ESET PROTECT On-Prem

Guía de administración

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

ESET PROTECT On-Prem 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. 17/04/2024

Introducción a ESET PROTECT On-Prem

Le damos la bienvenida a la versión 11.0 de ESET PROTECT On-Prem. ESET PROTECT On-Prem Le permite administrar los productos ESET en estaciones de trabajo, servidores y dispositivos móviles en un entorno de red desde una ubicación central. A través de la consola web de ESET PROTECT, puede implementar soluciones ESET, gestionar tareas, aplicar políticas de seguridad, controlar el estado del sistema y responder rápidamente a problemas o detecciones en equipos remotos.

Consulte el glosario de ESET para obtener más información acerca de las tecnologías de ESET y los tipos de detecciones o ataques contra los que protegen.

Se ha cambiado el nombre de las siguientes soluciones de seguridad empresarial de ESET:

Nombre anterior:	Nombre nuevo:	Se ha cambiado el nombre en la versión:
ESET PROTECT	ESET PROTECT On-Prem	11.0
ESET PROTECT Cloud	ESET PROTECT	5.0
ESET Inspect	ESET Inspect On-Prem	2.0
ESET Inspect Cloud	ESET Inspect	

ESET PROTECT componentes

- Servidor ESET PROTECT: puede instalar el servidor ESET PROTECT en servidores Windows y Linux o implementarlo como un aparato virtual preconfigurado. Maneja la comunicación con los agentes y recopila y archiva datos de la aplicación en la base de datos.

- Consola web ESET PROTECT: la consola web ESET PROTECT es la interfaz primaria que le permite administrar equipos del cliente en su entorno. Muestra una visión general del estado de los clientes en su red y le permite implementar las soluciones de ESET en equipos no administrados en forma remota. Luego de instalar el servidor ESET PROTECT, puede acceder a la consola web a través de su navegador web. Si elige que el servidor web sea accesible desde Internet, puede usar ESET PROTECT On-Prem desde prácticamente cualquier lugar y/o dispositivo con conexión a Internet. Puede instalar la consola web de ESET PROTECT en un equipo diferente a donde se ejecuta el servidor de ESET PROTECT. Consulte también Introducción a la Consola web de ESET PROTECT.

- Agente ESET Management: el agente ESET Management facilita la comunicación entre el servidor ESET PROTECT y los equipos cliente. El agente debe instalarse en el equipo cliente para establecer una comunicación entre dicho equipo y el servidor ESET PROTECT. Dado que se ubica en el equipo del cliente y puede almacenar diferentes escenarios de seguridad, el uso del agente ESET Management disminuye significativamente el tiempo de reacción frente a nuevas detecciones. A través de la consola web ESET PROTECT, puede implementar el agente ESET Management en equipos sin gestión reconocidos por Active Directory o ESET RD Sensor. Puede instalar manualmente el agente ESET Management en los equipos del cliente.

- Rogue Detection Sensor: Rogue Detection (RD) Sensor de ESET PROTECT On-Prem detecta equipos no gestionados en su red y envía su información al servidor de ESET PROTECT. Puede agregar fácilmente nuevos equipos del cliente a su red segura. El RD Sensor recuerda los equipos que ya han sido descubiertos y no enviará la misma información dos veces.

- ESET Bridge (HTTP Proxy) – Puede usar ESET Bridge con ESET PROTECT On-Prem como servicio Proxy para:

  - Descargar y caché: Actualizaciones de los módulos de ESET, paquetes de instalación y actualizaciones

insertados por ESET PROTECT On-Prem (por ejemplo, el instalador MSI de ESET Endpoint Security), actualizaciones de productos de seguridad de ESET (actualizaciones de componentes y productos), resultados de ESET LiveGuard.

- Reenviar la comunicación con agentes ESET Management al ESET PROTECT On-Prem.

- Conector de dispositivo móvil: es un componente que permite la Administración de dispositivos móviles con ESET PROTECT On-Prem, que le permite gestionar dispositivos móviles (Android e iOS) y administrar ESET Endpoint Security para Android.

⚠ El componente de conector/administración de dispositivos móviles (MDM/MDC) de ESET PROTECT (solo on-prem) llega al fin de ciclo de vida en enero de 2024. Leer más. Le recomendamos migrar a Cloud MDM.

Consulte también el resumen general de elementos de arquitectura e infraestructura de ESET PROTECT On-Prem.

herramientas independientes

- Herramienta de replicación: la herramienta de replicación es necesaria para la actualización de módulos fuera de línea. Si los equipos de su cliente no tienen conexión a Internet, puede usar la herramienta de replicación para descargar los archivos de actualización de los servidores de actualización de ESET y almacenarlos localmente.

- ESET Remote Deployment Tool: esta herramienta le sirve para implementar paquetes todo en uno creados en la consola web ESET PROTECT. Puede distribuir cómodamente el agente ESET Management con un producto de ESET en los equipos de una red.

Soluciones ESET adicionales

Para mejorar la protección de los dispositivos administrados de su red, puede usar estas soluciones de ESET adicionales:

- ESET Full Disk Encryption: ESET Full Disk Encryption es una característica adicional nativa de la consola web de ESET PROTECT y ofrece la administración del cifrado de disco completo de las estaciones de trabajo administradas de Windows y macOS con una capa de seguridad adicional en el inicio de sesión previo al arranque.

- ESET LiveGuard Advanced – ESET LiveGuard Advanced (Cloud Sandbox) es un servicio pago proporcionado por ESET. Su propósito es agregar una capa de protección específicamente diseñada para mitigar las amenazas nuevas en la jungla.

- ESET Inspect On-Prem: un sistema integral de detección y respuesta de punto final que incluye características como: detección de incidentes, administración y respuesta ante incidentes, recolección de datos, indicadores de detección de riesgos potenciales, detección de anomalías, detección de comportamiento e incumplimientos de políticas.

Sincronizar licencias

Sincronice licencias de ESET Business Account o ESET MSP Administrator 2 con ESET PROTECT On-Prem y úselas para activar los productos de seguridad de ESET en los dispositivos de su red.

- ESET Business Account: el portal de licencias de los productos empresariales de ESET le permite administrar licencias. Consulte la Ayuda en línea de ESET Business Account para obtener más información.

- ESET MSP Administrator 2: un sistema de administración de licencias para socios MSP de ESET. Consulte la Ayuda en línea de ESET MSP Administrator 2 para obtener más información.

Acerca de Ayuda

La Guía de administración tiene como finalidad ayudarle a conocer ESET PROTECT On-Prem y le proporciona instrucciones sobre cómousarlo.

Por coherencia y para evitar confusiones, la terminología usada en toda la guía está basada en los nombres de los parámetros de ESET PROTECT On-Prem. 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 On-Prem incluyen cuatro pestañas activas en la parte superior del encabezado: Instalación/Actualización, Administración e Implementación de aparato virtual.
- 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.

Leyenda del ícono

Se usan varios iconos en la consola web ESET PROTECT con su descripción. Algunos de los iconos describen acciones, tipos de elementos o estados de cuenta. La mayoría de los iconos se muestran en uno de tres colores para indicar la accesibilidad de un elemento:

Icono predeterminado: acción disponible

Icono azul: elemento resaltado al desplazar el puntero del mouse

Icono gris: acción no disponible

Ícono de estado	Descripciones
	Detalles sobre el dispositivo cliente.
	Agregar dispositivo: agrega nuevos dispositivos. **Tarea nueva** : agregar tarea nueva. **Notificación nueva** : agregar notificación nueva. **Nuevo grupo estático/dinámico**: agregar nuevos grupos.
	Editar : puede editar sus tareas creadas, notificaciones, plantilla de informes, grupos, políticas, etc.
	Duplicar: le permite crear un nueva directiva basada en la directiva existente que ha seleccionado, se requiere un nuevo nombre para el duplicado.
	Mover: equipos, directivas, grupos estáticos o dinámicos. **Grupo de acceso** Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen derechos suficientes para el grupo de destino. Cambiar el grupo de acceso es útil cuando se resuelven problemas de acceso con otros usuarios. El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario.
	Eliminar: quita el cliente, grupo seleccionado, etc. completamente.
	Renombrar múltiples elementos: si selecciona múltiples elementos puede renombrarlos de a uno en una lista o utilizar la búsqueda Regex y reemplazar múltiples elementos a la vez.
	Explorar: al usar esta opción, se ejecutará la tarea Exploración a pedido en el cliente que informó la detección.
	Actualización > **Actualizar módulos**: al usar esta opción, se ejecutará la tarea Actualizar módulos (desencadena una actualización manualmente). **Actualizar** > **Actualizar productos ESET**: actualiza los productos ESET instalados en el dispositivo seleccionado. **Actualizar** > **Actualizar sistema operativo**: actualiza el sistema operativo del dispositivo seleccionado.
	Registro de auditoría - Ver el registro de auditoría del elemento seleccionado.
	Ejecutar tarea para dispositivos móviles.
	Volver a inscribirse: vuelva a inscribir un dispositivo móvil.
	Desbloquear: el dispositivo se desbloqueará.
	Bloquear: el dispositivo se bloqueará o se marcará como perdido cuando se detecte actividad sospechosa.
	Encontrar: si desea solicitar las coordenadas GPS de su dispositivo móvil.
	Sirena/modo extraviado: desencadena una sirena muy fuerte en forma remota; la sirena se iniciará incluso si su dispositivo está silenciado.
	Restablecimiento de fábrica: todos los datos almacenados en su dispositivo se borrarán de forma permanente.
	Alimentación: haga clic en un equipo y seleccione **Alimentación** > **Reiniciar** para reiniciar el dispositivo. Puede configurar el comportamiento de reinicio o apagado de los equipos administrados. El equipo debe ejecutar el Agente de ESET Management 9.1 y versiones posteriores, además de un producto de seguridad de ESET compatible con esta configuración. **Restaurar**: restaura el archivo en cuarentena a su ubicación original.
	Apagar: haga clic en un equipo y seleccione **Alimentación** > **Apagar** para apagar el dispositivo. Puede configurar el comportamiento de reinicio o apagado de los equipos administrados. El equipo debe ejecutar el Agente de ESET Management 9.1 y versiones posteriores, además de un producto de seguridad de ESET compatible con esta configuración. Desactivar productos
	Cerrar sesión: haga clic en un equipo y seleccione **Alimentación** > **Cerrar sesión** para cerrar la sesión de todos los usuarios del equipo.
	Ejecutar tarea: seleccione una tarea y configure el límite (opcional) para esta tarea. La tarea se pondrá en cola de acuerdo con la configuración de tareas. Esta opción desencadena de inmediato una tarea existente, que se selecciona de una lista de tareas disponibles.
	Tareas recientes: muestra las tareas recientes. Haga clic en una tarea para volver a ejecutarla.
	Asignar usuario: asignar un usuario a un dispositivo. Puede administrar usuarios desde Usuarios de equipos.
	Administrar directivas : también puede asignar una Directiva de manera directa a un cliente (varios clientes), no solo a un grupo. Seleccione esta opción para asignar la política a los clientes seleccionados.
	Enviar llamada de reactivación - el servidor ESET PROTECT inicia una replicación inmediata del agente ESET Management en un equipo cliente a través de EPNS. Esto resulta útil cuando no desea esperar el intervalo regular cuando el agente ESET Management se conecta al servidor de ESET PROTECT. Por ejemplo, cuando desea que una tarea de cliente se ejecute de inmediato en los clientes o si desea que se aplique una política rápidamente.
	Implementar agente: se crea el Instalador del agente ESET Management para implementarlo el agente en el dispositivo seleccionado.
	Aislar de la red
	Finalizar aislamiento de la red **Conectarse por RDP**: genera y descarga un archivo *.rdp* que le permitirá conectarse al dispositivo objetivo a través de un protocolo de escritorio remoto.
	Silenciar: si selecciona un equipo y presiona **Silenciar**, el agente en este cliente deja de enviar informes a ESET PROTECT On-Prem, solo agregará la información. Se visualizará un ícono de silencio junto al nombre de un equipo en la columna Silenciado. Una vez que se deshabilita el silencio al hacer clic en **Quitar silencio**, el equipo silenciado volverá a informar y la comunicación entre ESET PROTECT On-Prem y el cliente se restablece.
	Deshabilitar: deshabilitar o eliminar una configuración o selección.
	Asignar - asigna una Directiva a un cliente o a grupos.
	Importar: seleccione los Informes / Políticas / Clave pública que desea importar.
	Exportar: seleccione los Informes / Políticas / Certificado de pares que desea exportar.
	Etiquetas - Editar etiquetas (asignar, desasignar, crear, quitar).
	grupo estático
	Grupo dinámico
	No aplicar la marca de política
	Aplicar la marca de política
	Forzar la marca de política
	Desencadenadores: vea la lista de Desencadenadores para la tarea del cliente seleccionada.
	Escritorio
	Móvil
	Servidor
	Servidor de archivos
	Servidor de correo

Ícono de estado	Descripciones
	Servidor de puerta de enlace
	Servidor de colaboración
	Agente ESET Management
	Conector de dispositivo móvil
	Sensor de Rogue Detection
	Servidor ESET PROTECT
	Servidor ESET Inspect
	ESET Bridge
	Tipo de detección de **antivirus**. Consulte todos los tipos de detección en Detecciones. Haga clic en un equipo y seleccione **Soluciones** > **Instalar producto de seguridad** para instalar un producto de seguridad ESET en el equipo.
	Haga clic en un equipo ícono del engranaje junto a un grupo estático y seleccione **Soluciones** > **Habilitar ESET LiveGuard** para activar y habilitar el ESET LiveGuard Advanced.
	ESET Inspect Connector Haga clic en **Equipos** > haga clic en un equipo o seleccione más equipos, y haga clic en **Equipo** > **Soluciones** > **Habilitar ESET Inspect On-Prem** para implementar el conector ESET Inspect en los equipos Windows/Linux/macOS administrados. El ESET Inspect On-Prem solo está disponible cuando tiene una licencia de ESET Inspect On-Prem y ESET Inspect On-Prem está conectado a ESET PROTECT On-Prem. Un usuario de la consola web necesita permiso de **Lectura** o superior para **Acceder a ESET Inspect** o permiso de **Lectura** o superior para el usuario **ESET Inspect**.
	Haga clic en un equipo y seleccione **Soluciones** > **Activar cifrado** para habilitar ESET Full Disk Encryption en el equipo seleccionado.
	El equipo tiene ESET Full Disk Encryption activado.

Ayuda fuera de línea

La ayuda fuera de línea de ESET PROTECT On-Prem no viene instalado de manera predeterminada. Si necesita ayuda con ESET PROTECT On-Prem que pueda usar fuera de línea (en caso de no contar con acceso a Internet en algún momento o en todo momento), siga los siguientes pasos para agregar la ayuda fuera de línea.

> La consola web y la actualización de Apache Tomcat limpian los archivos de ayuda sin conexión. Si ha utilizado la ayuda sin conexión con una versión anterior de ESET PROTECT On-Prem, vuelva a crearla para ESET PROTECT On-Prem 11.0 después de la actualización. Así se garantiza que usted cuenta con la ayuda sin conexión más reciente que coincide con la versión de su ESET PROTECT On-Prem.

