en el servidor de base de datos de destino

No es necesario ejecutar las siguientes instrucciones SQL a través de la línea de comando. Si existe una herramienta GUI disponible, puede usar una aplicación que conozca.

1. Detenga los servicios del Servidor/MDM de ESET PROTECT.

2. Genere una copia de seguridad completa de la base de datos ESET PROTECT fuente (la base de datos que planea migrar):

```
mysqldump --host SRCHOST --disable-keys --extended-insert --routines -
u SRCROOTLOGIN -p SRCDBNAME > BACKUPFILE
```

3. Prepare 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 caracter de apóstrofo ' en lugar de las comillas ".

4. Restaure la base de datos en el servidor MySQL de destino en la base de datos vacía preparada anteriormente:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p TARGETDBNAME < BACKUPFILE
```

5. Genere un usuario de base de datos 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 minúsculas, números y guion bajo “_”

Caracteres recomendados para **TARGETPASSWD:**

- Solo caracteres ASCII, tanto en mayúscula como minúscula, números, espacios y caracteres especiales
- No use caracteres que no sean ASCII, como llaves {} o @

Tenga en cuenta que si no sigue las recomendaciones de caracteres anteriores, puede tener problemas de conectividad de bases de datos o tendrá que evitar los caracteres especiales en los siguientes pasos durante la modificación de cadenas de conexión de la base de datos. No se incluyen en este documento las reglas de escape de caracteres.

6. Provea los derechos de acceso adecuados para el usuario de la base de datos 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 caracter de apóstrofo ' en lugar de las comillas ".

7. Elimine los contenidos de la tabla **tbl_authentication_certificate** (de lo contrario, puede fallar la conexión de los agentes con el nuevo servidor):