Haga clic en el código de idioma para descargar la ayuda fuera de línea de ESET PROTECT On-Prem en el idioma que desee. Incluso puede tener ayuda fuera de línea instalada en varios idiomas.

Instrucciones de configuración de ayuda fuera de línea para Windows

1. Descargue un archivo *.zip* al hacer clic en el código de idiomas de la tabla a continuación para descargar la ayuda fuera de línea para su ESET PROTECT On-Prem en el idioma que desee.
2. Guarde el archivo *.zip* (por ejemplo, a una unidad flash USB).
3. Cree una carpeta nueva llamada *help* en el equipo que ejecute la consola web de ESET PROTECT en la siguiente ubicación: *%ProgramFiles%\Apache Software Foundation\[carpeta Tomcat]\webapps\era\webconsole*
4. Copie el archivo *.zip* en la carpeta *help*.
5. Extraiga los contenidos del archivo *.zip* , por ejemplo, *en-US.zip*, a una carpeta con el mismo nombre, en este caso **en-US** de manera que la estructura de la carpeta se vea de esta manera:*%ProgramFiles%\Apache Software Foundation\[Tomcat folder]\webapps\era\webconsole\help\en-US*

Ahora puede abrir su consola web ESET PROTECT, seleccione el idioma e inicie sesión. ESET PROTECT On-Prem Para acceder a la ayuda fuera de línea, haga clic en **Ayuda** en la esquina superior derecha y luego en **Tema actual**: **Ayuda**.

> Puede agregar la ayuda fuera de línea en varios idiomas si lo desea mediante los mismos pasos anteriores.

> Si su equipo o dispositivo móvil desde el cual accede a la consola web ESET PROTECT no tiene una conexión a Internet, deberá cambiar la configuración de la consola web ESET PROTECT para **forzar la Ayuda de ESET PROTECT On-Prem fuera de línea** para abrirla de manera predeterminada (en lugar de la Ayuda en línea). Para hacerlo, siga las instrucciones debajo de la tabla.

Instrucciones de configuración de ayuda fuera de línea para Linux

1. Descargue un archivo *.tar* al hacer clic en el código de idiomas de la siguiente tabla para descargar la ayuda fuera de línea para su ESET PROTECT On-Prem en el idioma que desee.
2. Guarde el archivo *.tar* (por ejemplo, a una unidad flash USB).
3. Abra el terminal y vaya a */usr/share/tomcat/webapps/era/webconsole*
4. Cree una nueva carpeta llamada *ayuda* mediante la ejecución del comando `mkdir help`.
5. En la carpeta *help*, cree una nueva carpeta de idioma con el mismo nombre que el archivo *.tar*, por ejemplo: ejecute el comando `mkdir en-US` en inglés.
6. Copie el archivo *.tar* en la carpeta de idioma (por ejemplo, */usr/share/tomcat/webapps/era/webconsole/help/en-US*) y extráigalo, por ejemplo, al ejecutar el comando `tar -xvf en-US.tar`.

Ahora puede abrir su consola web ESET PROTECT, seleccione el idioma e inicie sesión. ESET PROTECT On-Prem Para acceder a la ayuda fuera de línea, haga clic en **Ayuda** en la esquina superior derecha y luego en **Tema actual**: **Ayuda**.

Para actualizar la Ayuda sin conexión después de migrar desde una versión anterior, elimine la carpeta de ayuda existente (*...webapps\era\webconsole\help*) y cree una nueva en la misma ubicación durante el paso 3 del procedimiento que se muestra más arriba. Continúe de forma normal luego de reemplazar la carpeta.

Puede agregar la ayuda fuera de línea en varios idiomas si lo desea mediante los mismos pasos anteriores.

Si su equipo o dispositivo móvil desde el cual accede a la consola web ESET PROTECT no tiene una conexión a Internet, deberá cambiar la configuración de la consola web ESET PROTECT para **forzar la Ayuda de ESET PROTECT On-Prem fuera de línea** para abrirla de manera predeterminada (en lugar de la Ayuda en línea). Para hacerlo, siga las instrucciones debajo de la tabla.

Idioma compatible	Ayuda HTML fuera de línea .zip	Ayuda HTML fuera de línea .tar
English	en-US.zip	en-US.tar
Árabe	ar-EG.zip	ar-EG.tar
Chino simplificado	zh-CN.zip	zh-CN.tar
Chino tradicional	zh-TW.zip	zh-TW.tar
Croata	hr-HR.zip	hr-HR.tar
Checo	cs-CZ.zip	cs-CZ.tar
Francés	fr-FR.zip	fr-FR.tar
Francés (Canadá)	fr-CA.zip	fr-CA.tar
Alemán	de-DE.zip	de-DE.tar
Griego	el-GR.zip	el-GR.tar
Italiano	it-IT.zip	it-IT.tar
Japonés	ja-JP.zip	ja-JP.tar
Coreano	ko-KR.zip	ko-KR.tar
Polaco	pl-PL.zip	pl-PL.tar
Portugués (Brasil)	pt-BR.zip	pt-BR.tar
Ruso	ru-RU.zip	ru-RU.tar
Español	es-ES.zip	es-ES.tar
Español latinoamericano	es-CL.zip	es-CL.tar
Eslovaco	sk-SK.zip	sk-SK.tar
Turco	tr-TR.zip	tr-TR.tar

Idioma compatible	Ayuda HTML fuera de línea .zip	Ayuda HTML fuera de línea .tar
Ucraniano	uk-UA. zip	uk-UA. tar

Forzar la ayuda fuera de línea en Windows

1. **Abra** `C:\Program Files\Apache Software Foundation\[carpeta Tomcat]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties` en un editor de texto.
2. **Encuentre** la línea que dice `help_show_online=true`, cambie el valor de esta configuración a `false` y guarde los cambios.
3. **Reinicie** el servicio Tomcat dentro de los servicios o mediante la línea de comando.

ESET PROTECT On-Prem Para acceder a la ayuda fuera de línea, haga clic en **Ayuda** en la esquina superior derecha y luego en **Tema actual: Ayuda**. Se visualizará la ventana de ayuda correspondiente a la página actual.

Forzar la ayuda fuera de línea en Linux

1. **Abra el archivo de configuración** `/usr/share/tomcat/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties` en un editor de texto (por ejemplo, `nano`).
2. **Encuentre** la línea que dice `help_show_online=true`, cambie el valor de esta configuración a `false` y guarde los cambios.
3. Detenga el servicio `tomcat`, ejecute el comando `tomcat stop`.
4. Inicie el servicio `tomcat`, ejecute el comando `tomcat start`.

ESET PROTECT On-Prem Para acceder a la ayuda fuera de línea, haga clic en **Ayuda** en la esquina superior derecha y luego en **Tema actual: Ayuda**. Se visualizará la ventana de ayuda correspondiente a la página actual.

Nuevas características en ESET PROTECT On-Prem

ESET LiveGuard Advanced informe de comportamiento

A modo de preparación para entregar nuevos informes de comportamiento más completos para nuestros clientes de EDR, hemos agregado la opción de descargar informes de comportamiento generados por ESET LiveGuard Advanced. Obtener más información

Una nueva tarea del cliente que busca actualizaciones del producto

Esta tarea del cliente comprueba la disponibilidad de una nueva versión del producto. Si se encuentra una, se descargará y comenzará el proceso de instalación. Obtener más información

Reglas de tiempo para grupos dinámicos

Hemos introducido la opción de incluir reglas de tiempo como criterios adicionales para las plantillas de grupos dinámicos. Cuando se configuren reglas de tiempo, los equipos solo se colocarán en grupos dinámicos durante el periodo de tiempo especificado. Obtener más información

Cambio de nombre del producto

El nombre del producto se ha cambiado de ESET PROTECT a ESET PROTECT On-Prem y hay algunos cambios adicionales relacionados con el nombre del producto incluidos en esta versión.

Otras mejoras y correcciones de errores

Averigüe qué más se ha mejorado en el registro de cambios.

Registro de cambios

Consulte también:
- Consulte la lista de todas las versiones de componentes ESET PROTECT
- ESET PROTECT On-Prem problemas conocidos
- Política sobre el fin de ciclo de vida de ESET para productos empresariales

Herramientas independientes

Mirror Tool

Build version 1.0.1560.0 (Windows), 1.0.2481.0 (Linux)
Released: June 27, 2023

- FIXED: Filtering ESET Management Agent packages by Agent versions defined in *.json filter
- FIXED: A potential security vulnerability

Build version 1.0.1421.0 (Windows), 1.0.2346.0 (Linux)
Released: November 8, 2022

Build version 1.0.1383 (Windows), 1.0.2310 (Linux)
Released: April 28, 2022

- FIXED: MirrorTool downloads ESET Endpoint 6 modules from the ESET Endpoint 6.6 folder, allowing updates of newer ESET Endpoint 6 versions and using DLL modules
- FIXED: MirrorTool fails with "--mirrorFileFormat dll" on ESET Endpoint 6
- FIXED: Mirror chain linking fails with: Error: GetFile: Host 'update.eset.com' not found [error code: 20002]
- FIXED: MirrorTool v1.0.2226.0 ignores proxy setting for downloading product list

ESET Bridge (replaces Apache HTTP Proxy in ESET PROTECT 10 and later)

Vea la Ayuda en línea de ESET Bridge.

Apache HTTP Proxy (applies to ESET PROTECT 9.1 and earlier)

Build version: 2.4.56.64
Released: March 30, 2023

- FIXED: Apache HTTP Proxy (v 2.4.55.58) replaced with the latest version (v 2.4.56.64) due to discovered vulnerabilities in the earlier version. This release fixes vulnerability CVE-2023-25690

Build version: 2.4.55.58
Released: March 2, 2023

- FIXED: Apache HTTP Proxy (v 2.4.54.25) was replaced with the latest version (v 2.4.55.58) due to discovered vulnerabilities in the earlier version. This release updates OpenSSL from version 1.1.1q to version 1.1.1t to fix security vulnerabilities

Build version: 2.4.54.25
Released: September 26, 2022

- FIXED: Apache HTTP Proxy (v 2.4.54.0) replaced with the latest version (v 2.4.54.25) due to discovered vulnerabilities in the earlier version

Build version: 2.4.54.0
Released: August 3, 2022

- FIXED: Apache HTTP Proxy (v 2.4.53.1) replaced with the latest version (v 2.4.54.0) due to discovered vulnerabilities in the earlier version

Build version: 2.4.53.1
Released: July 7, 2022

- FIXED: Apache HTTP Proxy replaced with the latest version due to discovered vulnerabilities in the earlier version

Build version: 2.4.53.0
Released: March 31, 2022

- FIXED: Apache HTTP Proxy replaced with the latest version due to discovered vulnerabilities in the earlier version

Navegadores web, productos de seguridad ESET, e idiomas compatibles

Los siguientes sistemas operativos son compatibles con ESET PROTECT On-Prem:

- 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.

Últimas versiones de productos ESET que se pueden administrar mediante ESET PROTECT On-Prem 11.0

Las versiones del producto de seguridad de ESET que se enumeran a continuación se pueden administrar con la versión del agente ESET Management 11.0 y posteriores.
Se recomienda usar la versión más reciente del agente ESET Management para administrar completamente la versión más reciente de los productos de seguridad ESET y sus características. Si utiliza una versión del agente ESET Management anterior a la versión del servidor ESET PROTECT, es posible que algunas de las funciones de administración más recientes no estén disponibles.
Las versiones anteriores de los productos de seguridad de ESET a las que se muestran en la tabla siguiente no se pueden administrar con ESET PROTECT On-Prem 11.0.
Para obtener más información sobre la compatibilidad, visite la Política de Fin de Vida Útil para productos comerciales de ESET.

Producto	Versión del producto
ESET Endpoint Security para Windows	7.3, 8.x, 9.x, 10.x
ESET Endpoint Antivirus para Windows	7.3, 8.x, 9.x, 10.x
ESET Endpoint Security para macOS	6.10+
ESET Endpoint Antivirus para macOS	Superiores a 6.10
ESET Endpoint Security para Android	3.3+
ESET Server Security para Microsoft Windows Server (anteriormente ESET File Security para Microsoft Windows Server)	7.3, 8.x, 9.x, 10.x, 11.x
ESET Mail Security para Microsoft Exchange Server	7.3, 8.x, 9.x, 10.x, 11.x
ESET Security para Microsoft SharePoint Server	7.3, 8.x, 9.x, 10.x, 11.x
ESET Mail Security para IBM Domino	7.3, 8.x, 9.x, 10.x

Producto	Versión del producto
ESET Server Security para Linux (anteriormente ESET File Security para Linux)	7.2, 8.1, 9.x, 10.x
ESET Endpoint Antivirus para Linux	7.1, 8.1, 9.x, 10.x
ESET LiveGuard Advanced	
ESET Inspect Connector	1.8+
ESET Full Disk Encryption para Windows	
ESET Full Disk Encryption para macOS	

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
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 On-Prem (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

Idioma	Código
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.

Introducción a ESET PROTECT On-Prem

ESET PROTECT On-Prem puede administrarse y configurarse a través de la consola web de ESET PROTECT. Después de instalarESET PROTECT On-Prem o implementar VA ESET PROTECT correctamente, podrá conectarse al servidor ESET PROTECT a través de la consola web ESET PROTECT.

Después de haber instalado correctamente ESET PROTECT On-Prem, puede comenzar con la configuración.

Primeros pasos luego de la instalación de ESET PROTECT Server

1.En primer lugar, abra la Consola web ESET PROTECT en su navegador web e inicie sesión.

2.Agregue su(s) licencia(s) a ESET PROTECT On-Prem.

3.Asigne equipos cliente, servidores y dispositivos móviles de su red a la estructura de ESET PROTECT On-Prem.

4.Asigne la política incorporada **Informe de aplicaciones: informar todas las aplicaciones instaladas** a todos los equipos.

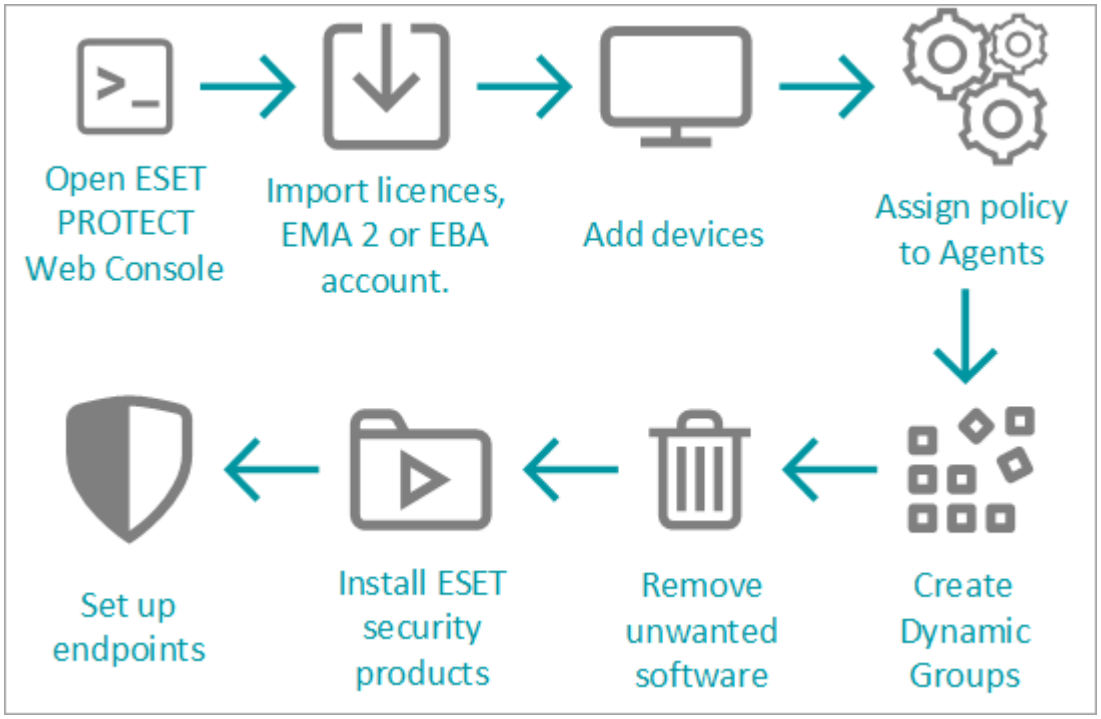
5.Cree un grupo dinámico para todos los equipos con productos de inicio de ESET.

6.Quite las aplicaciones antivirus de terceros mediante el uso de la tarea Desinstalación de software.

7.Instale los productos de seguridad de ESET con la tarea Instalación de software (excepto que haya instalado el agente por medio del Instalador todo en uno).

8.Asigne una política con configuración recomendada a cada equipo que tenga productos de seguridad

ESET instalados. Por ejemplo, para equipos Windows con ESET Endpoint, asigne la política incorporada **Antivirus - Seguridad máxima - recomendado**. Consulte también Cómo gestionar productos Endpoint desde ESET PROTECT On-Prem.



Pasos adicionales recomendados

• Le recomendamos que se familiarice con la consola web de ESET PROTECT, ya que es la interfaz que utilizará para administrar los productos de seguridad ESET.

• Durante la instalación creó una cuenta de administrador predeterminada. Le recomendamos que guarde las credenciales de la cuenta de administrador en un lugar seguro y cree una cuenta nueva para administrar los clientes y configurar sus permisos.

No recomendamos usar la cuenta predeterminada del **Administrador** de ESET PROTECT On-Prem como una cuenta de usuario normal. Sirve como copia de seguridad por si le ocurre algo a las cuentas de usuarios normales o si queda bloqueado, etc. Podrá iniciar sesión con la cuenta del administrador para solucionar dichos problemas.

• Utilice las notificaciones y los informes para controlar el estado de los equipos cliente en su entorno. Por ejemplo, si desea que se le notifique sobre un cierto evento ocurrido o desea ver o descargar un informe.

• Realice una copia de seguridad de su base de datos en forma regular para evitar la pérdida de datos.

• Le recomendamos exportar la autoridad de certificación del servidor y los certificados de pares. Si debe reinstalar el servidor ESET PROTECT, puede usar la AC y los certificados de pares del servidor ESET PROTECT original y no necesita reinstalar los agentes ESET Management en los equipos cliente.

Abrir la Consola web ESET PROTECT.

La consola web ESET PROTECT es la interfaz principal que se usa para comunicarse con el servidor ESET PROTECT. Puede considerarla como un panel de control, un lugar central desde el que puede administrar todas sus

soluciones de seguridad de ESET. Es una interfaz basada en la web a la que se puede acceder mediante un navegador desde cualquier lugar y cualquier dispositivo con acceso a Internet. Puede instalar la consola web de ESET PROTECT en un equipo diferente a donde se ejecuta el servidor de ESET PROTECT.

Hay varias maneras de abrir la Consola web ESET PROTECT:

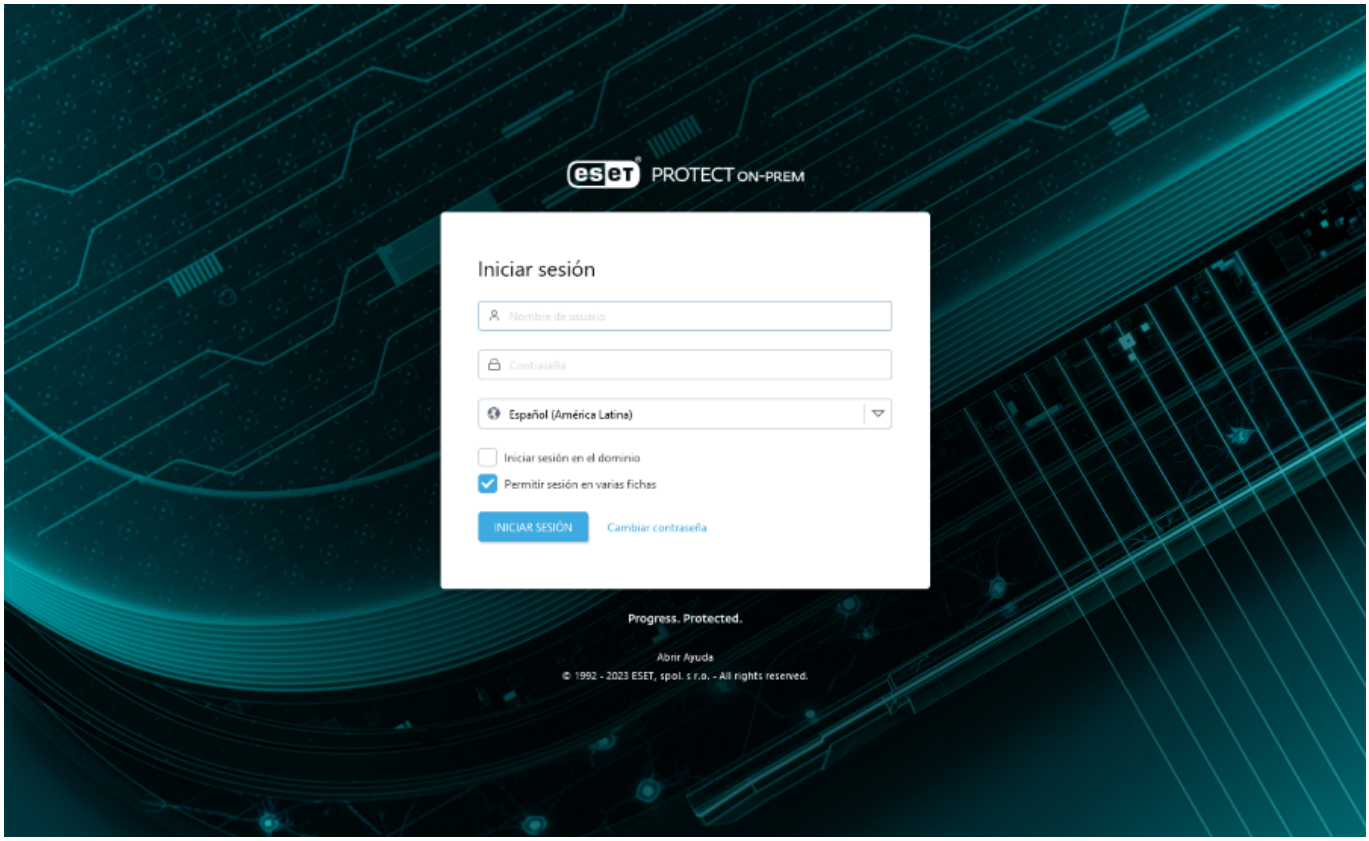
- En su **servidor local** (el equipo que aloja su Consola web) ingrese esta URL en el navegador: https://localhost/era/

- Desde **cualquier lugar con acceso a Internet** a su servidor web, escriba la URL en el siguiente formato: *https://yourservername/era/*
  Sustituya “yourservername” por el nombre o la dirección IP reales de su servidor web.

- Para iniciar sesión en el **aparato virtual ESET PROTECT On-Prem**, use la siguiente URL: *https://[IP address]/*
  Sustituya “[IP address]” por la dirección IP de su ESET PROTECT On-Prem VM.

- En su servidor local (la máquina que aloja su consola web), haga clic en **Inicio** > **Todos los programas** > **ESET** > **ESET PROTECT On-Prem** > **consola web ESET PROTECT**, se abrirá una pantalla de inicio de sesión en su navegador predeterminado. Esto no se aplica al aparato virtual ESET PROTECT.

Cuando el servidor web (que ejecuta la consola web ESET PROTECT) está activo, se visualiza la siguiente pantalla de inicio de sesión.



Si este es su primer inicio de sesión, proporcione las credenciales que escribió durante el proceso de instalación (siga su escenario de instalación: Instalador todo en uno en Windows, implementación del aparato virtual, otros escenarios de instalación).

El usuario predeterminado de la consola web es el **administrador**. Para obtener más detalles acerca de esta pantalla, consulte Pantalla de inicio de sesión de la consola web.

> Si tiene problemas para iniciar sesión y recibe mensajes de error cuando intenta hacerlo, consulte Solución de problemas de la Consola web.

Consola web ESET PROTECT

La consola web ESET PROTECT es la interfaz principal que se usa para comunicarse con el servidor ESET PROTECT. Puede pensar en ella como un panel de control, un lugar central donde puede administrar todas sus soluciones de seguridad de ESET. Está basada en la web y se puede acceder mediante un navegador (consulte Navegadores web compatibles) desde cualquier lugar y cualquier dispositivo con acceso a Internet. Cuando inicie sesión en la consola web por primera vez, aparecerá el Recorrido por ESET PROTECT On-Prem.

En la disposición estándar de la consola web ESET PROTECT:

- El usuario actual siempre se muestra en la esquina superior derecha, donde se realiza la cuenta hacia atrás correspondiente al tiempo de espera de su sesión. Puede hacer clic en **Cerrar sesión** para cerrar sesión en cualquier momento. Cuando expira una sesión (por la inactividad del usuario), debe iniciar sesión nuevamente. Para cambiar la Configuración del usuario, haga clic en su nombre de usuario en la esquina superior derecha de la consola web ESET PROTECT.

- Se puede acceder al Menú principal desde la izquierda en todo momento, excepto mientras se utiliza un asistente. Haga clic en para expandir el menú en el lateral izquierdo de la pantalla. Para colapsarlo, haga clic en **Colapsar**.

- Si necesita ayudar al trabajar con ESET PROTECT On-Prem, haga clic en el ícono **Ayuda** en la esquina superior derecha y haga clic en**Tema actual - Ayuda**. Se mostrará la ventana de ayuda de la página actual. Haga clic en **Ayuda** > sobre para ver la versión ESET PROTECT On-Prem y otros detalles.

- Puede usar la herramienta Búsqueda en la parte superior de la consola web de ESET PROTECT. Escriba al menos 3 y un máximo de 30 caracteres en el campo de búsqueda para buscar en estas categorías: **Nombre del equipo**, **Descripción del equipo**, **Dirección IP del equipo**, **Nombre de grupo estático**, **Causa de detección**, **Usuarios del equipo**, **Nombre de usuario nativo** y **Nombre de usuario de dominio**. Puede encontrar un máximo de 3 resultados en cada categoría. Haga clic en el resultado para ver los detalles y haga clic en **Todos los resultados** para ver la sección específica de la consola web con el filtro de categoría aplicado.

- Haga clic en el botón **Vínculos rápidos** para ver el menú:

Vínculos rápidos
Configurar Equipos
• Agregar equipo
• Añadir dispositivo móvil
• Implementar el agente
• Agregar usuario al equipo
Administrar equipos

Vínculos rápidos
• Crear tarea de cliente
• Crear nueva política
• Asignar política
Revisar estado
• Generar informe
• Componentes del servidor

• En la parte superior izquierda de la pantalla, junto al nombre de ESET PROTECT On-Prem, verá el ícono de navegación del producto que lo ayuda a desplazarse entre ESET PROTECT On-Prem y sus otros productos: ESET Inspect On-Prem, ESET Business Account, ESET MSP Administrator (podrá ver los respectivos productivos según la licencia y los derechos de acceso que tenga)

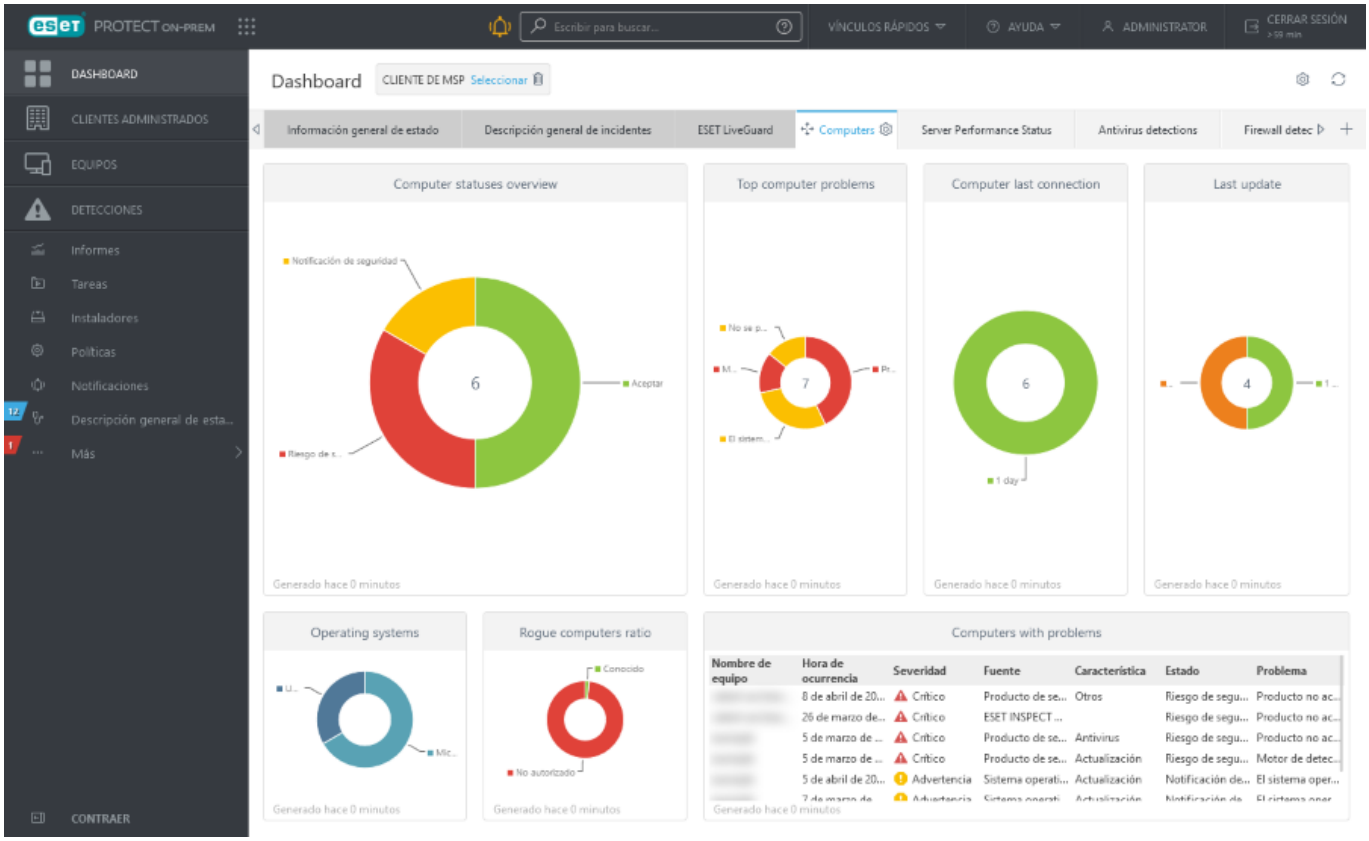
• El ícono de **engranaje** siempre se refiere al menú contextual.