```
 mysql --host TARGETHOST -u root -p "--
execute=DELETE FROM era_db.tbl_authentication_certificate where certificate_id = 1;"
```

8. Conecte el servidor de ESET PROTECT o MDM a la base de datos.

Conexión del servidor de ESET PROTECT o MDM a una base de datos

Siga los pasos a continuación en el equipo donde está instalado el servidor de ESET PROTECT o MDM de ESET PROTECT para conectarlo a base de datos.

1. Detenga el servicio del Servidor/MDM de ESET PROTECT.
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 el Servidor/MDM de ESET PROTECT *startupconfiguration.ini*

   - Establezca la dirección y el puerto del servidor de la nueva base de datos.
   - Ingrese el nuevo nombre de usuario y contraseña ESET PROTECT en la cadena de conexión.

El resultado final debería verse así:

- 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 de arriba, reemplace siempre:
> - **TARGETHOST** con la dirección del servidor de base de datos de destino
> - **TARGETDBNAME** con el nombre de la base de datos ESET PROTECT de destino (luego de la migración)
> - **TARGETLOGIN** con el nombre de inicio de sesión para el usuario de la nueva base de datos ESET PROTECT en el servidor de base de datos de destino
> - **TARGETPASSWD** con la contraseña para el usuario de la nueva base de datos ESET PROTECT en el servidor de base de datos de destino

4. Inicie el Servidor de ESET PROTECT o MDM de ESET PROTECT y verifique que el servicio del Servidor se ejecute correctamente.

Migración de MDM

Este procedimiento es migrar su instancia existente de MDM ESET PROTECT y **mantener su base de datos de MDM ESET PROTECT existente**, incluidos los dispositivos móviles registrados. El MDM ESET PROTECT migrado tendrá **los mismos dirección IP/nombre de host** que el antiguo MDM ESET PROTECT, y la base de datos del antiguo MDM ESET PROTECT se importará al nuevo host de MDM antes de la instalación.

- La migración de las bases de datos solo es compatible entre tipos de bases de datos idénticas (desde MySQL hacia MySQL o desde MS SQL hacia MS SQL).
- cuando migre una base de datos, debe migrar entre instancias de la misma versión de ESET PROTECT. Consulte nuestro artículo en la base de conocimiento para obtener instrucciones para determinar las versiones de los componentes ESET PROTECT. Después de finalizar la migración de la base de datos, podrá realizar una actualización, si fuera necesario, para obtener la última versión de ESET PROTECT.

❑ **En su servidor actual (antiguo) de MDM ESET PROTECT:**

1. Cree una copia de seguridad de la configuración de MDM.

   a)En **Equipos**, haga clic en el servidor MDM y seleccione **Detalles**.

   b)Haga clic en **Configuración** > **Solicitar configuración**. Es posible que deba esperar algo de tiempo (según el 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 exacto de host de su Servidor de MDM.
   - Certificados de pares: el archivo *.pfx* exportado incluirá la clave privada.

   Si está ejecutando el servidor 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 al **Certificado HTTPS**.
   II.Haga clic en **Descargar** y descargue el certificado HTTPS en formato PFX.

   e)Exporte los siguientes certificados y tokens si están presentes:

   - El certificado de firma del perfil de inscripción.
   - Un certificado de APNS (exporte tanto el certificado de APNS como la Clave privada APNS).
   - Token de autorización del Programa de inscripción de dispositivo (DEP) de Apple

2. Detenga el servicio de MDM ESET PROTECT.

3. Exporte/haga copias de respaldo de la base de datos de MDM de ESET PROTECT.

4. Apague el equipo del MDM de ESET PROTECT actual.

No desinstale/quite su MDM ESET PROTECT anterior todavía.

❑ **En su servidor de MDM nuevo de ESET PROTECT:**

Asegúrese de que la configuración de red en el nuevo Servidor de MDM de ESET PROTECT (el nombre de host que exportó desde la configuración de su «antiguo» servidor de MDM) coincide con el del MDM ESET PROTECT anterior.

1. Instalar/Lanzar una base de datos de MDM compatible ESET PROTECT.

2. Importar/Restaurar la ESET PROTECTbase de datos de MDM desde su Servidor MDM de ESET PROTECT anterior.

3. Instale el Servidor/MDM ESET PROTECT mediante el instalador de paquetes todo en uno (Windows) o elija otro método de instalación (instalación manual Windows, Linux o Aparato virtual). Especifique la configuración de conexión de la base de datos durante la instalación del MDM ESET PROTECT.

Al instalar MDM de ESET PROTECT en Linux, utilice el certificado HTTPS de la copia de seguridad.

4. Conéctese a la Consola web ESET PROTECT.

5. Reinicie el servicio de MDM de ESET PROTECT.

Los dispositivos móviles deben conectarse ahora a su nuevo servidor MDM ESET PROTECT usando su certificado original.

❑ **Desinstalación del Servidor/MDM ESET PROTECT anterior:**

Cuando tenga todo funcionando correctamente en el nuevo Servidor ESET PROTECT, desinstale con cuidado su Servidor/MDM ESET PROTECT anterior mediante las instrucciones paso a paso.

Cambio de dirección IP o nombre de host de ESET PROTECT en el servidor después de la migración

Para cambiar un nombre de host o una dirección IP en su Servidor ESET PROTECT, siga estos pasos:

1. Si su certificado de Servidor ESET PROTECT contiene una dirección IP específica y/o nombre de host, cree un nuevo certificado del Servidor e incluya el nombre de host o la dirección IP nueva. Sin embargo, si tiene un comodín* en el campo host del certificado del servidor, **pase al paso 2**. De lo contario, cree un nuevo certificado de servidor mediante el agregado de una nueva dirección IP y nombre de servidor separado por coma e incluya además el nombre de host y la dirección IP anterior.

2. Firme el certificado del Servidor nuevo con la Autoridad de Certificación del Servidor ESET PROTECT.

3. Cree una política de cambio de conexiones de clientes al nombre de host o la dirección IP nueva (preferentemente la dirección IP), pero incluya una segunda conexión (alternativa) al nombre de host o dirección IP anterior para dar al Agente ESET Management la posibilidad de conectarse con ambos servidores. Para obtener más información, consulte Crear una política para que los Agentes ESET Management se

conecten al nuevo Servidor ESET PROTECT.

4. Implemente la política en los equipos cliente y permita replicar a los Agentes ESET Management. Aunque la política redirigirá los clientes a su nuevo servidor (que no está en ejecución), los Agentes ESET Management usarán la información del Servidor alternativo para conectarse con la dirección IP original.

5. Configure sunuevo certificado del Servidor en Más > Configuración.

6. Reinicie el servicio del Servidor ESET PROTECT y cambie el nombre del host o la dirección IP.

Consulte nuestro Artículo en la Base de conocimiento para obtener instrucciones ilustradas para cambiar la dirección del Servidor ESET PROTECT.

Migración desde ERA 5.x

No puede actualizar ni migrar directamente ERA 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 el servidor de ESET PROTECT y sus componentes

Seleccione uno de los capítulos a continuación para desinstalar el servidor de ESET PROTECT y sus componentes:

- Desinstalar el Agente ESET Management
- Windows: desinstalar el servidor de ESET PROTECT y sus componentes
- Linux: actualizar, volver a instalar o desinstalar los componentes de ESET PROTECT
- macOS: desinstalar el agente de ESET Management y el producto ESET Endpoint
- Desactivar el servidor ESMC/ESET PROTECT/MDM anterior luego de realizar la migración a otro servidor

Desinstalar el Agente ESET Management

El Agente ESET Management se puede desinstalar de varias formas.

Desinstalación remota mediante la Consola web ESET PROTECT

1. Conéctese a la Consola web ESET PROTECT .

2. Desde el panel **Equipos**, seleccione un equipo desde donde desea quitar el Agente ESET Management y haga clic en **Nueva tarea**.

Como alternativa, seleccione varios equipos mediante la selección de las casillas de verificación correspondientes y luego haga clic en **Equipo** > **Tareas** > **Nueva tarea**.

3. Ingrese el **Nombre** de la tarea.

4. En el menú desplegable **Categoría de tarea**, seleccione **ESET PROTECT**.

5. En el menú desplegable **Tarea**, seleccione Detener la administración (desinstalar Agente ESET Management).

Cuando desinstala el agente ESET Management del equipo del cliente, el dispositivo ya no es administrado por ESET PROTECT:
- El producto de seguridad de ESET puede conservar algunas configuraciones después de desinstalar el agente ESET Management.
- Si el agente está protegido por contraseña, no podrá desinstalarlo. Se recomienda reiniciar algunas configuraciones que no desea conservar (por ejemplo, la protección de contraseña) a los valores predeterminados a través de una política, antes de que el dispositivo sea eliminado de la administración.
- Se abandonarán todas las tareas que se ejecuten en el agente. Es posible que los estados de ejecución **Ejecutando**, **Finalizado** o **Falló** de esta tarea no se observen adecuadamente en la consola web ESET PROTECT que depende de la replicación.
- Luego de que se haya desinstalado el agente, puede administrar su producto de seguridad mediante EGUI o eShell integrados.

6. Revise la tarea **Resumen** y haga clic en **Finalizar**.

7. Haga clic en Crear desencadenador para especifica cuándo se debe ejecutar esta Tarea de cliente y en qué **Destinos**.

Desinstalación local: Windows

Consulte también las instrucciones de desinstalación local del Agente ESET Management en Linux o macOS. Para resolver problemas de desinstalación del agente, consulte la Resolución de problemas de desinstalación del agente ESET Management.

1. Conéctese al equipo de terminal donde desea eliminar el Agente ESET Management (por ejemplo, mediante RDP).

2. Vaya a **Panel de control** > **Programas y características** y haga doble clic en **ESET Management Agente**.

3. Haga clic en **Siguiente** > **Eliminar** y siga las instrucciones de desinstalación.

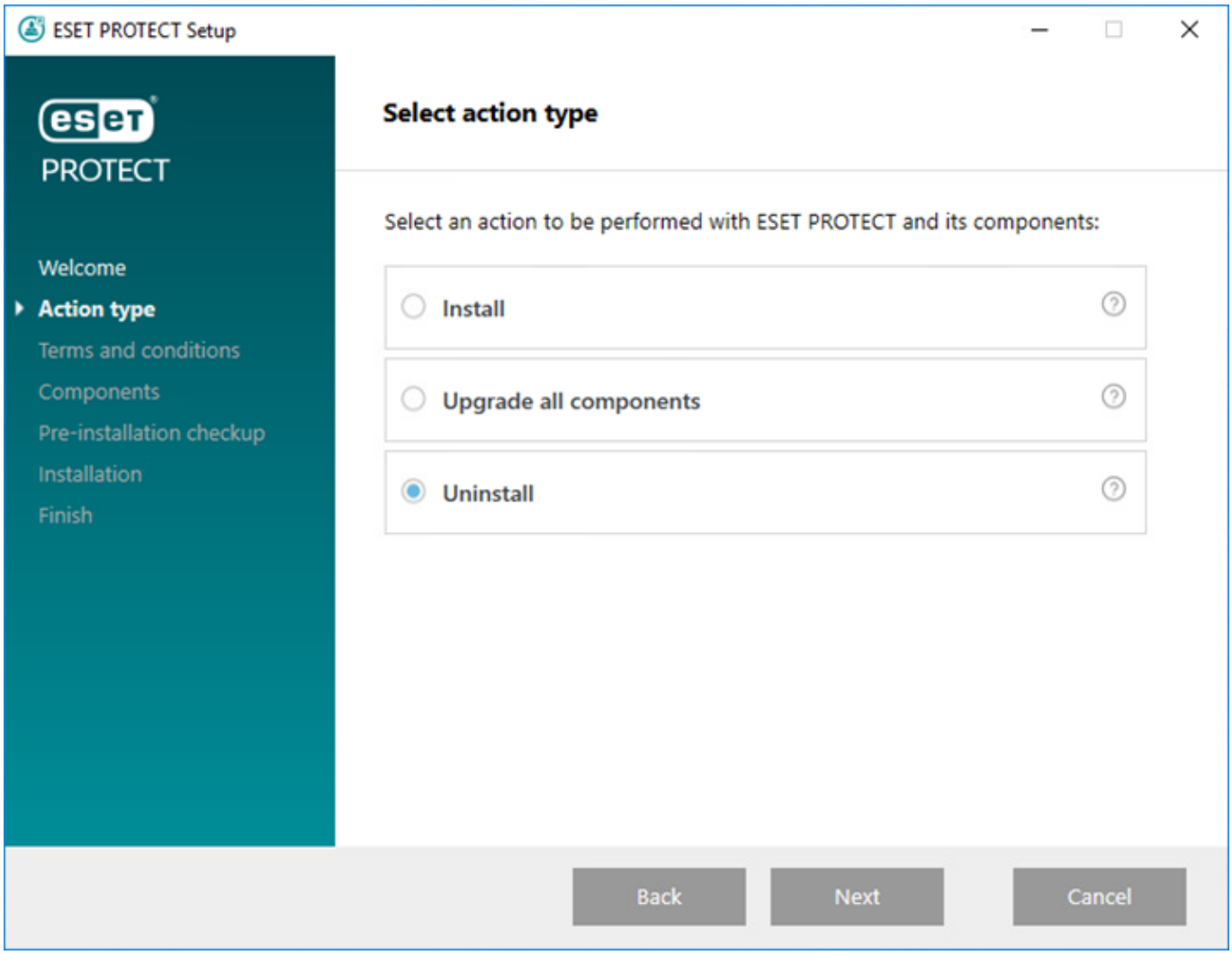
Si ha establecido una contraseña con una política para los Agentes ESET Management, tiene estas opciones:
- Tendrá que escribir la contraseña durante la desinstalación.
- Desasigne la política primero antes de desinstalar el Agente ESET Management.
- Vuelva a implementar el Agente ESET Management en un Agente existente protegido por contraseña (un artículo de la base de conocimiento).

Windows: desinstalar el servidor de ESET PROTECT y sus componentes

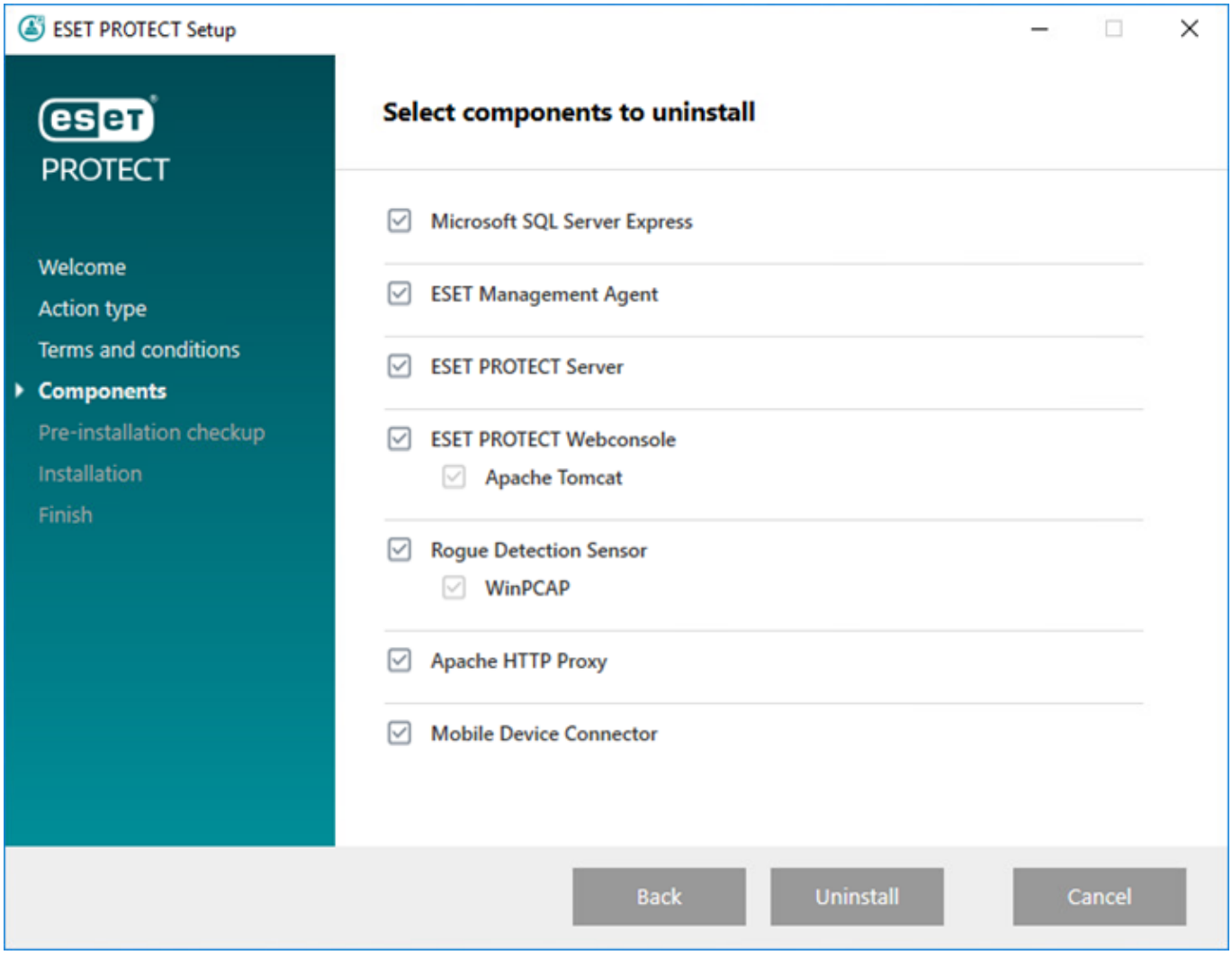
Antes de desinstalar ESET PROTECT, desinstale los agentes de los equipos administrados.
Antes de instalar el Conector de dispositivo móvil, lea funcionalidad de la licencia MDM iOS.

Siga estos pasos para desinstalar el servidor ESET PROTECT y sus componentes en Windows:

1. Descargue el instalador todo en uno de ESET PROTECT y descomprima el paquete.
2. Ejecute *Setup.exe*. Puede seleccionar el **Idioma** en el menú desplegable. Haga clic en **Siguiente**.
3. Seleccione **Desinstalar** y haga clic en **Siguiente**.



4. Acepte los EULA y haga clic en **Siguiente**.
5. Seleccione los componentes que desea desinstalar y haga clic en **Desinstalar**.



6. Es posible que sea necesario reiniciar el equipo para finalizar la eliminación de componentes particulares.

Consulte también Desactivar el servidor ESMC/ESET PROTECT/MDM anterior luego de realizar la migración a otro servidor.

Linux: actualizar, volver a instalar o desinstalar los componentes de ESET PROTECT

Si desea reinstalar o actualizar el componente a una versión más reciente, ejecute el script de instalación nuevamente.

Para desinstalar un componente (en ese caso, el Servidor ESET PROTECT), ejecute el instalador con el parámetro `--uninstall`, según se indica a continuación:

```
sudo ./server-linux-x86_64.sh --uninstall --keep-database
```

Si desea desinstalar otro componente, use el nombre del paquete adecuado en el comando. Por ejemplo, Agente ESET Management:

```
sudo ./agent-linux-x86_64.sh --uninstall
```

La configuración y los archivos 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 use el parámetro `--keep-database`.

Después de la desinstalación, verifique si

- el servicio `eraserver` se eliminó.
- la carpeta `/etc/opt/eset/RemoteAdministrator/Server/` se eliminó.

Se recomienda que realice un volcado de la base de datos en una copia de seguridad antes de realizar la desinstalación en caso de que necesite restablecer sus datos.
Para obtener más información acerca de cómo volver a instalar el Agente, consulte el capítulo correspondiente.
Para resolver problemas de desinstalación del agente, consulte la Resolución de problemas de desinstalación del agente ESET Management.

macOS: desinstalar el agente de ESET Management y el producto ESET Endpoint

Desinstale el agente de ESET Management y el producto ESET Endpoint a nivel local o en forma remota a través de ESET PROTECT.

Encontrará instrucciones más detalladas para la desinstalación local del agente de ESET Management y del producto ESET Endpoint en nuestro artículo de la base de conocimiento.

Si quiere desinstalar en forma remota el producto ESET Endpoint, asegúrese de hacerlo antes de desinstalar el agente de ESET Management.

Desinstalar el agente de ESET Management a nivel local

1. Haga clic en **Buscador** para abrir una nueva ventana del **Buscador**.
2. Haga clic en **Aplicaciones** > mantenga presionada la tecla **CTRL** > haga clic en el agente de **ESET Management** > seleccione **Mostrar contenidos del paquete** del menú contextual.
3. Vaya a **Contenidos** > **Scripts** y haga doble clic en **Uninstaller.command** para ejecutar el desinstalador.
4. Escriba la contraseña de administrador y presione **Aceptar** si se le pide que ingrese una contraseña.
5. Verá el mensaje **Proceso finalizado** cuando se haya desinstalado el agente de ESET Management.

Desinstalar el Agente de ESET Management a nivel local a través del terminal

1. Abra **Buscador** > **Aplicaciones** > **Utilidades** > **Terminal**.
2. Escriba el siguiente código y presione **Intro**:

```
sudo /Applications/ESET\ Management\ Agent.app/Contents/Scripts/Uninstall.command ;
 exit;
```

3. Escriba la contraseña de administrador y presione **Aceptar** si se le pide que ingrese una contraseña.

4. Verá el mensaje **Proceso finalizado** cuando se haya desinstalado el agente de ESET Management.

Desinstalar el agente de ESET Management en forma remota a través de ESET PROTECT

En **Equipos**, haga clic en el equipo macOS cliente y seleccione **Quitar** para desinstalar el agente de ESET Management y quitar el equipo de la administración.

Para resolver problemas de desinstalación del agente, consulte la Resolución de problemas de desinstalación del agente ESET Management.

Desinstalar el producto ESET Endpoint a nivel local

1. Haga clic en **Buscador** para abrir una nueva ventana del **Buscador**.

2. Haga clic en **Aplicaciones** > mantenga presionada la tecla **CTRL** > haga clic en **ESET Endpoint Security** o **ESET Endpoint Antivirus** > seleccione **Mostrar contenidos del paquete** del menú contextual.

3. Vaya a **Contenidos** > **Ayuda** 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 ingrese una contraseña.

6. Verá el mensaje **Desinstalación correcta** cuando ESET Endpoint Security o ESET Endpoint Antivirus se hayan desinstalado correctamente. Haga clic en **Cerrar**.

Desinstalar el producto ESET Endpoint a nivel local desde el terminal

1. Abra **Buscador** > **Aplicaciones** > **Utilidades** > **Terminal**.

2. Escriba el siguiente código y presione **Intro**:

- 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 presione **Aceptar** si se le pide que ingrese una contraseña.

4. Verá el mensaje **Proceso finalizado** cuando se haya desinstalado el producto ESET Endpoint.

Desinstalar el producto ESET Endpoint de manera remota a través de ESET PROTECT

Para desinstalar el agente de ESET Management en forma remota a través de ESET PROTECT, puede recurrir a alguna de estas opciones:

- En **Equipos**, haga clic en el equipo macOS cliente, seleccione **Detalles** > **Aplicaciones instaladas** > seleccione **ESET Endpoint Security** o **ESET Endpoint Antivirus** y haga clic en el botón **Desinstalar**.
- Use la tarea **Desinstalación de software** ***.

Desactivar el servidor ESMC/ESET PROTECT/MDM anterior luego de realizar la migración a otro servidor

Asegúrese de que el nuevo Servidor/MDM ESET PROTECT esté en funcionamiento y que los equipos cliente y los dispositivos móviles estén conectados al nuevo ESET PROTECT correctamente.

Existen algunas opciones cuando desactiva su servidor ESMC/ESET PROTECT/MDM anterior tras la migración a otro servidor:

I.**Mantenga el sistema operativo de la máquina del servidor y vuelva a usarlo**

1. Detenga el antiguo servicio de servidor de ESMC/ESET PROTECT.

2. Quite (`DROP DATABASE`) la instancia de base de datos del servidor anterior ESMC/ESET PROTECT (MS SQL o MySQL).

Si migró la base de datos al nuevo servidor de ESET PROTECT, asegúrese de quitar la base de datos en el antiguo servidor ESMC/ESET PROTECT antes de su desinstalación para evitar que las licencias se eliminen de la nueva base de datos del servidor de ESET PROTECT.

3. Desinstale el servidor ESMC/ESET PROTECT/MDM anterior y todos sus componentes (incluidos el agente ESET Management, Rogue Detection Sensor, MDM, etc.):

   - Desinstalar ESMC 7.2 - Windows
   - Desinstalar ESET PROTECT 8.x - Windows
   - Desinstalar ESET PROTECT 9.x - Windows
   - Desinstalar ESET PROTECT - Linux

No desinstale la base de datos si hay otro software dependiente de su base de datos.

4. Planee reiniciar el sistema operativo de su servidor después de la desinstalación.

II.**Mantenga la máquina del servidor**

La manera más sencilla de quitar ESMC/ESET PROTECT/MDM consiste en formatear el disco en el que está instalado.

⚠ Esto borrará todo lo del disco, incluido el sistema operativo.

Solución de problemas

Dado que ESET PROTECT es un producto complejo que usa diversas herramientas externas y admite diversas plataformas de sistemas operativos, existe la posibilidad de encontrarse con problemas que requieran resolución de problemas.

La documentación de ESET contiene diversos métodos para resolver problemas de ESET PROTECT. Consulte Respuestas a problemas comunes de instalación para resolver algunos problemas comunes con ESET PROTECT. Consulte también los problemas conocidos de los productos empresariales de ESET.

¿No puede resolver su problema?

- Cada componente de ESET PROTECT tiene un archivo de registro que se puede configurar más o menos detallado. Revise los registros para identificar errores que pudieran explicar el problema que tiene.

- El detalle de registros de cada componente se configura en esta política > **Configuración avanzada** > **Inicio de sesión** > **Rastrear la verbosidad de los registros** : puede configurar el nivel del detalle del registro que determina el nivel de información que se recopilará y registrará; desde **Seguimiento** (informativo) hasta**Grave** (información crítica más importante).

  - Política del Agente ESET Management: para que funcione, la política debe implementarse en el dispositivo. Para permitir el registro completo del agente de ESET Management en el archivo *trace.log*, cree un archivo ficticio con el nombre *traceAll* sin una extensión en la misma carpeta donde se encuentra *trace.log* y, luego, reinicie el equipo (para reciniciar el servicio del agente de ESET Management).

  - ESET PROTECT Configuración del servidor

  - Política del Mobile Device Connector de ESET: para que funcione, la política debe implementarse en el dispositivo. Consulte también Resolución de problemas de MDM.

- Si no puede resolver su problema, puede visitar el Foro de seguridad de ESET y consultar a la comunidad de ESET para obtener información sobre los problemas que pudiera encontrar.

- Cuando se comunique con Soporte técnico de ESET, es posible que se le pida que recopile los archivos de registro con ESET Log Collector o la Herramienta de diagnóstico. Le recomendamos especialmente incluir los registros cuando se comunique con el soporte técnico para acelerar la solicitud de servicio de atención al cliente.

Actualización de los componentes ESET PROTECT en un

entorno fuera de línea

Siga estos pasos para actualizar los componentes ESET PROTECT y los productos de terminales de ESET sin acceso a Internet:

Es posible usar la Tarea de actualización de componentes para un entorno sin conexión en los siguientes casos:
- Hay un repositorio fuera de línea disponible.
- La ubicación del repositorio para el Agente ESET Management se configura con una política a una ubicación accesible.

Realice una actualización del Servidor ESET PROTECT y la Consola web:

1. Verifique qué versión de la consola de administración de ESET se está ejecutando en el servidor.

2. Descargue el instalador todo en uno para Windows más reciente o los instaladores de componentes de ESET PROTECTindependientes más recientes para Linux del sitio de descargas de ESET.

3. Realice una actualización del Servidor ESET PROTECT y la Consola web ESET PROTECT:

   - Windows: actualización con el instalador todo en uno

   - Linux: actualización manual basada en componentes

La consola web y la actualización de Apache Tomcat limpian los archivos de ayuda sin conexión. Si utilizó la ayuda sin conexión con ESMC o una versión anterior de ESET PROTECT, vuelva a crearla para ESET PROTECT 9.1 luego de realizar la actualización para asegurarse de tener la versión más reciente de la ayuda sin conexión que coincida con su versión de ESET PROTECT.

Continúe con la actualización fuera de línea de los productos Endpoint de ESET

1. Vea cuáles productos de ESET se encuentran instalados en los clientes: Abra la Consola web ESET PROTECT y vaya a **Tablero** > **Aplicaciones de ESET**.

2. Asegúrese de tener las versiones más recientes de los productos de punto de conexión de ESET.

3. Descargue los instaladores desde el sitio de descarga de ESET al repositorio local configurado durante la instalación fuera de línea.

4. Ejecute una Tarea de instalación de software desde la Consola web ESET PROTECT.

Respuestas a problemas comunes de instalación

Expanda la sección para el mensaje de error que desea resolver:

ESET PROTECTServidor

El servicio del Servidor ESET PROTECT no se inicia:

Instalación dañada

- Podría ser el resultado de claves de registro faltantes, archivos faltantes o permisos de archivos no válidos.
- El instalador todo en uno de ESET tiene su propio archivo de registro. Cuando instala un componente en forma manual, use el método Emisión de registros MSI.

Puerto de escucha ya usado (principalmente 2222 y 2223)

Use el comando adecuado para su sistema operativo:

- Windows:

```
netstat -an | find "2222"
netstat -an | find "2223"
```

- Linux:

```
netstat | grep 2222
netstat | grep 2223
```

La base de datos no funciona/no se puede localizar

- Servidor MS SQL: Verifique que el puerto 1433 esté disponible en el servidor de la base de datos o intente iniciar sesión en SQL Server Management Studio
- MySQL: Verifique que el puerto 3306 esté disponible en el servidor de la base de datos o intente iniciar sesión en su interfaz de base de datos (por ejemplo, mediante la interfaz de líneas de comandos MySQL o `phpmyadmin`)

Base de datos dañada

Se mostrarán varios errores de SQL en el archivo de registro del Servidor ESET PROTECT. Le recomendamos restaurar la base de datos desde una copia de seguridad. Si la copia de seguridad no está presente, reinstale ESET PROTECT.

Recursos insuficientes del sistema (RAM, espacio en disco)

Revisar procesos en ejecución y rendimiento del sistema:

- Usuarios de Windows: Ejecutar y revisar información en el gestor de tareas o visor de eventos
- Usuarios de Linux: Ejecute uno de los siguientes comandos:

`df -h` (para revisar la información del espacio en el disco)
`cat /proc/meminfo` (para revisar la información del espacio en la memoria)
`dmesg` (para revisar el estado del sistema Linux)

Error con el conector ODBC durante la instalación del ServidorESET 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 ODBC que admite procesamiento múltiple o reconfigure *odbcinst.ini* tal como se muestra en la sección de configuración de ODBC.

Error con la conexión a la base de datos durante la instalación del Servidor ESET PROTECT

La instalación del Servidor ESET PROTECT 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.
```

Verifique que la configuración del controlador de su base de datos coincide con el que se muestra en la sección de configuración de ODBC.

Agente ESET Management

Resolución de problemas de desinstalación del agente ESET Management

• Vaya a los archivos de registro para el Agente ESET Management.

• Puede desinstalar el Agente ESET Management con el desinstalador de ESET o mediante una forma no estándar (como quitar archivos, quitar el servicio de Agente ESET Management y las entradas de registros). Si hay un producto de terminales de ESET en el mismo equipo, no será posible debido a una autodefensa habilitada.

• Se muestra el mensaje “No se pudo actualizar la base de datos. Quite primero el producto." durante la desinstalación del Agente: Reparación del Agente ESET Management:

1.Haga clic en **Panel de control** > **Programas y características** y haga doble clic en **ESET Management Agente**.

2.Haga clic en **Siguiente** > **Reparar** y siga las instrucciones.

Todas las maneras posibles de desinstalar el Agente ESET Management se describen en la Sección desinstalación.

Ocurrió un error código 1603 durante la instalación del agente

Este error puede ocurrir cuando los archivos del instalados no se encuentran en el disco local. Para solucionarlo, copie los archivos del instalados en el directorio local y ejecute la instalación nuevamente. Si los archivos ya están presentes, o si el error persiste, siga nuestras instrucciones de la base de conocimientos.

Durante la instalación del Agente en Linux, aparece el mensaje de error

Mensaje de error:

```
Checking certificate ... failed
Error checking peer certificate: NOT_REGULAR_FILE
```

Una causa posible de este error es el nombre incorrecto de un archivo en el comando de instalación. La consola diferencia entre mayúsculas y minúsculas. Por ejemplo: `Agent.pfx`, no es lo mismo que`agent.pfx`.

La implementación remota desde Linux a Windows 8.1 (32bit) falló

Este es un problema de autenticación originado por KB3161949 de Microsoft. Se puede resolver únicamente al eliminar esa actualización de los hosts donde falla la implementación.