• Haga clic en **Actualizar** para volver a cargar/actualizar la información mostrada.

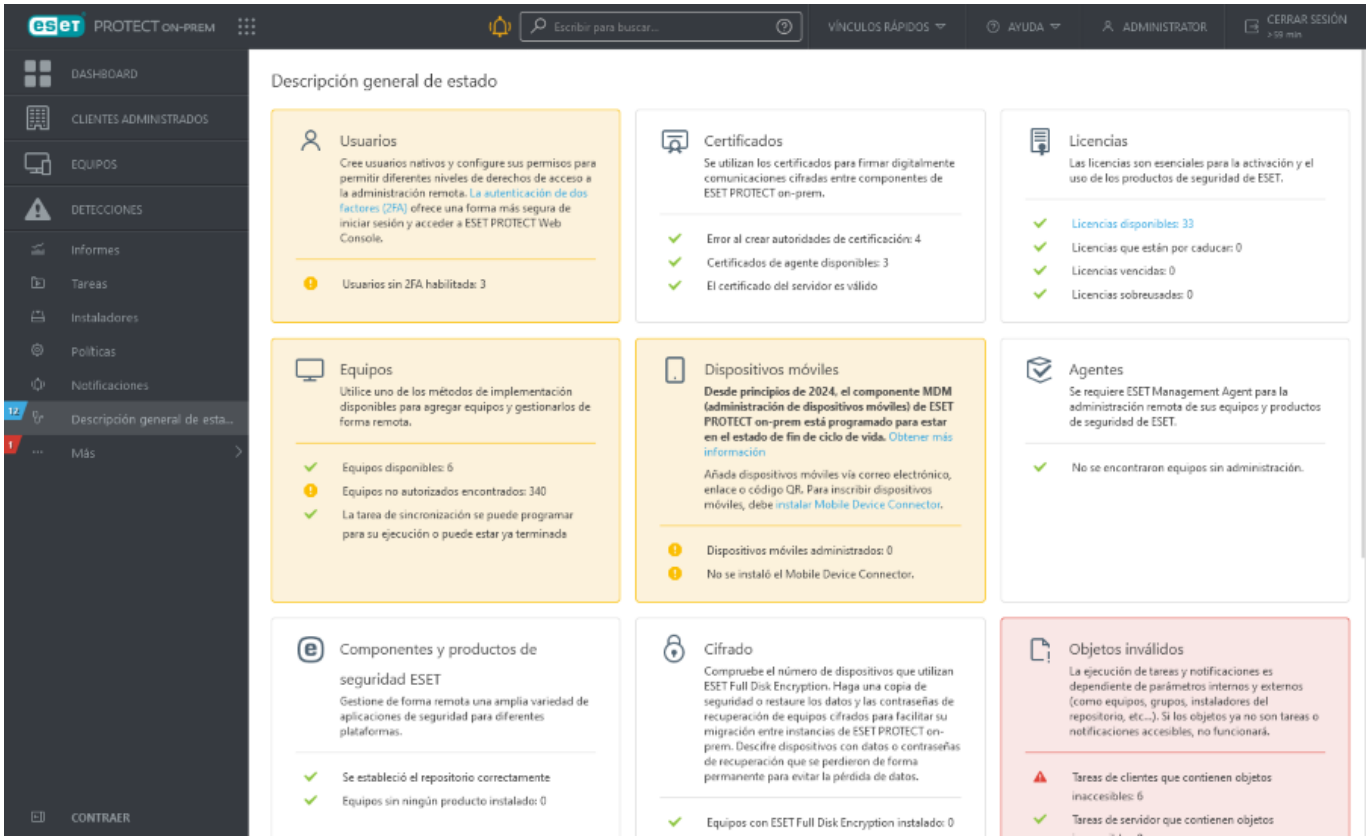
• Los botones de la parte inferior de la página son exclusivos para cada sección y función y se describen en detalle en sus respectivos capítulos.

• La consola web de ESET PROTECT informa al administrador sobre los Acuerdos de licencia de usuario final actualizados de los productos de seguridad ESET administrados

• Haga clic en el logotipo de ESET PROTECT On-Prem para abrir la pantalla Panel de información.

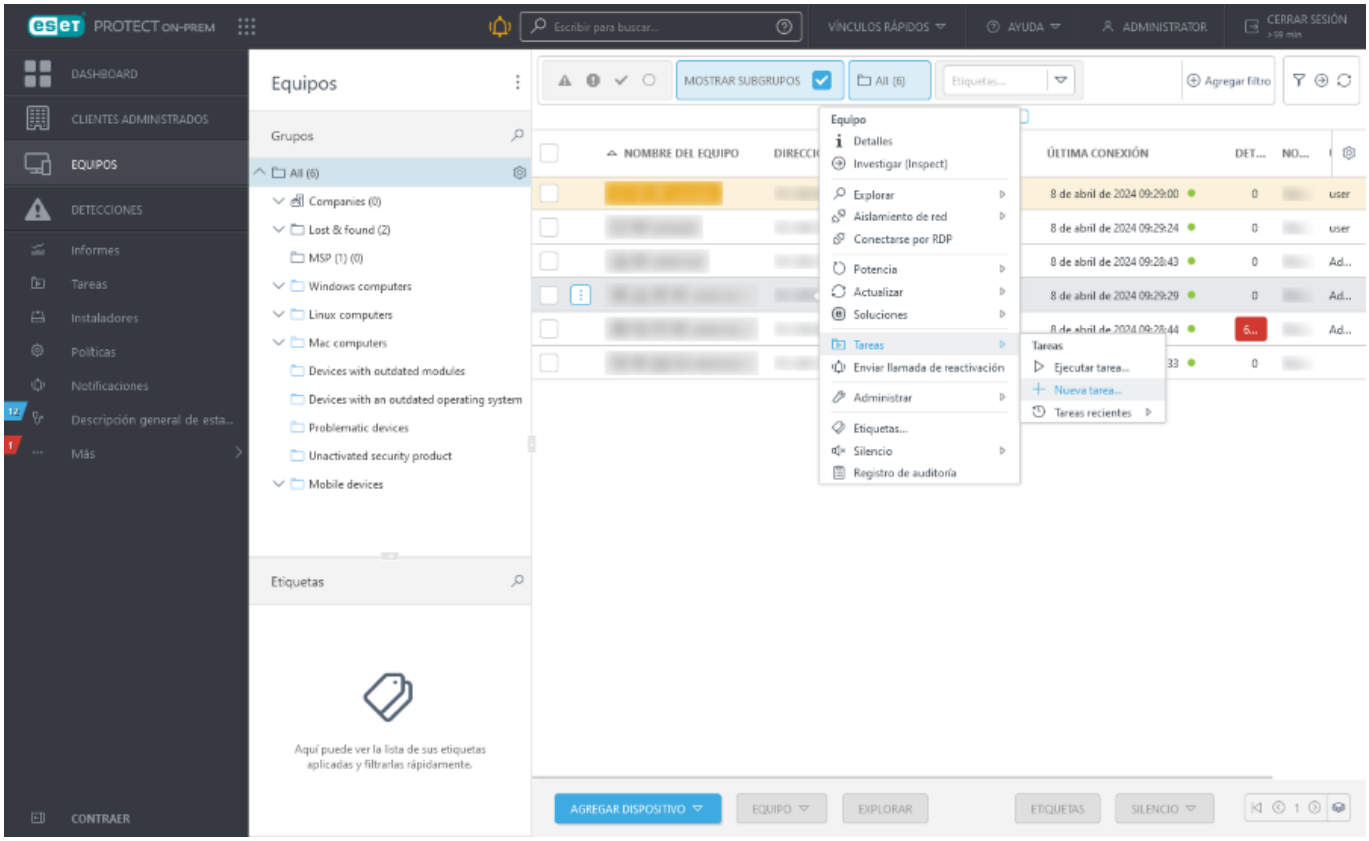


En **Información general del estado** se muestra cómo sacar el mayor provecho de ESET PROTECT On-Prem. Esto lo guiará por los pasos recomendados.



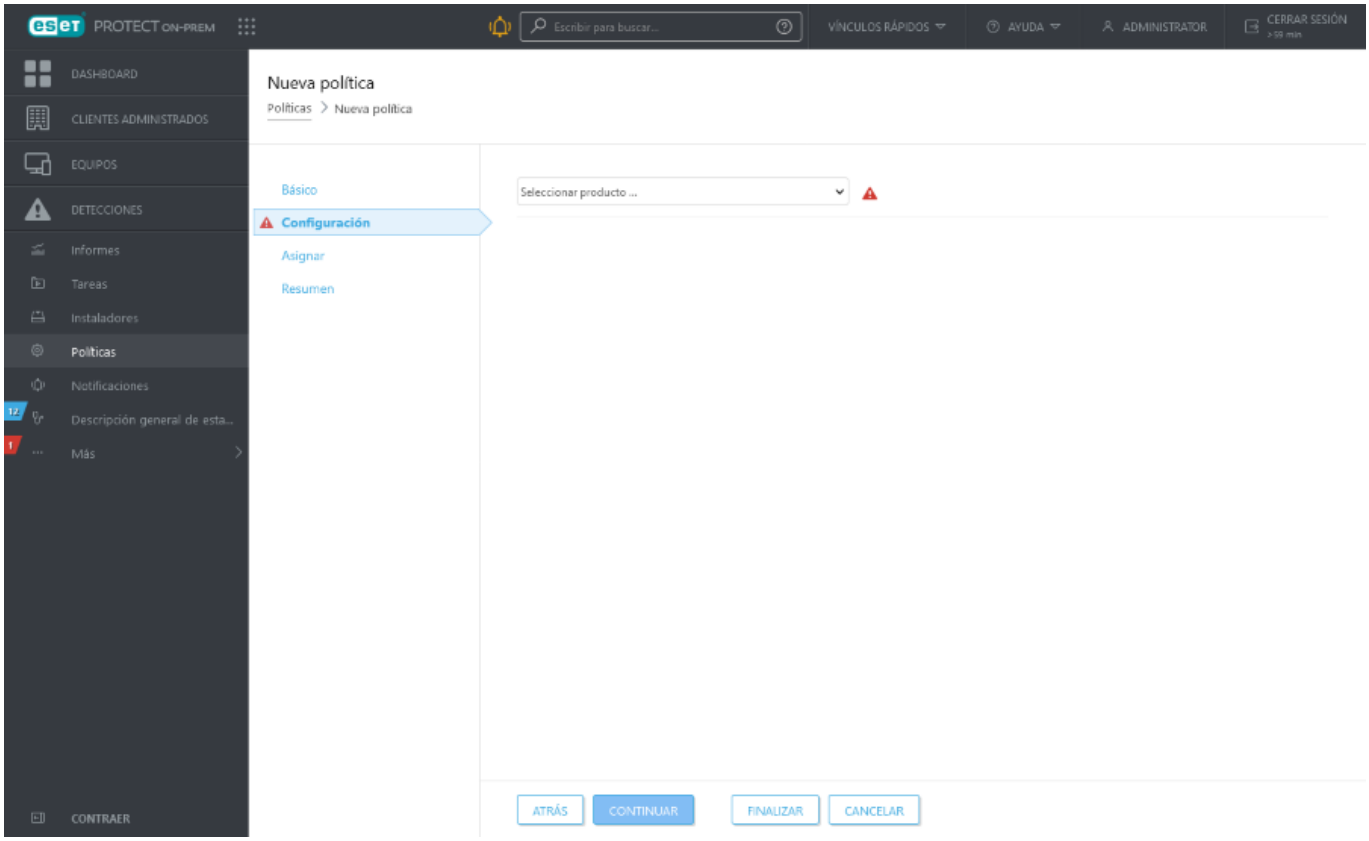
Las pantallas con árbol tienen controles específicos. El árbol mismo se encuentra a la izquierda con las acciones debajo. Haga clic en un elemento del árbol para visualizar las opciones.

Las tablas le permiten administrar las unidades desde las filas de forma individual o en un grupo (cuando se seleccionan más filas). Haga clic en una fila para visualizar las opciones de las unidades en dicha fila. Los datos de las tablas se pueden filtrar y ordenar.



Puede editar objetos de ESET PROTECT On-Prem utilizando asistentes. Todos los asistentes comparten los siguientes comportamientos:

- Los pasos están orientados en forma vertical desde arriba hacia abajo
- Puede volver a cualquier paso anterior en cualquier momento
- La configuración requerida (obligatoria) siempre se marca con un signo de exclamación rojo junto a la sección y la respectiva configuración.
- Los datos de entrada no válidos se marcan cuando mueve el cursor a un nuevo campo, y también se marca el paso del asistente que contiene datos no válidos
- **Finalizar** no está disponible hasta que todos los datos de entrada sean correctos.



Pantalla de inicio de sesión

El usuario necesita credenciales de inicio de sesión (nombre de usuario y contraseña) para iniciar sesión en la consola web.

Para iniciar sesión como un usuario de dominio (miembro del grupo de seguridad de dominio asignado), seleccione la casilla de verificación situada junto a **Iniciar sesión en el dominio**. El formato de inicio de sesión depende de su tipo de dominio:

- Windows Active Directory: `DOMAIN\username`
- Linux y ESET PROTECT aparato virtual LDAP: `username@FULL.DOMAIN.NAME`

> Si tiene problemas para iniciar sesión y recibe mensajes de error cuando intenta hacerlo, consulte Solución de problemas de la Consola web para obtener sugerencias para resolverlos.

Puede **seleccionar su idioma** al hacer clic en la flecha desplegable junto al idioma seleccionado actualmente; para obtener información, consulte nuestro Artículo de la base de conocimiento.

> 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 On-Prem y su idioma no puede cambiarse.

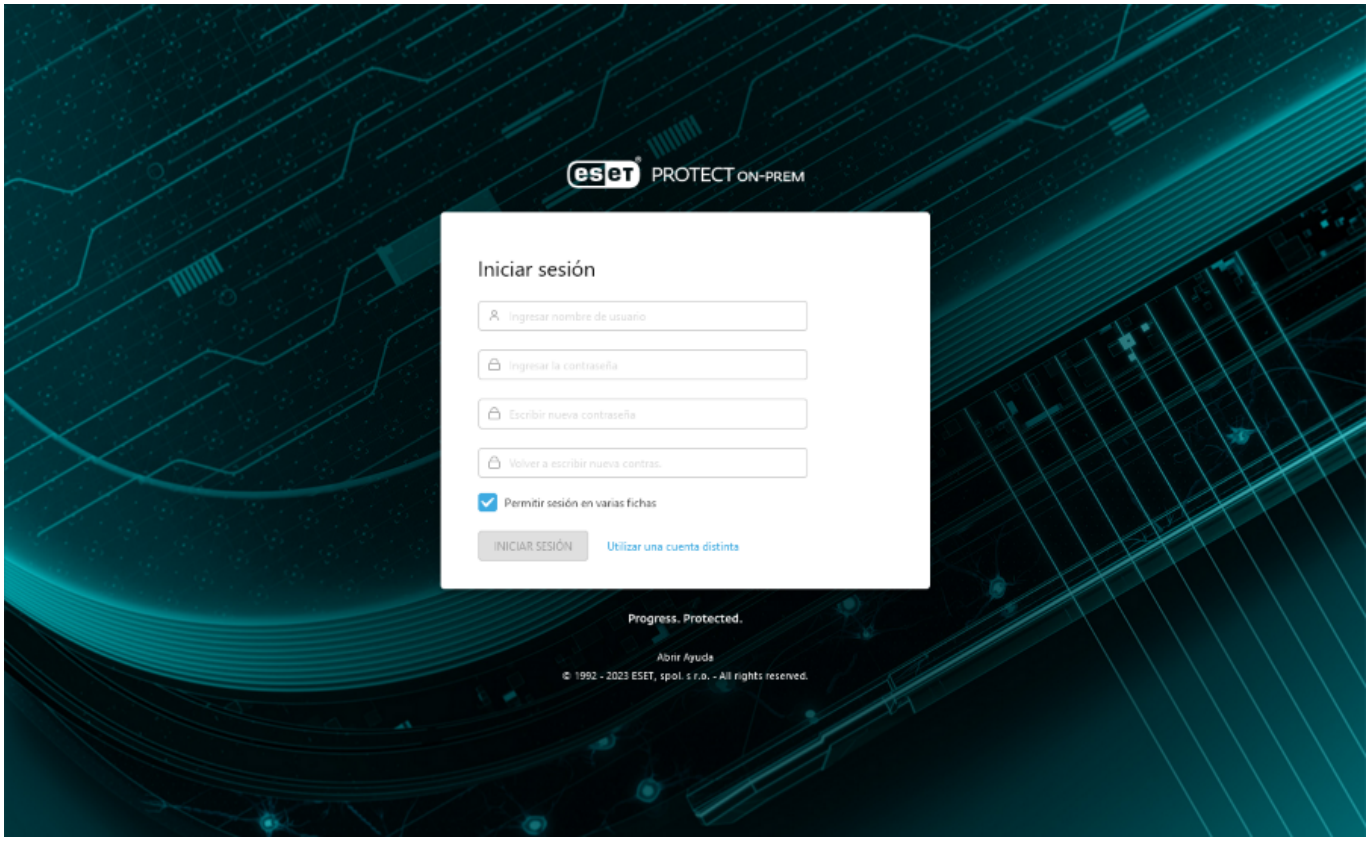
Permitir sesión en múltiples pestañas: se puede abrir la consola web en múltiples pestañas de un solo navegador.

- Si se selecciona la casilla de verificación, cada pestaña con una sesión abierta de la consola web en un navegador se conectará a la misma sesión. Si se abre una nueva pestaña, todas las demás pestañas

conectadas con la misma configuración se conectarán a esta nueva sesión. Si se cierra la sesión en una de las pestañas, también se cerrará la sesión de todas las demás.

• Si no se selecciona la casilla de verificación, cada nueva pestaña abre una nueva sesión independiente de la consola web ESET PROTECT.

Cambiar contraseña/Usar cuenta diferente: le permite cambiar la contraseña o volver a la pantalla de inicio de sesión.



Administración de sesión y medidas de seguridad:

Bloqueo de la dirección IP de inicio de sesión

Después de 10 intentos de inicio de sesión sin éxito desde la misma dirección IP (por ejemplo, utilizando credenciales de inicio de sesión incorrectas), no se podrán hacer más intentos de inicio de sesión desde esta dirección IP temporalmente. Esto se indica mediante el mensaje de error: **Error en el inicio de sesión: Usuario bloqueado. Vuelva a intentarlo más tarde.** Después de 10 minutos, inicie sesión con las credenciales correctas. El bloqueo de la dirección IP para intentos de inicio de sesión no afecta las sesiones existentes.

Bloqueo de la dirección por ID de sesión incorrecta

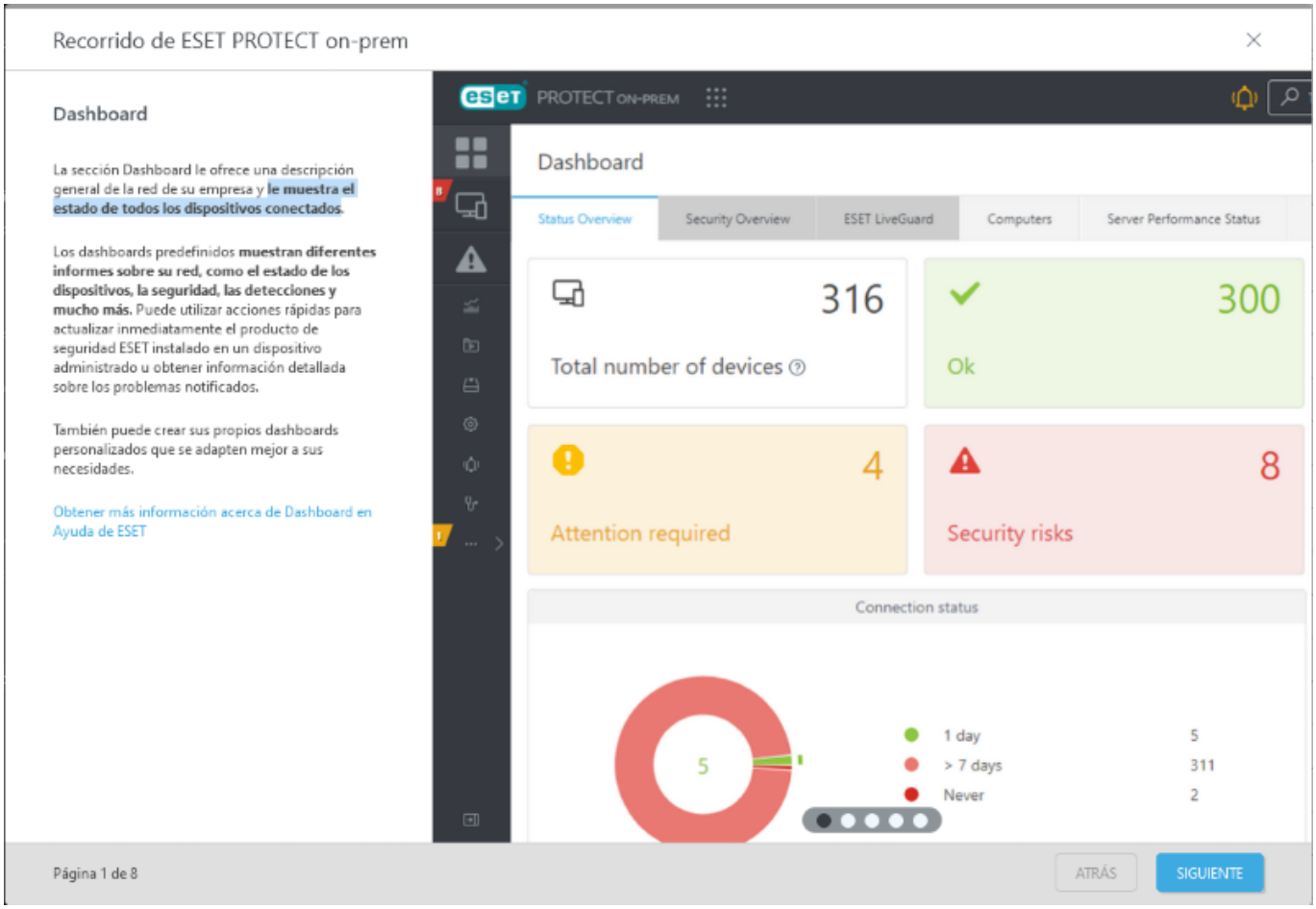
Luego de usar una ID de sesión no válida 15 veces desde una misma dirección IP, se bloquean todas las conexiones posteriores desde esta dirección IP por aproximadamente 15 minutos. No se tienen en cuenta las ID de sesión vencida. Si existe una ID de sesión vencida en el navegador, no se la considera un ataque. El bloqueo de la dirección IP de 15 minutos se aplica a todas las acciones (incluidas las solicitudes válidas). Se puede liberar el bloqueo mediante el reinicio de la consola web (servicio `tomcat`).

Recorrido por ESET PROTECT On-Prem

Cuando inicie sesión en la consola web por primera vez, aparecerá el **Recorrido por ESET PROTECT On-Prem**.

Este asistente le dará una explicación básica de las secciones importantes de la consola web ESET PROTECT, el agente ESET Management y los productos de seguridad ESET. Podrá leer información sobre Dashboards, Equipos, Detecciones, Tareas, Políticas, Notificaciones y las Actualizaciones del producto automáticas.

Haga clic en **Proteger dispositivos** en el último paso del **Recorrido por ESET PROTECT On-Prem** para instalar agentes ESET Management en sus equipos de red. También puede crear el instalador del agente sin usar el asistente haciendo clic en **Instaladores** > Crear instalador.



Haga clic en **X** si no desea utilizar el **Recorrido por ESET PROTECT On-Prem**. Se abrirá la consola web de ESET PROTECT. El **recorrido por ESET PROTECT On-Prem** no aparecerá la próxima vez que ingrese a la consola web de ESET PROTECT.

Puede volver a ver el **Recorrido por ESET PROTECT On-Prem** haciendo clic en ? **Ayuda** > **Recorrido por ESET PROTECT On-Prem**.

> Después del primer inicio de sesión en la consola web de ESET PROTECT, recomendamos que ejecute la tarea de cliente Actualización del sistema operativo en el equipo donde está instalado ESET PROTECT On-Prem para garantizar que el sistema operativo esté actualizado (por cuestiones de seguridad y rendimiento).

Configuración del usuario

En esta sección podrá personalizar la configuración del usuario. Haga clic en **Cuenta de usuario** en la esquina superior derecha de la Consola web ESET PROTECT (a la izquierda del botón **Cerrar sesión**) para visualizar todos los usuarios activos. Puede iniciar sesión en la consola web ESET PROTECT desde diferentes exploradores web, equipos o dispositivos móviles a la vez. Aquí verá todas sus sesiones.

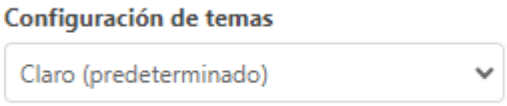
Este ajuste solo aplica al usuario que tiene la sesión iniciada.

Configuración de temas

Puede seleccionar la configuración de tema que desea que muestre ESET PROTECT On-Prem:

- **Claro (predeterminado)**
- **Oscuro**
- **Tema del sistema operativo**: el tema de color de la consola web coincide con el tema de color del sistema operativo.

Seleccione el tema del menú desplegable:



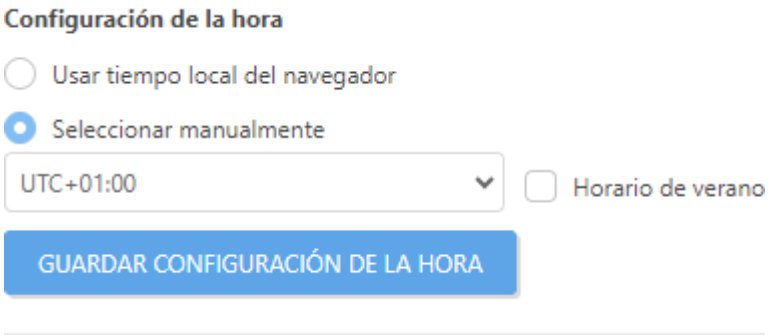
La pantalla permanece en el tema seleccionado tras cerrar sesión en Web Console e iniciar sesión de nuevo.

Configuración de la hora

Cada usuario puede tener su configuración de huso horario preferida para la consola web ESET PROTECT. Los ajustes de horario específicos del usuario se aplican para dicho usuario sin importar desde dónde ingresan a la consola web ESET PROTECT.

Toda la información se almacena internamente en ESET PROTECT On-Prem mediante el estándar UTC (Horario universal coordinado). El horario UTC se convierte automáticamente al huso horario usado por la consola web ESET PROTECT (considera el horario de verano). La consola web ESET PROTECT muestra el horario local del sistema donde se ejecuta la consola web ESET PROTECT (no el horario UTC interno). Si lo desea, puede anular la configuración manualmente para configurar el horario que se muestra en la consola web ESET PROTECT.

Si desea anular la configuración predeterminada **Usar la hora local del navegador**, puede seleccionar la opción **Seleccionar manualmente**, especificar el huso horario de la consola manualmente y decidir si habilitar o no el horario de verano.

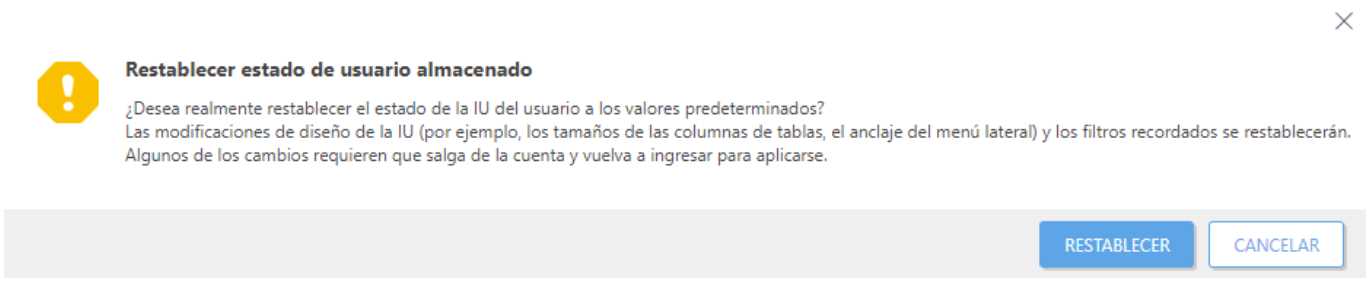


En algunos casos, la opción de usar una zona horaria diferente estará disponible. Al configurar un desencadenador, la zona horaria de la Consola web de ESET PROTECT se usa de forma predeterminada. De forma alternativa, puede seleccionar la casilla de verificación **Usar la hora local de destino** para usar la zona horaria local del dispositivo de destino, en lugar de la zona horaria de la consola web de ESET PROTECT para el desencadenador.