El Agente ESET Management no se puede conectar al servidor de ESET PROTECT

Consulte la resolución de problemas de conexión con el agente y nuestro artículo de la base de conocimiento.

El instalador de scripts del Agente se cerró con el código 30

Usó el instalador de scripts del Agente con una ubicación de instalador personalizada y no pudo editar el script de forma correcta. Revise la página de ayuda e intente de nuevo.

Consola web

Apache HTTP Proxy

El tamaño del caché de Apache HTTP Proxy es de varios GB y continúa en aumento

Si ha instalado el proxy Apache HTTP mediante el instalador todo en uno, las limpiezas se habilitan automáticamente. Si las limpiezas no funcionan correctamente, realice una limpieza manual o programe una tarea de limpieza.

Las actualizaciones de motor de detección no funcionan luego de instalar el Apache HTTP Proxy

Si no puede actualizar las estaciones de trabajo de clientes, consulte las instrucciones de la base de conocimientos para deshabilitar el proxy Apache HTTP en estaciones de trabajo de punto final durante un período temporal. Después de resolver los problemas de conexión, considere habilitar el proxy Apache HTTP nuevamente.

Error en la actualización remota del Agente ESET Management con código de error 20008

Si hay un error en la actualización del Agente ESET Management con el siguiente mensaje:
GetFile: Error al procesar la solicitud de HTTP (código de error 20008, url: 'http://repository.eset.com/v1//info.meta')

Siga los pasos I a III de este artículo para solucionar los problemas de conexión. Si el equipo desde donde debe actualizar el Agente ESET Management está fuera de la red corporativa, configure una política para que el Agente ESET Management no use un proxy para conectarse al repositorio cuando esté fuera de la red corporativa.

ESET Rogue Detector Sensor

¿Por qué se ingresa continuamente el siguiente mensaje de error en el Detector Rogue de ESET trace.log?

```
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)
```

Hay un problema con WinPcap. Detenga el servicio de ESET Rogue Detector Sensor, vuelva a instalar la versión más reciente de WinPcap (al menos 4.1.0) y reinicie el servicio ESET Rogue Detector Sensor.

Linux

Dependencia libQtWebKit faltante en CentOS Linux

Si se muestra 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 en nuestro artículo de la base de conocimiento.

ESET PROTECT Error en la instalación del Servidor en CentOS 7

Si se muestra el siguiente error:

```
Error: DbCheckConnection: locale::facet::_S_create_c_locale name not valid
```

El problema probablemente fue ocasionado por configuraciones locales/del medioambiente. Ejecutar el siguiente comando antes del script del instalador del servidor debería ayudar:

```
export LC_ALL="en_US.UTF-8"
```

Código de error -2068052081 durante la instalación de Microsoft SQL Server.

Reinicie el equipo y ejecute la configuración nuevamente. Si continúa el problema, desinstale SQL Server Native Client y vuelva a ejecutar la instalación. Si esto no resuelve el problema, desinstale todos los productos de Microsoft SQL Server, reinicie el equipo y ejecute nuevamente la instalación.

Código de error -2067922943 durante la instalación de Microsoft SQL Server.

Verifique que su sistema cumpla con todos los requisitos de la base de datos para ESET PROTECT.

Código de error -2067922934 durante la instalación de Microsoft SQL Server.

Asegúrese de tener los privilegios de la cuenta de usuario correctos.

La Consola web muestra "Error al cargar los datos".

MS SQL Server intenta usar todo el espacio del disco disponible para los registros de transacción. Si desea limpiarlo, visite el sitio web oficial de Microsoft.

Código de error -2067919934 durante la instalación de Microsoft SQL Server.

Asegúrese de que se hayan finalizado todos los pasos anteriores correctamente. La causa de este error son archivos del sistema desconfigurados. Reinicie el equipo y ejecute la instalación nuevamente.

Archivos de registro

Cada componente ESET PROTECT realiza los registros. Los componentes ESET PROTECT escriben información sobre determinados eventos en archivos de registro. La ubicación de los archivos de registro varía según el componente. En la siguiente lista se enumeran las ubicaciones de los archivos de registro:

Windows

ESET PROTECT componente	Ubicación de los archivos de registro
ESET PROTECTServidor	*C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs*
Agente ESET Management	*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs* Consulte también resolución de problemas de conexión con el agente.
ESET PROTECTConsola web y Apache Tomcat	*C:\ProgramData\ESET\RemoteAdministrator\Tomcat\Logs* Consulte además https://tomcat.apache.org/tomcat-9.0-doc/logging.html
Conector de dispositivo móvil	*C:\ProgramData\ESET\RemoteAdministrator\MDMCore\Logs* Consulte también Resolución de problemas de MDM.
Sensor de Rogue Detection	*C:\ProgramData\ESET\Rogue Detection Sensor\Logs*
Apache HTTP Proxy	*C:\Program Files\Apache HTTP Proxy 2.[x.xx]\logs* *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\logs\errorlog*

C:\ProgramData está oculto en forma predeterminada. Para mostrar la carpeta:
1.Vaya a **Inicio** > **Panel de control** > **Opciones de carpeta** > **Ver**.
2.Seleccione **Mostrar archivos ocultos, carpetas y unidades** y haga clic en **Aceptar**.

Linux

ESET PROTECT componente	Ubicación de los archivos de registro
ESET PROTECTServidor	*/var/log/eset/RemoteAdministrator/Server/* */var/log/eset/RemoteAdministrator/EraServerInstaller.log*
Agente ESET Management	*/var/log/eset/RemoteAdministrator/Agent/* */var/log/eset/RemoteAdministrator/EraAgentInstaller.log*
Conector de dispositivo móvil	*/var/log/eset/RemoteAdministrator/MDMCore/* */var/log/eset/RemoteAdministrator/MDMCore/Proxy/* Consulte también Resolución de problemas de MDM.
Apache HTTP Proxy	*/var/log/httpd/*
ESET PROTECTConsola web y Apache Tomcat	*/var/log/tomcat/* Consulte además https://tomcat.apache.org/tomcat-9.0-doc/logging.html
ESET RD Sensor	*/var/log/eset/RogueDetectionSensor/*

Aparato virtual ESET PROTECT

ESET PROTECT componente	Ubicación de los archivos de registro
ESET PROTECT Configuración AV	*/root/appliance-configuration-log.txt*
ESET PROTECTServidor	*/var/log/eset/RemoteAdministrator/EraServerInstaller.log*
Apache HTTP Proxy	*/var/log/httpd*

macOS

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/

/Users/%user%/Library/Logs/EraAgentInstaller.log

Herramienta de diagnóstico

Esta herramienta de diagnóstico forma parte de todos los componentes ESET PROTECT. Se usa para recopilar y empacar registros que los agentes de soporte técnico y desarrolladores usan 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 **Diagnostic<product>** ejecutable (una palabra, por ejemplo, **DiagnosticServer**, **DiagnosticAgent**)

Uso (Linux)

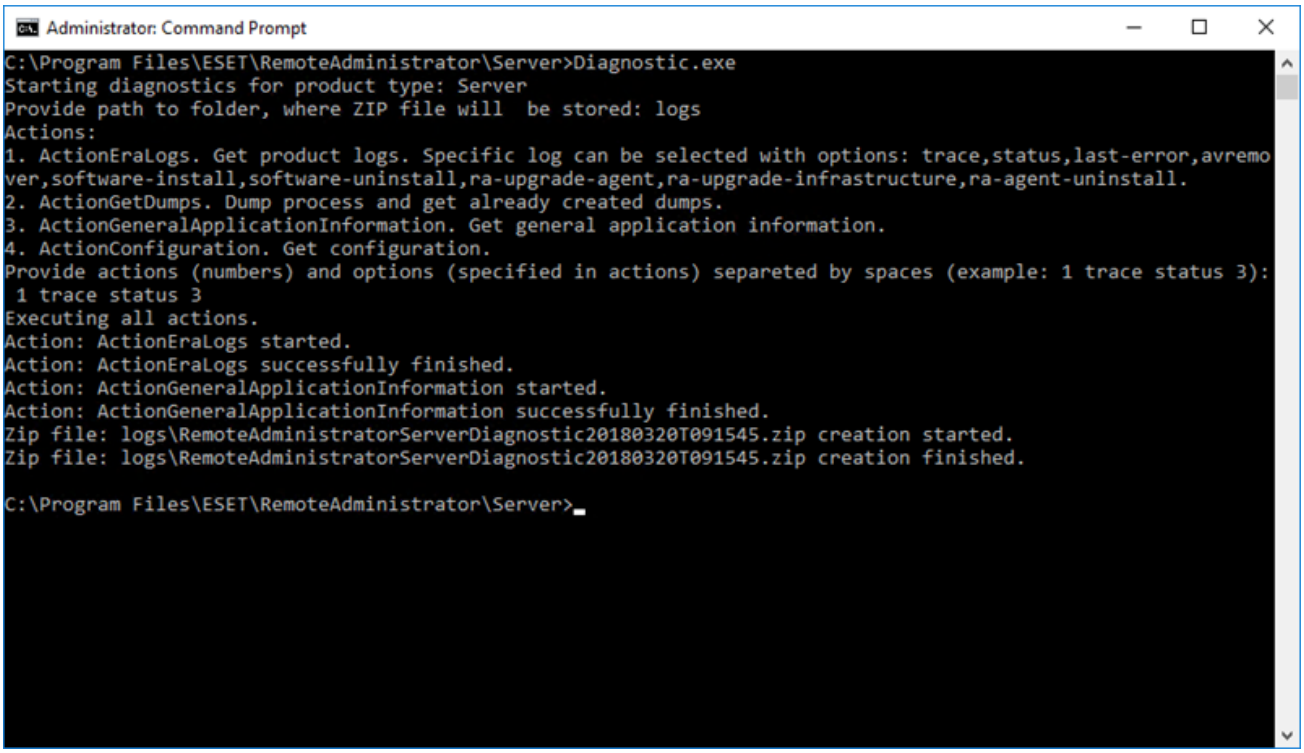
Ejecute los diagnósticos ejecutables en la terminal como root y siga las instrucciones que aparecen en su pantalla.

Uso (Windows)

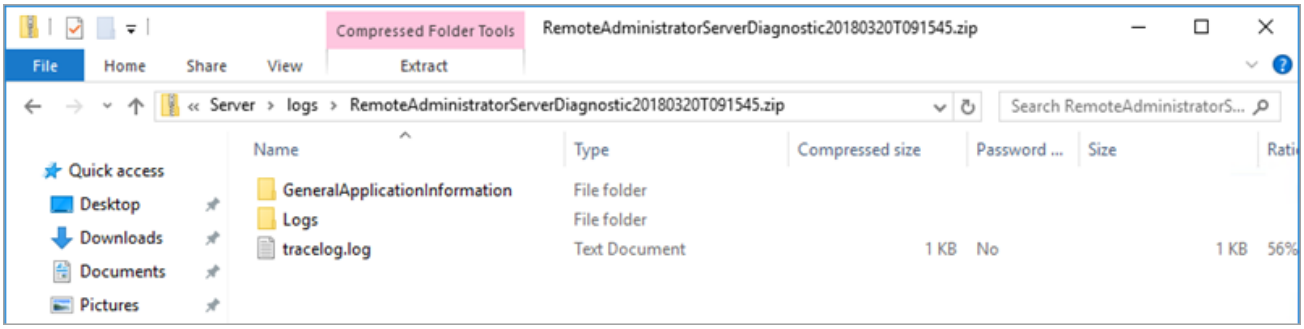
1. Ejecute la herramienta con un símbolo del sistema.

2. Introduzca la ubicación de los archivos de registro que almacenará (en nuestro ejemplo “logs”) y pulse **Intro**.

3. Ingrese la información que desea 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**” en la ubicación Herramienta de diagnóstico.



Acciones

- **ActionEraLogs**: se crea una carpeta de registros donde se guardan todos los registros. Para especificar solo determinados registros, use un espacio para separar cada registro.

- **ActionGetDumps**: se crea una carpeta nueva. Si se detectó un problema. se suele crear un archivo de volcado del proceso. Cuando se detecta un problema grave, el sistema crea un archivo de volcado. Para comprobarlo 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 esta el archivo *GeneralApplicationInformation.txt*. Este archivo contiene información textual que incluye el nombre del producto y la versión del producto actualmente instalado.

- **ActionConfiguration**: se crea una carpeta de configuración donde se guarda el archivo storage.lua.

Problemas después de la actualización/migración del Servidor ESET PROTECT

Si no puede iniciar el servicio de Servidor ESET PROTECT debido a una instalación dañada o mensajes de error de archivos de registro desconocidos, realice una operación de reparación mediante los pasos que se muestra a continuación:

> Le recomendamos realizar una copia de seguridad del servidor de la base de datos antes de comenzar la operación de reparación.

1. Vaya a **Inicio** > **Panel de control** > **Programa y características** y haga doble clic en el servidor de **ESET PROTECT**.

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

3. Vuelva a usar la configuración de conexión de la base de datos existente y haga clic en **Siguiente**. Haga clic en **Sí si se le pide confirmación**. Puede encontrar la información de conexión de la base de datos aquí: *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*

4. Seleccione **Usar la contraseña del administrador almacenada en la base de datos** y haga clic en **Siguiente**.

5. Seleccione **Mantener los certificados actualmente existentes** y haga clic en **Siguiente**.

6. Active el servidor de ESET PROTECT 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 la consola web nuevamente y verifique que todo esté bien.

Otros escenarios de resolución de problemas:

El Servidor ESET PROTECT no se ejecuta pero hay una copia de seguridad de la base de datos:

1. Restaure la copia de seguridad de la base de datos.

2. Verifique que el equipo nuevo usa la misma dirección IP o nombre del host que su instalación anterior para asegurarse de que los Agentes se conectarán.

3. Repare el Servidor de ESET PROTECT y use la base de datos que restauró.

El Servidor ESET PROTECT no se ejecuta pero ha exportado el certificado del servidor y la Autoridad de certificación:

1. Verifique que el equipo nuevo usa la misma dirección IP o nombre del host que su instalación anterior para asegurarse de que los Agentes se conectarán.

2. Repare el Servidor de ESET PROTECT mediante certificados de copias de seguridad (cuando realice la reparación, seleccione **Cargar certificados del archivo** y siga las instrucciones).

El Servidor ESET PROTECT no se ejecuta y no tiene una copia de seguridad de base de datos o certificado del Servidor ESET PROTECT y autoridad de certificación:

1. Repare el Servidor de ESET PROTECT.

2. Repare los Agentes ESET Management mediante uno de los siguientes métodos:

- Script del instalador de agentes
- Implementación remota (para ello, deberá desactivar el firewall en los equipos de destino)
- Instalador del componente del agente manual

Emisión de registros MSI

Resulta útil si no puede instalar un componente ESET PROTECT en Windows correctamente, por ejemplo, un Agente ESET Management:

```
msiexec /i C:\Users\Administrator\Downloads\Agent_x64.msi /L*v log.txt
```

ESET PROTECT API

El ESET PROTECT ServerApi (*ServerApi.dll*) es una interfaz de programación de aplicaciones, un conjunto de funciones y herramientas para crear aplicaciones de software personalizadas para cumplir sus necesidades y temas específicos. Al usar ServerApi, su aplicación puede proporcionar una interfaz personalizada, funcionalidad y operaciones que normalmente realizaría mediante la Consola web ESET PROTECT, como administrar ESET PROTECT para generar y recibir informes, etc.

Para obtener más información y ejemplos en el idioma C y una lista de mensajes JSON disponibles, consulte la siguiente ayuda en línea:

API ESET PROTECT 9

Preguntas frecuentes

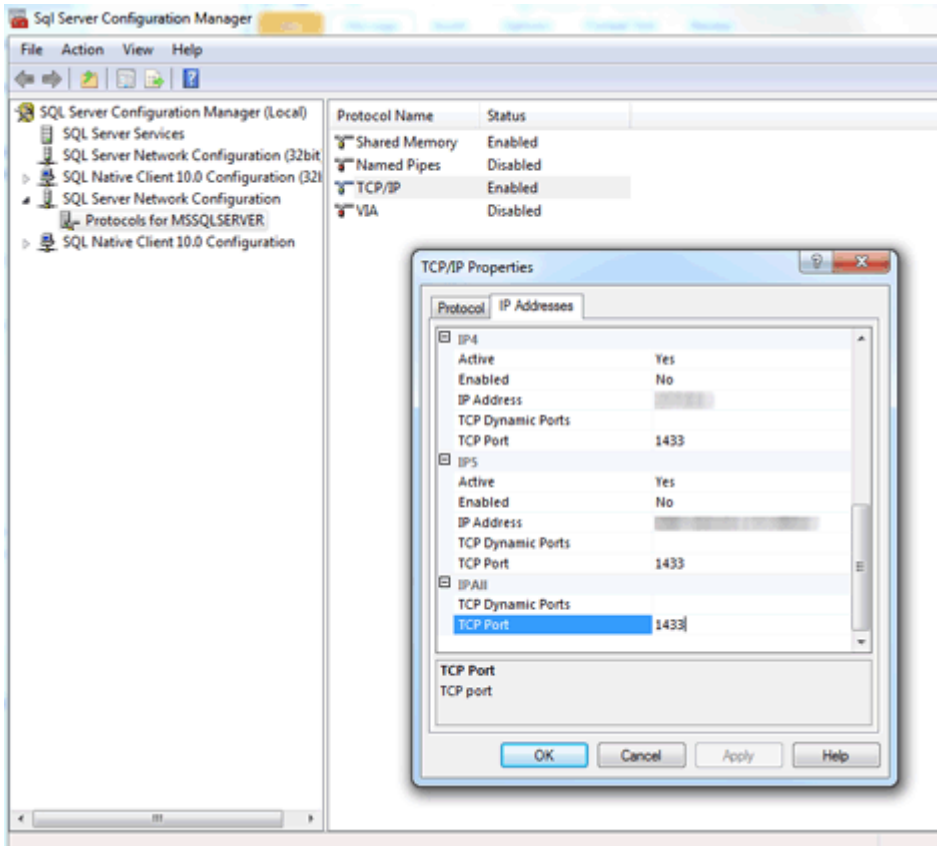
¿Por qué instalamos Java en un servidor? ¿Esto no crea un riesgo de seguridad? La mayoría de las compañías y los marcos de seguridad recomiendan desinstalar Java de sus computadores y, especialmente, de sus servidores.