Haga clic en el **Guardar configuración de la hora** para confirmar los cambios.

Estado de usuario almacenado

Puede restablecer el estado de la IU del usuario almacenado a los valores predeterminados al hacer clic en **Restablecer estado de usuario almacenado**. Comprende el recorrido por ESET PROTECT On-Prem, tamaños de columnas de tablas, filtros recordados, menú lateral anclado, etc.



Dispositivos recordados

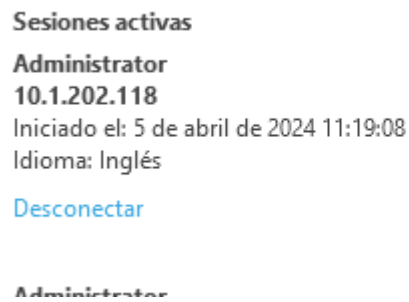
Olvidar dispositivos recordados: requiere la autenticación de dos factores en los dispositivos recordados del usuario actual.

Sesiones activas

La información sobre todas las sesiones activas del usuario actual contiene:

- Nombre de usuario actual.
- Detalles del equipo que accede a la consola web: navegador web y sistema operativo.
- Dirección IP de un equipo o dispositivo cliente desde el cual está conectado el usuario a la consola web de ESET PROTECT. La dirección IP de un servidor web que ejecuta la consola web de ESET PROTECT se muestra entre paréntesis. Si la consola web ESET PROTECT se está ejecutando en el mismo equipo que el servidor ESET PROTECT, se mostrará **via 127.0.0.1**.
- Fecha y hora en que el usuario inició sesión.

- Idioma seleccionado para la consola web ESET PROTECT.



La sesión actual se denomina **Esta sesión**. Si desea desconectar una sesión activa, haga clic en **Desconectar**.

Personalización del diseño y de los filtros

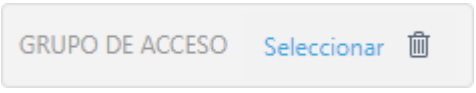
La consola web de ESET PROTECT le permite personalizar el diseño de los elementos que se muestran en las principales secciones (por ejemplo, **equipos**, **tareas**, etc.) de varias maneras:

Agregar filtro y filtros preestablecidos

Para agregar criterios de filtrado, haga clic en **Agregar filtro** y seleccione los elementos de la lista. Escriba las cadenas de búsqueda o seleccione los elementos del menú desplegable en los campos de filtrado y pulse **Intro**. Los filtros activos están resaltados en azul.

Es posible guardar los filtros en su perfil de usuario para usarlos nuevamente en el futuro. Haga clic en el ícono de **Preestablecidos** para administrar los conjuntos de filtros:

Filtrar conjuntos	Los filtros guardados. Haga clic en uno de ellos para aplicarlo. El filtro aplicado se identifica con una marca de verificación. Seleccione **Incluir columnas visibles, clasificación y paginado** para guardar estos parámetros en la configuración preestablecida.
Guardar conjunto de filtros	Guarde la configuración actual del filtro como nueva configuración preestablecida. Una vez que la configuración preestablecida está guardada, ya no podrá editar la configuración del filtro en la configuración preestablecida.
Administrar conjuntos de filtros	Quitar o cambiar el nombre a las configuraciones preestablecidas. Haga clic en **Guardar** para aplicar los cambios a las configuraciones preestablecidas.
Borrar valores de filtros	Haga clic para quitar únicamente los valores actuales de los filtros seleccionados. Las configuraciones preestablecidas guardadas se mantendrán sin cambios.
Quitar filtros	Haga clic para quitar los filtros seleccionados. Las configuraciones preestablecidas guardadas se mantendrán sin cambios.
Quitar filtros sin uso	Quitar los campos de filtros sin valor.
Restablecer filtros predeterminados	Restablezca el panel de filtros y muestre los filtros predeterminados.



El botón de filtro **Grupo de acceso** le permite a los usuarios seleccionar un grupo estático y filtrar los objetos mostrados en función del grupo en el que se encuentran.

Puede usar etiquetas para filtrar los elementos mostrados.

Disposición del panel lateral

Haga clic en el ícono ⋮ junto al nombre de la sección y ajuste el diseño del panel lateral desde el menú de contexto (las opciones disponibles pueden variar en función del diseño actual):

- **Ocultar panel lateral**
- **Mostrar panel lateral**
- **Grupos**
- **Grupos y etiquetas**
- **Etiquetas**

Si los grupos están visibles, puede seleccionar también una de estas opciones:

- **Ampliar todo**
- **Colapsar todo**

Administrar la tabla principal

Para reordenar una columna, desplace el mouse sobre el ícono ✥, ubicado junto al nombre de la columna, y arrastre y suelte la columna. Consulte también **Editar columnas** a continuación.

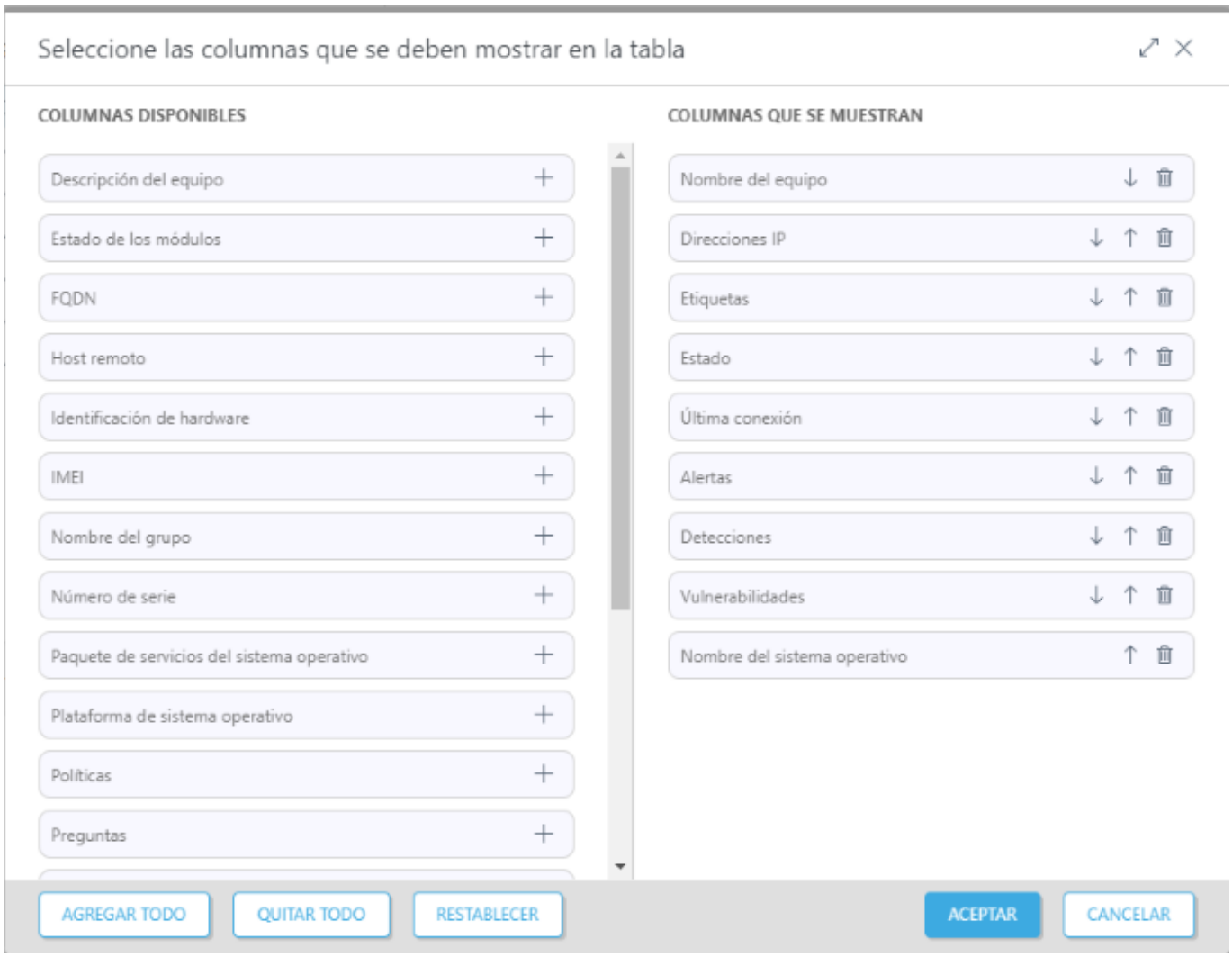
Para ordenar por una sola columna, haga clic en el encabezado de la columna y ordene las filas de la tabla en función de los datos de la columna seleccionada.

- La clasificación por orden ascendente (A–Z, 0–9) o descendente (Z–A, 9–0) se genera con uno o dos clics.
- Una vez aplicada la clasificación, una flecha pequeña antes del encabezado de la columna indica el comportamiento de clasificación.
- Consulte también varias clasificaciones a continuación.

Haga clic en el ícono del engranaje ⚙ para administrar la tabla principal:

Acciones

- **Editar columnas** –Utilice el asistente para ajustar (+ agregar, 🗑 quitar, ↓ ↑ reordenar) las columnas exhibidas. También puede arrastrar y soltar para ajustar las columnas. Haga clic en **Restablecer** para restablecer las columnas de la tabla a su estado predeterminado (las columnas disponibles predeterminadas en el orden predeterminado).



• **Columnas de ajuste automático**: ajusta el ancho de las columnas de manera automática.

• **Mostrar tiempo relativo/Mostrar tiempo absoluto**: cambie el formato de visualización de los datos de tiempo en la tabla principal (por ejemplo, **Última conexión** en **ordenadores** u **Ocurrido** en **Detecciones**). Cuando active **Mostrar tiempo relativo**, sitúe el ratón sobre el tiempo relativo en la tabla para ver el tiempo absoluto.

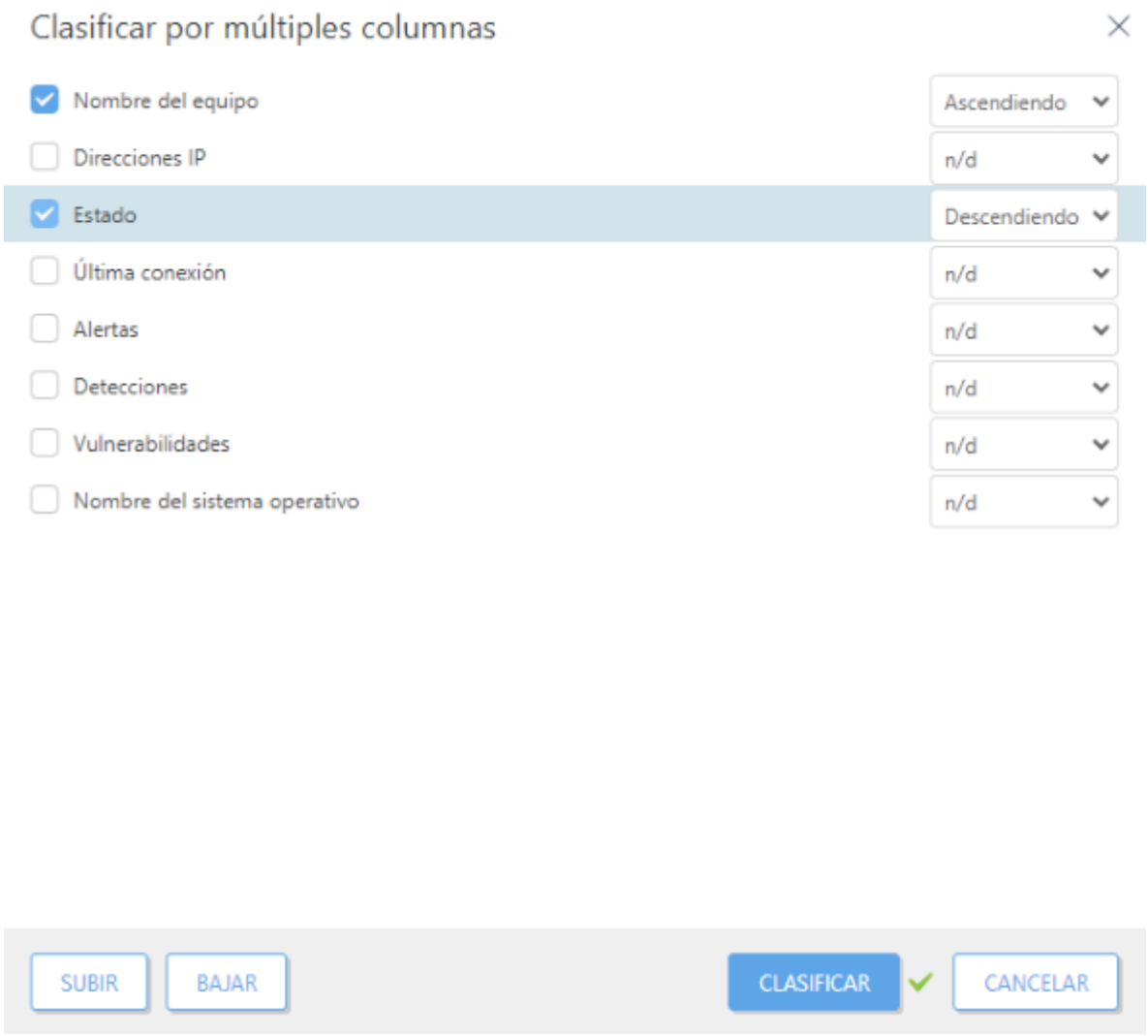
Clasificación de tablas

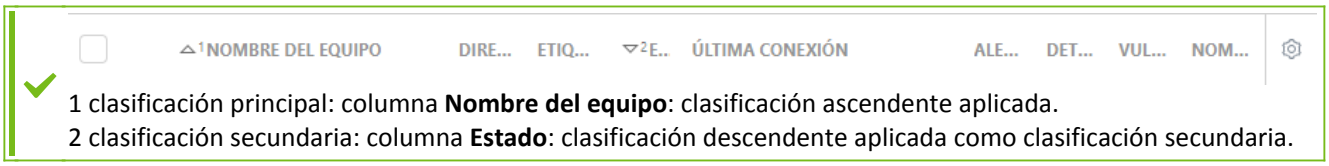
• **Restablecer clasificación**: restablece la clasificación de la columna.

• **Clasificación múltiple**: puede clasificar los datos de una tabla al seleccionar varias columnas (hasta 4). Para cada una de las columnas puede modificar su:

oprioridad de clasificación: cambie el orden de las columnas al hacer clic en el botón **Subir** o **Bajar** (la primera columna: clasificación principal; la segunda columna, clasificación secundaria, etc.). Tras aplicar varias clasificaciones, los números de índice aparecerán antes que los encabezados de columna para indicar la prioridad de clasificación.

ocomportamiento de clasificación: seleccione **Ascendente** o **Descendente** en el menú desplegable.