La consola web de ESET PROTECT requiere Java/OpenJDK para funcionar. Java es un estándar de la industria para consolas basadas en la web y todas las principales consolas web usan Java y Web Server (Apache Tomcat) para funcionar. Java es necesario para admitir un servidor web de plataforma múltiple. 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 pasar a una alternativa sin costo. Consulte las versiones compatibles de JDK.

¿Cómo determino qué puerto usa SQL Server?

Hay varias formas de determinar el puerto usado por SQL Server. Puede obtener el resultado más exacto a través del Administrador de configuración de SQL Server. Consulte la imagen a continuación para ver un ejemplo de dónde ubicar esta información en el Administrador de configuración de SQL:



Luego de instalar SQL Server Express (incluido en el paquete de ESET PROTECT) en el Servidor Windows 2012, no parece que se esté escuchando en un puerto SQL estándar. Es más probable que se esté escuchando en un puerto diferente al predeterminado, puerto 1433.

¿Cómo configuro MySQL para aceptar un paquete de gran tamaño?

Consulte Instalación y configuración de MySQL para Windows o Linux.

Si instalo SQL por mi cuenta, ¿cómo debo crear una base de datos para ESET PROTECT?

No tiene que hacerlo. El instalador *Server.msi* crea la base de datos, no el instalador ESET PROTECT. El instalador de ESET PROTECT se incluye para simplificar pasos, instala el Servidor SQL y luego crea la base de datos mediante el instalador *Server.msi*.

¿El ESET PROTECT instalador crea una nueva base de datos para mí en una instalación del Servidor MS SQL si le doy los detalles y las credenciales de conexión al Servidor MS SQL apropiadas? Sería conveniente si el instalador es compatible con diferentes versiones de SQL Server (2014, 2019, etc.).

La base de datos es creada por *Server.msi*. Entonces, sí, puede crear una base de datos de ESET PROTECT para usted en instancias del Servidor de SQL instaladas individualmente. Las versiones compatibles del Servidor MS SQL son 2014 y posteriores.

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

- Si usa una edición anterior de Windows (servidor 2012 o SBS 2011), Microsoft SQL Server Express 2014 se instalará de manera 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 de cada base de datos relacionada. No recomendamos el uso de Microsoft SQL Server Express:
> - En entornos empresariales o redes de gran tamaño.
> - Si desea usar ESET PROTECT con ESET Inspect.

Si se instala en un SQL Server existente, ¿debe el SQL Server usar el modo de autenticación integrado en Windows de forma predeterminada?

No, porque el modo de autenticación de Windows se puede deshabilitar en SQL Server y la única manera de iniciar sesión es usar la autenticación de SQL Server (ingresando el nombre de usuario y la contraseña). Durante la instalación del servidor ESET PROTECT, se requiere la autenticación de Modo mixto (autenticación de SQL Server y autenticación de Windows). Cuando SQL Server se instala de forma manual, recomendamos crear una contraseña raíz (el usuario raíz se denomina “sa”, que significa administrador de seguridad) y almacenarla para más adelante en un lugar seguro. La contraseña raíz puede ser necesaria cuando se actualiza el Servidor ESET PROTECT. Puede configurar la autenticación de Windows después de instalar el servidor ESET PROTECT.

¿Puedo usar MariaDB en lugar de MySQL?

No, MariaDB no es compatible. Asegúrese de instalar una versión compatible de MySQL Server y ODBC Connector. Consulte la sección Instalación y configuración de MySQL.

Tuve que instalar Microsoft .NET Framework 4 tal como me indicó que hiciera el instalador de ESET PROTECT (http://www.microsoft.com/en-us/download/details.aspx?id=17851), pero no funcionaba en una instalación nueva de Windows Server 2012 R2 con SP1.

El instalador no se puede usar en Windows Server 2012 debido a la política de seguridad de Windows Server 2012. Microsoft .NET Framework se debe instalar a través del **Asistente para agregar roles y características**.

Es muy difícil saber si la instalación de SQL Server está en ejecución. ¿Cómo puedo saber qué está sucediendo si la instalación toma más de 10 minutos?

En muy pocos casos, la instalación de SQL Server puede demorar hasta 1 hora. Los tiempos de instalación dependen del rendimiento del sistema.

¿Cómo se puede restablecer la contraseña del Administrador para la consola web (que se ingresó durante la configuración)?

Es posible restablecer la contraseña al ejecutar el instalador del servidor y elegir **Reparar**. Recuerde que es posible que necesite la contraseña para acceder a la base de datos ESET PROTECT si no usó la Autenticación de Windows durante la creación de la base de datos.

- Tenga cuidado, ya que algunas de las opciones de reparación pueden eliminar datos almacenados.
- El restablecimiento de la contraseña deshabilita 2FA.

Al importar un archivo que contiene un listado de equipos para agregar a ESET PROTECT, ¿de qué formato debe ser el archivo?

El formato son las siguientes líneas:

All\Group1\GroupN\Computer1
All\Group1\GroupM\ComputerX
All es el nombre requerido del grupo raíz.

¿Puedo usar IIS en lugar de Apache? ¿Y otro servidor HTTP?

IIS es un servidor HTTP. La consola web necesita un contenedor Java servlet (como Tomcat) para funcionar, y el servidor HTTP no es suficiente. Han habido soluciones sobre cómo cambiar IIS a un contenedor Java servlet, pero en general, no es compatible.

No usamos un servidor Apache HTTP, usamos Apache Tomcat, que es un producto diferente.

¿Tiene ESET PROTECT una interfaz de línea de comandos?

Sí, tenemos 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/Essentials). Recomendamos que instale ESET PROTECT en un servidor diferente o que no seleccione el componente SQL Server Express durante la instalación (esto requiere que use un SQL Server o un MySQL existente para ejecutar la base de datos ESET PROTECT).

¿Detectará la instalación del Servidor ESET PROTECT si ya está instalado SQL en el sistema? ¿Qué ocurre si lo hace? ¿Qué ocurre con MySQL?

ESET PROTECT verificará si se está ejecutando SQL en el sistema si usted usa el asistente de instalación y ha

seleccionado SQL express para la instalación. Si ya hay un SQL en ejecución en el sistema, el asistente mostrará una notificación para desinstalar el SQL existente y, luego, ejecutará la instalación nuevamente o instalará ESET PROTECT sin SQL Express. Vea los requisitos de la base de datos de ESET PROTECT.

¿Dónde puedo encontrar la asignación de componentes de ESET PROTECT por versión de lanzamiento?

Consulte nuestro artículo de la base de conocimiento.

¿Cómo realizo una actualización de ESET PROTECT a la versión más reciente?

Consulte los procedimientos de actualización.

¿Cómo actualizo un sistema sin conexión a Internet?

Use el proxy HTTP instalado en una máquina que se pueda conectar a los servidores de actualización de ESET (si los archivos de actualización están en la caché) y lleve Endpoints a dicho proxy HTTP en una red local. Si su servidor no tiene conexión a Internet, puede habilitar la característica Mirror en el producto de terminales en una sola máquina, usar una unidad USB para enviar los archivos de actualización a este equipo y configurar los restantes equipos fuera de línea para usarlos como servidor de actualización.

Para información sobre cómo realizar una instalación fuera de línea, siga estas instrucciones.

¿Cómo vuelvo a instalar mi Servidor ESET PROTECT y conectarlo a un servidor SQL existente si el servidor SQL se configuró automáticamente mediante la instalación inicial de ESET PROTECT?

Si está instalando la nueva instancia del Servidor ESET PROTECT usando la misma cuenta de usuario (por ejemplo, una cuenta de administrador de dominio) bajo la cual instaló el Servidor ESET PROTECToriginal, puede usar el **Servidor MS SQL mediante autenticación de Windows**.