Informes

- **Exportar tabla como**: exporta la tabla como un informe en el formato deseado. Puede seleccionar entre *.pdf* o *.csv*. CSV es apto únicamente para datos de tablas y usa ; (punto y coma) como delimitador Si descarga un informe de CSV y ve los números en una columna en la que esperaba ver texto, le recomendamos descargar un informe de PDF para ver los valores de texto.

- **Guardar una plantilla de informe**: crea una nueva plantilla de informe a partir de la tabla.

Etiquetas

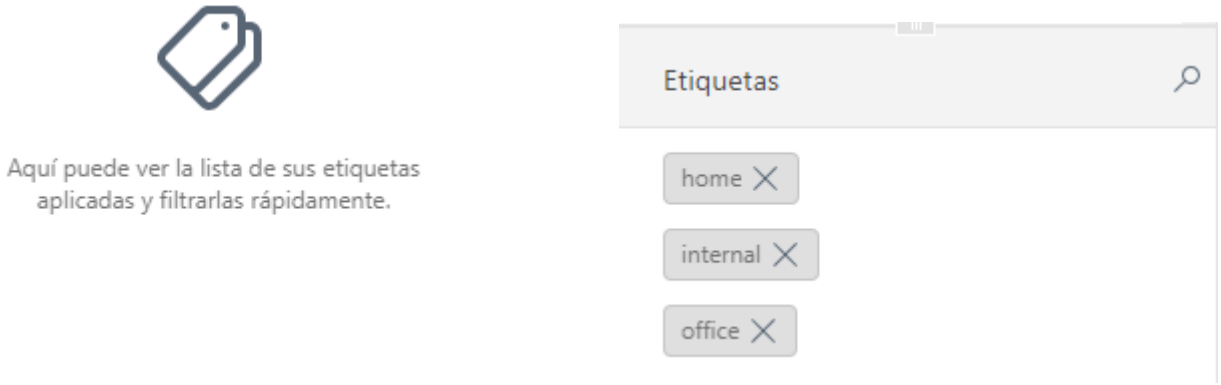
ESET PROTECT On-Prem permite marcar todos los objetos relevantes (equipos, detecciones, tareas, instaladores, políticas, notificaciones, licencias, etc.) con etiquetas definidas por el usuario, que pueden usarse además para lograr una mejor capacidad de búsqueda y filtrado. El etiquetado se encuentra integrado de manera nativa en las principales pantallas de la consola web de ESET PROTECT.

Las etiquetas son palabras clave definidas por el usuario (rótulos) que pueden agregarse a distintos objetos de manera tal que resulte más fácil agruparlos, filtrarlos y buscarlos. Por ejemplo, puede asignar una etiqueta 'VIP' a los activos relevantes e identificar con rapidez todos los objetos asociados con ella.

Puede crear y asignar etiquetas en forma manual. Los objetos de MSP se etiquetan de manera automática con el nombre del cliente.

Panel de etiquetas

Puede ver las etiquetas existentes en la sección **Etiquetas**, ubicada en el extremo inferior izquierdo de la pantalla del menú de la consola web de ESET PROTECT:



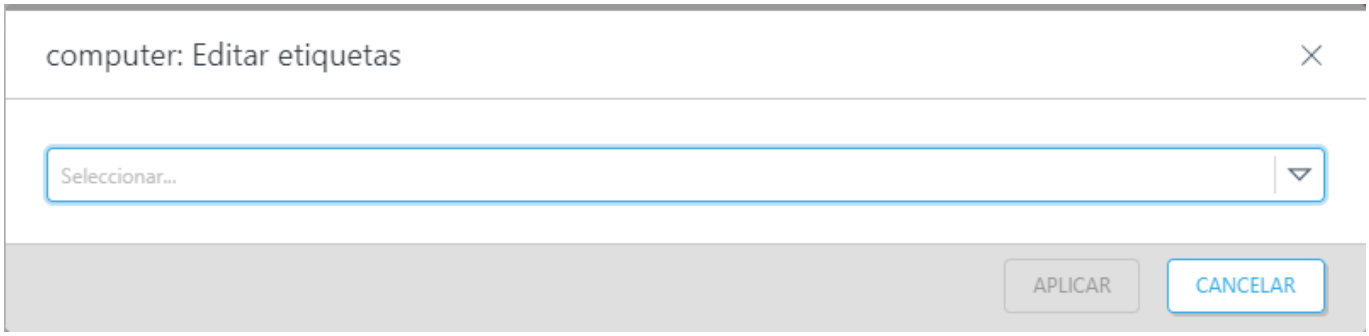
Permisos para la administración de etiquetas

Para administrar las etiquetas de un objeto, el usuario debe contar con los derechos de acceso de **uso** (conjunto de permisos asignados) en relación con el objeto. Los usuarios adicionales pueden administrar etiquetas, es decir, otro usuario puede quitar una etiqueta que usted haya creado.

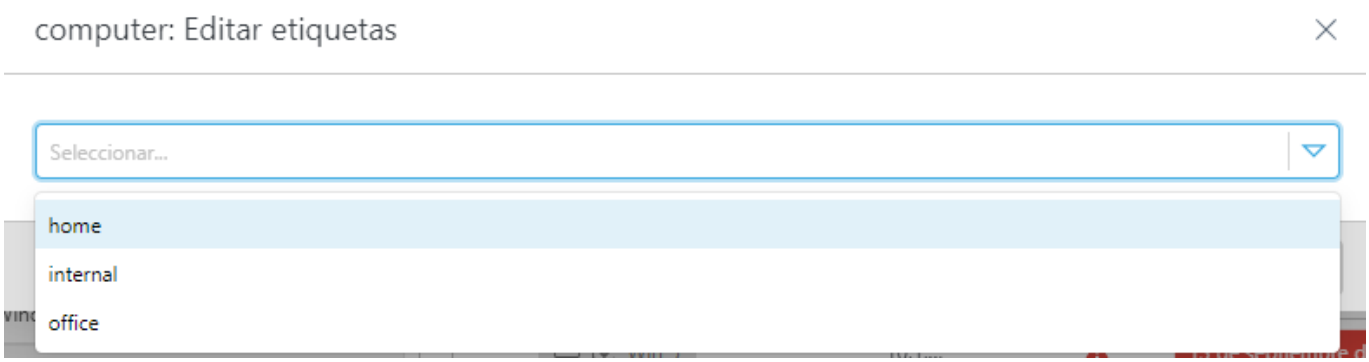
Asignar etiquetas

Puede asignar etiquetas a uno o más objetos.

Para asignar etiquetas, seleccione la(s) casilla(s) de verificación ubicada(s) junto al(a los) objeto(s) y haga clic en **Equipo** > **Etiquetas**:

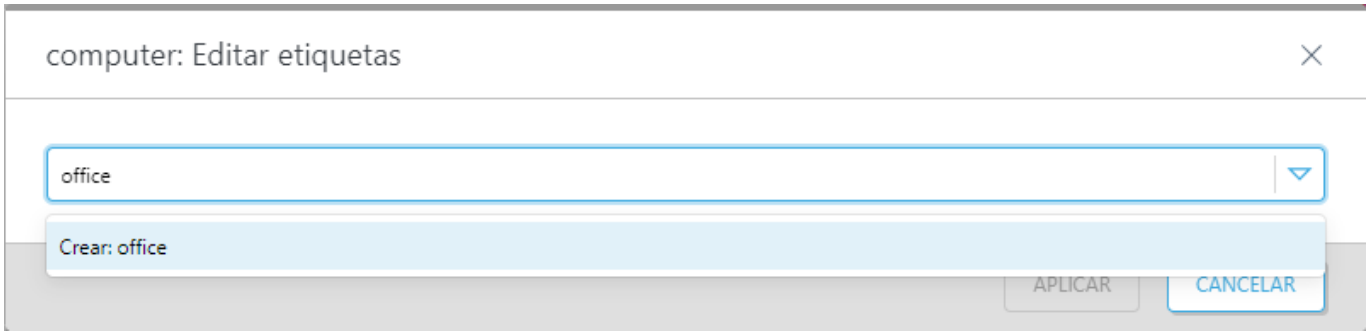


Para asignar etiquetas existentes, haga clic en el campo de escritura de una etiqueta de la lista y, luego, en **Aplicar**.



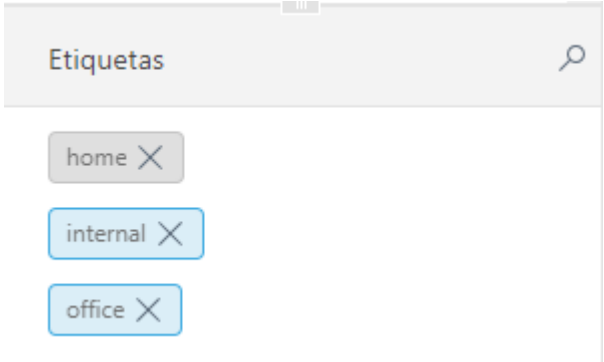
Crear una nueva etiqueta

Para crear una nueva etiqueta, escriba el nombre de la etiqueta, seleccione **Crear "nombre_etiqueta"** y, luego, haga clic en **Aplicar**. No puede editar el nombre de una etiqueta existente.



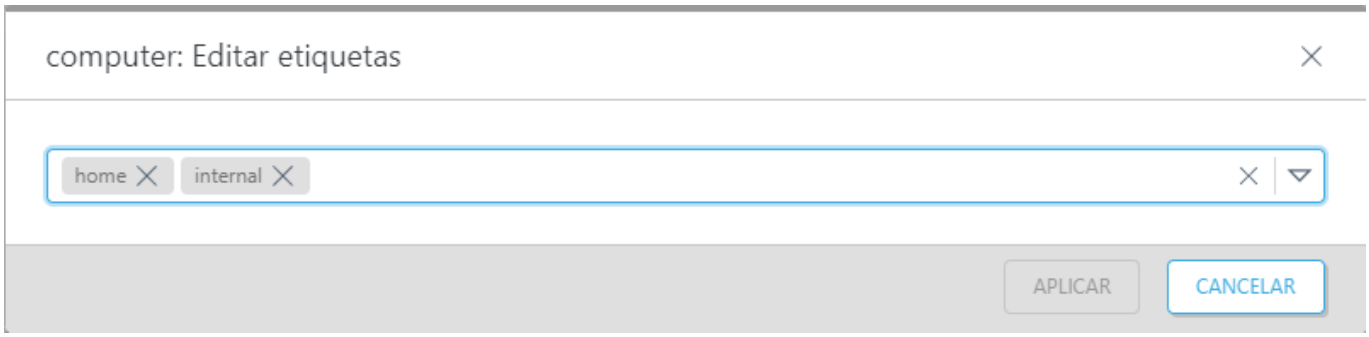
Filtrar los objetos por etiqueta

Haga clic en una etiqueta para aplicar un filtro a los objetos de la lista. Las etiquetas seleccionadas se muestran en azul.



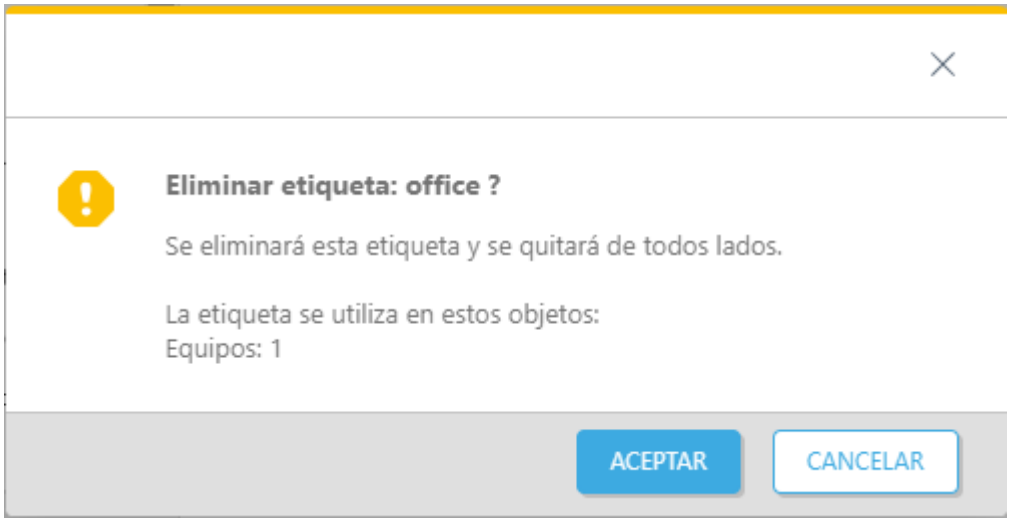
Desasignar etiquetas

Para asignar etiquetas, seleccione la(s) casilla(s) de verificación ubicada(s) junto al(a los) objeto(s) y haga clic en **Equipo** > **Etiquetas**. Para quitar la etiqueta, haga clic en la X y, luego, en **Aplicar**.



Quitar una etiqueta

Para quitar una etiqueta, desplace el mouse sobre la etiqueta en el panel **Etiquetas**, haga clic en el ícono del engranaje y, luego, en **Aceptar** para confirmar que desea quitar la etiqueta de todos los objetos en la consola web de ESET PROTECT.



Importar CSV

Se puede importar una lista con el archivo *.csv* personalizado con una estructura adecuada. Se usa esta función en varios menús de la interfaz de usuario de ESET PROTECT On-Prem. Dependiendo de qué se debe importar, las columnas cambian.

1.Haga clic en **Importar CSV**.

2.**Carga**: haga clic en el botón **Elegir archivo**, busque el archivo *.csv* (con la codificación UTF-8) que desea cargar y, luego, haga clic en **Cargar**.