¿Cómo soluciono los problemas con la sincronización de Active Directory en Linux?

Verifique que el ingreso de su nombre de dominio sea en letras mayúsculas (`administrator@TEST.LOCAL` en lugar de `administrator@test.local`).

¿Hay una manera de usar mi propio recurso de red (como intercambio de SMB) en lugar del repositorio?

Puede optar por proporcionar la URL directa donde se ubica el paquete. Si está usando un archivo de uso compartido, especifíquelo en el siguiente formato: file:// seguido por toda la ruta de red al archivo, por ejemplo:

file://\\eraserver\install\ees_nt64_ENU.msi

¿Cómo restablezco o cambio mi contraseña?

Idealmente, la cuenta del administrador solo se debería usar para crear cuentas para administradores individuales. Una vez que se crean las cuentas de administrador, se debe guardar la contraseña del administrador y no se debe usar la cuenta. Esta práctica permite que la cuenta del administrador se use para restablecer las contraseñas y para los detalles de cuentas únicamente.

Cómo restablecer la contraseña de una cuenta de administrador ESET PROTECT incorporada:

1.Abra **Programas y características** (ejecute appwiz.cpl), ubique el Servidor ESET PROTECT y haga clic con el botón derecho.

2.Seleccione **Cambiar** en el menú contextual.

3.Seleccione **Reparar**.

4.Especifique los detalles de conexión de la base de datos.

5.Seleccione **Usar base de datos existente y aplique la actualización**.

6.Anule la selección de **Usar una contraseña ya almacenada en la base de datos** e ingrese la nueva contraseña.

7.Inicie sesión en la Consola web ESET PROTECT con su nueva contraseña.

Se aconseja firmemente que cree cuentas adicionales con derechos de acceso específicos en función de las competencias deseadas para su cuenta.

¿Cómo cambio los puertos del Servidor ESET PROTECT y la Consola web ESET PROTECT?

Es necesario cambiar el puerto en la configuración de su servidor web para permitir las conexiones del servidor web al nuevo puerto. Para hacerlo, siga los siguientes pasos:

1. Apague su servidor web.
2. Modifique el puerto en la configuración de su servidor web.
   a) Abra el archivo *webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties*
   b) Defina el número del nuevo puerto (por ejemplo, `server_port=44591`)
3. Vuelva a iniciar el servidor web.

¿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 resolución de problemas.

Acuerdo de licencia de usuario final

Vigente a partir del 19 de octubre de 2021.

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

Acuerdo de Licencia de Usuario Final

Los términos de este Acuerdo de licencia para el usuario final ("Acuerdo") ejecutado por y entre ESET, spol. s r. o., con domicilio social en Einsteinova 24, 85101 Bratislava, Slovak Republic, registrado en el Registro Mercantil administrado por el tribunal de distrito de Bratislava I, sección Sro, n.° de entrada 3586/B, número de registro de negocio: 31333532 ("ESET" o el "Proveedor") y usted, una persona física o jurídica ("Usted" o el "Usuario final"), tienen derecho a usar el Software definido en el Artículo 1 de este Acuerdo. El Software definido en este artículo puede almacenarse en un soporte digital, enviarse mediante correo electrónico, descargarse de Internet, descargarse de servidores del Proveedor u obtenerse de otras fuentes bajo los términos y condiciones mencionados más adelante.

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

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

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

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

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

3. **Licencia**. Siempre que haya aceptado los términos de este Acuerdo y cumpla con todos los términos y

condiciones aquí especificados, el Proveedor le concederá los siguientes derechos (la "Licencia"):

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

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

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

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

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

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

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

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

automática de Actualizaciones. Para aprovisionar Actualizaciones, es necesario verificar la autenticidad de la Licencia, lo que incluye información sobre el equipo o la plataforma en los que está instalado el Software, de acuerdo con la Política de Privacidad.

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

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

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

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

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

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

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

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

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

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

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

f) Usted acepta que solamente usará el Software y sus funciones de una manera que no limite las posibilidades de otros Usuarios finales para acceder a estos servicios. El Proveedor se reserva el derecho de limitar el alcance los servicios proporcionados a Usuarios finales individuales, para activar el uso de los servicios por parte de la mayor cantidad posible de Usuarios finales. La limitación del alcance de los servicios también significará la terminación

completa de la posibilidad de usar cualquiera de las funciones del Software y la eliminación de los Datos y de la información de los servidores de los Proveedores o de los servidores de terceros relacionados con una función específica del Software.

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

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

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

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

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

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

PARA LOGRAR SUS RESULTADOS DESEADOS Y POR LA INSTALACIÓN, EL USO Y LOS RESULTADOS QUE OBTENGA DEL MISMO.

12. **Sin más obligaciones**. Este Acuerdo no crea obligaciones del lado del Proveedor y sus licenciatarios, excepto las obligaciones específicamente indicadas en este Acuerdo.

13. **LIMITACIÓN DE RESPONSABILIDAD**. EN LA MEDIDA EN QUE LO PERMITA LA LEGISLACIÓN APLICABLE, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O LICENCIADORES SERÁN RESPONSABLES DE PÉRDIDAS DE INGRESOS, GANANCIAS, VENTAS, DATOS O COSTOS DE ADQUISICIÓN DE BIENES O SERVICIOS SUSTITUIDOS, DAÑOS A LA PROPIEDAD, DAÑOS PERSONALES, INTERRUPCIÓN DEL NEGOCIO, PÉRDIDA DE INFORMACIÓN COMERCIAL O DE CUALQUIER VALOR ESPECIAL, DIRECTO, INSONDADO, ACCIDENTAL, ECONÓMICO, DE COBERTURA, DAÑOS PUNITIVOS, ESPECIALES O CONSECUENCIALES, QUE SIN EMBARGO DERIVEN O SURJAN POR CONTRATO, AGRAVIOS, NEGLIGENCIA U OTRA TEORÍA DE RESPONSABILIDAD QUE DERIVE DE LA INSTALACIÓN, EL USO O LA INCAPACIDAD DE USAR EL SOFTWARE, AUNQUE EL PROVEEDOR, SUS LICENCIADORES O FILIALES RECIBAN INFORMACIÓN DE LA POSIBILIDAD DE DICHOS DAÑOS. DADO QUE DETERMINADOS PAÍSES Y 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. Nada de lo contenido en este Acuerdo perjudicará los derechos estatutarios de ninguna parte que actúe en calidad de consumidor si infringe dicho Acuerdo.

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

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

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

18. **Licencias para autoridades públicas y el gobierno de los Estados Unidos**. Se deberá suministrar el Software a

las autoridades públicas, incluyendo el gobierno argentino, con los derechos de la Licencia y las restricciones descritas en este Acuerdo.

19. **Cumplimiento del control comercial**.

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

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

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

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

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

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

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

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

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

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

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

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

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

ANEXO AL ACUERDO

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

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

El Software requiere que se instale un componente en el equipo administrado, lo que permite la transferencia de información entre un equipo administrado y un software de administración remota. La información, que está sujeta a la transferencia, contiene datos de administración tal como información sobre el Hardware y el Software de un ordenador administrado así como sobre las instrucciones de administración provenientes de un Sofware de administración remota. Cualquier otro tipo de datos que transfiera el equipo administrado debe estar determinado por la configuración del Software instalado en ese equipo. Las instrucciones del Software de administración deben estar determinadas por la configuración del Software de administración remota.

EULAID: EULA-PRODUCT-PROTECT; 3537.0

Política de privacidad

ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, República Eslovaca, inscripta en el Registro comercial del Tribunal de distrito de Bratislava I, Sección Sro, Registro No 3586/B, Número de registro de empresa: 31333532 como Controlador de datos (“ESET” o “Nosotros”) desea ser transparente con el procesamiento de datos personales y la privacidad de nuestros clientes. A fin de cumplir con el objetivo, publicamos la presente Política de privacidad con el único propósito de informar a nuestros clientes (“Usuario final” o “Usted”) acerca de los siguientes temas:

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

Procesamiento de datos personales

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

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

Confidencialidad de los datos

ESET es una compañía que opera globalmente a través de entidades o socios afiliados como parte de nuestra red de distribución, servicio y soporte. Los datos procesados por ESET pueden ser transferidos desde y hasta las

entidades afiliadas o socios para ejecutar EULA, como por ejemplo la prestación de servicios o soporte o facturación. Según la ubicación y servicio que Usted decida utilizar, Nosotros podemos solicitarle que transfiera sus datos a un país sin una decisión adecuada de la Comisión Europea. Incluso en tal situación, cada transferencia de datos se encuentra sujeta a la regulación de la protección de datos y se realiza solo si es necesaria. Se deben establecer cláusulas contractuales estándar, normas corporativas vinculantes u otra forma de protección adecuada sin excepción.

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

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

Derechos de la persona registrada

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

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

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

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