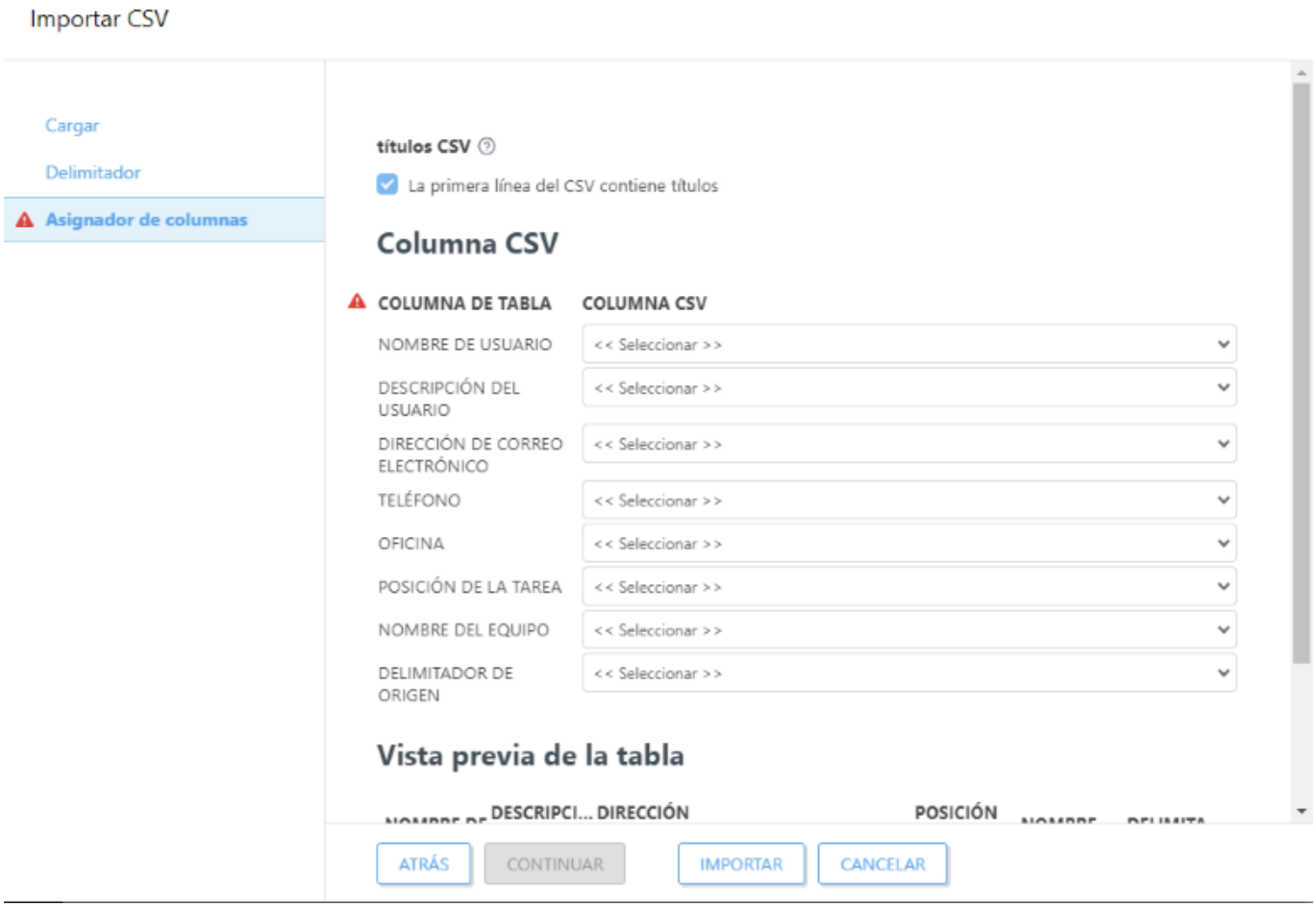
3.**Delimitador**: un delimitador es un carácter que se usa para separar cadenas de texto. Seleccione el delimitador adecuado (**punto y coma**, **coma**, **espacio**, **tabulación**, **punto**, **barra vertical**) para que coincida con el que usa su archivo *.csv*. Si su archivo *.csv* usa un carácter diferente como delimitador, seleccione la casilla de verificación junto a **Otro** e ingrese el carácter. **Vista preliminar de datos** muestra los contenidos

de su archivo *.csv* que puede ayudarle a identificar el tipo de delimitador que se usa para separar cadenas.

4.**Asignador de columnas**: después de cargar y analizar el archivo *.csv*, debe asignar cada columna deseada en el archivo *.csv* importado a la columna de ESET PROTECT On-Prem que se **muestra en la tabla. Use las listas desplegables para seleccionar la columna CSV que debe estar asociada con una columna de ESET PROTECT On-Prem específica. Si su archivo** *.csv* **no tiene una fila de encabezado**, quite la selección de **Primera línea de CSV que contiene encabezados**.

5.Consulte la **Vista preliminar de la tabla** para asegurarse de que la asignación de columna esté configurada correctamente y que la operación de importación funcionará como desea.

6.Después de asignar satisfactoriamente cada una de las columnas y de que la vista previa de la tabla luzca correcta, haga clic en el botón Después de asignar satisfactoriamente cada una de las columnas y la vista previa de la tabla se vea correcta, haga clic en **Importar** para iniciar la operación.



Resolución de problemas - Consola web

La tabla que se encuentra a continuación le dará una idea de los mensajes y estados de error más comunes de inicio de sesión en la Consola web, su significado y algunos pasos adicionales para la solución de problemas:

Mensaje de error	Posibles causas
Error en el inicio de sesión: Nombre de usuario o contraseña no válidos	Asegúrese que ingresó el nombre de usuario y la contraseña correctamente. Puede restablecer la contraseña de la consola web de ESET PROTECT.

Mensaje de error	Posibles causas
⚠ Error en el inicio de sesión: Se produjo un error en la conexión con estado 'No conectado'	Verifique si el servicio del servidor ESET PROTECT y el servicio de su base de datos se encuentran activos; consulte el Artículo de la base de conocimiento para obtener instrucciones paso a paso.
⚠ Error en el inicio de sesión: Usuario bloqueado. Vuelva a intentarlo más tarde.	Después de 10 intentos de inicio de sesión sin éxito desde la misma dirección IP (por ejemplo, utilizando credenciales de inicio de sesión incorrectas), no se podrán hacer más intentos de inicio de sesión desde esta dirección IP temporalmente. Después de 10 minutos, inicie sesión con las credenciales correctas.
⚠ Error en el inicio de sesión: Error de comunicación	Verifique que el servicio del servidor ESET PROTECT esté funcionando y el servicio de Apache Tomcat esté activo y funcione correctamente. Revise los archivos de registro de Apache Tomcat. Lea nuestro artículo de la base de conocimientos para obtener más información sobre este tema.
⚠ Error en el inicio de sesión: Límite de tiempo de la conexión	Verifique la conexión de red y la configuración del firewall para asegurarse de que la consola web ESET PROTECT pueda llegar al servidor ESET PROTECT. Además, el servidor ESET PROTECT podría estar sobrecargado, intente reiniciar el equipo. Este problema también puede ocurrir si usa versiones distintas de la consola web ESET PROTECT y el servidor ESET PROTECT.
⚠ Error en el inicio de sesión: El usuario no tiene derechos de acceso asignados	El usuario no tiene derechos de acceso asignados. Inicie sesión como administrador y edite la cuenta del usuario, para que tenga asignado al menos un Conjunto de permisos.
⚠ Error en el inicio de sesión: Error de análisis de respuesta	La versión de la Consola web y el servidor ESET PROTECT no son compatibles. Esto puede ocurrir durante o después de la actualización de componentes. Si el problema persiste, implemente la versión correcta de la consola web manualmente.
⚠ Usando conexión cifrada! Configure el servidor web para usar HTTPS	Por motivos de seguridad, le recomendamos configurar la consola web ESET PROTECT para usar HTTPS.
JavaScript está deshabilitado. Habilite JavaScript en su navegador.	Habilite JavaScript o actualice su navegador web.
SEC_ERROR_INADEQUATE_KEY_USAGE (solo Mozilla Firefox).	Mozilla Firefox tiene un almacén de certificados dañados.

Error	Posibles causas
No ve la pantalla de inicio de sesión o la misma parece estar cargando de manera constante.	• Reinicie el servicio ESET PROTECT On-Prem Server. Una vez que el servicio de ESET PROTECT On-Prem Server esté activo y en funcionamiento nuevamente, reinicie el servicio de Apache Tomcat. Luego, la pantalla de inicio de sesión de la Consola web ESET PROTECT se cargará correctamente. Lea también nuestro artículo de la base de conocimiento. • Si Apache Tomcat no puede extraer contenido del archivo *era.war* y la consola web no está accesible, siga los pasos del artículo de la base de conocimiento.
El texto falta en el menú contextual y el menú de **Enlaces rápidos** en la Consola web ESET PROTECT.	Este problema puede ser ocasionado por una extensión del navegador que bloquea los anuncios. Para resolver este problema, deshabilite la extensión del navegador que bloquea los anuncios para la página de la Consola Web ESET PROTECT.

Error	Posibles causas
Luego de iniciar sesión, la consola web no se muestra correctamente (faltan elementos, etc.).	Asegúrese de estar usando un navegador web compatible.

Tras el inicio de sesión, algunas pantallas de la consola web no se cargan.	Si no se cargan algunas de las pantallas de la consola web de ESET PROTECT (p. ej., Equipos), abra el archivo *Tomcat9w.exe* situado en carpeta *C:\Program Files\Apache Software Foundation\[Tomcat]*
	• En la ficha **General**, haga clic en **Detener** para detener el servicio de Apache Tomcat.
	• Seleccione la ficha **Java** y agregue el siguiente código en **Java Options**:
	`-Duser.country=US`
	`-Duser.language=en`
	• En la ficha **General**, haga clic en **Iniciar** para iniciar el servicio de Apache Tomcat.

La consola web tarda mucho tiempo en cargarse. Cuando se carga una gran cantidad de objetos, la consola se bloquea.	La consola web requiere de más memoria para tratar conjuntos de objetos de gran tamaño. Consulte la consola web para configuraciones empresariales.
Algunas pantallas de la consola web no se cargan correctamente y ve un error. Por ejemplo, al editar una política, ve el error: "ERROR WHILE INITIALIZING CONFIGURATION EDITOR.: (TYPEERROR) : ((INTERMEDIATE VALUE)(INTERMEDIATE VALUE) , K).INITCONFIGEDITOR IS NOT A FUNCTION".	Esto sucede si utiliza un proxy inverso que evita que se carguen los módulos de la consola web. Los strings de la URL para los módulos individuales de la consola web (cargados en Apache Tomcat) pueden modificarse de manera dinámica (por ejemplo, luego de `era/webconsole/configEngine/` en `era/webconsole/configEngine/02645EFC6ABCDE2B449042FB8S63FD3/v0.0/css/001_ce.ltr.css`). Para solucionar el problema, asegúrese de configurar correctamente su proxy inverso.
Al importar un archivo grande (más de 20 MB) (por ejemplo, una política), el proceso arroja un error.	El límite de tamaño del archivo para la consola web es de 20 MB. Para cambiarlo, edite el archivo *EraWebServerConfig.properties*, ubicado en la carpeta *[Tomcat folder]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config*. Cambie `file_size_limit=20` por un valor superior. El valor máximo es 250.

i
- Luego de actualizar ESET PROTECT On-Prem, le recomendamos quitar el caché del navegador web y las cookies antes de iniciar sesión en la consola web actualizada.
- Debido a que la consola web usa el protocolo seguro (HTTPS), es posible que obtenga un mensaje en su navegador web con respecto a un certificado de seguridad o a una conexión no confiable (las palabras exactas del mensaje dependen del navegador que use). Esto se debe a que su navegador requiere que verifique la identidad del sitio al que intenta acceder. Haga clic en **Avanzado** > **Continuar hasta [dirección] (no segura)** (Chrome/Edge) o **Avanzado** > **Aceptar el riesgo y continuar** (Firefox) para permitir el acceso a la consola web de ESET PROTECT. Esto solo se aplica cuando intenta acceder a la URL de la Consola web ESET PROTECT. Lea nuestro artículo de la Base de conocimiento para obtener más información sobre cómo configurar la conexión HTTPS/SSL.

Cómo gestionar productos Endpoint desde ESET PROTECT On-Prem

Antes de poder comenzar a administrar ESET Business Solution, necesitará realizar la configuración inicial. Le recomendamos que utilice Descripción general del estado, especialmente si se omitido el recorrido por ESET PROTECT On-Prem. El administrador puede realizar diferentes tareas desde la consola web ESET PROTECT para instalar productos y controlar equipos cliente.

Instalación de agente ESET Management y productos de seguridad Endpoint

ESET PROTECT On-Prem requiere que el agente ESET Management se instale en cada equipo cliente administrado. El agente ESET Management se puede instalar en combinación con su producto de seguridad Endpoint. Antes de la instalación, le recomendamos que importe su licencia en ESET PROTECT On-Prem para que pueda usarse en sus instalaciones posteriores. Existen diversos métodos para instalar el producto Endpoint:

- Use el instalador del producto de seguridad del agente y ESET o ESET Remote Deployment Tool para instalar su producto Endpoint y el agente ESET Management al mismo tiempo.
- Haga clic en un equipo y seleccione **Soluciones** > **Instalar producto de seguridad** para instalar un producto de seguridad ESET en el equipo.
- Instale su producto ESET Endpoint en los clientes donde ya tiene instalado el agente ESET Management mediante una tarea del cliente

Administrar el producto de seguridad Endpoint desde ESET PROTECT On-Prem

Todos los productos de seguridad Endpoint pueden ser administrados desde la consola web ESET PROTECT. Las políticas se utilizan para aplicar configuraciones a equipos únicos o grupos. Por ejemplo, puede crear una política para bloquear el acceso a ciertas ubicaciones web, cambiar la configuración de la sensibilidad de la detecciónde explorador o cambiar todas las demás configuraciones de seguridad de ESET. Las directivas se pueden combinar, tal se muestra en nuestro ejemplo. Las políticas configuradas mediante ESET PROTECT On-Prem no se pueden sobrescribir por un usuario en un equipo cliente. Sin embargo, el administrador puede usar la función sobrescribir para permitir al usuario realizar cambios temporales en un cliente. Una vez finalizados los cambios, puede solicitar la configuración final del cliente y guardarla como una nueva política.

También se pueden utilizar las Tareas para administrar clientes. Las tareas se implementan desde la consola web y el agente ESET Management las ejecuta en el cliente. Las tareas de cliente más comunes para Endpoint de Windows son:

- Actualizar módulos (también actualiza la base de datos de virus)
- Ejecutar análisis a petición
- Ejecutar comandos personalizados
- Solicitar la configuración del equipo y el producto

Actualizar productos de seguridad de ESET

1. Haga clic en **Dashboard** > **Descripción general de estado** > Estado de la versión del componente.

2. Haga clic en el gráfico amarillo o rojo que representa los componentes o aplicaciones desactualizadas y seleccione **Actualizar los componentes de ESET instalados** para iniciar una actualización.

Informar el estado del equipo y obtener información de clientes para ESET PROTECT On-Prem

Cada equipo cliente se conecta a ESET PROTECT On-Prem a través del agente ESET Management. El agente envía toda la información solicitada sobre el equipo cliente y su software al servidor de ESET PROTECT. La conexión entre el agente y el servidor está configurada, por defecto, en 1 minuto, pero puede ser modificada en su política del agente ESET Management. Todos los registros desde Endpoint u otros productos de seguridad ESET se envían al servidor de ESET PROTECT.

En **Equipos**, puede encontrar información sobre los productos ESET instalados y otra información básica sobre el SO de un cliente y su estado. Seleccione un cliente y haga clic en **Detalles**. En la sección **Configuración** de esta ventana, un usuario puede buscar configuraciones anteriores o solicitar la configuración actual. En la sección **Sysinspector** un usuario puede solicitar registros (solo desde equipos con Windows).

La consola web también le permite acceder a una lista de todas las detecciones de los dispositivos cliente. Las detecciones de un dispositivo específico se pueden ver en **Equipos**. Seleccione un cliente y haga clic en **Detalles** > **Detecciones y Cuarentena**. Si el equipo del cliente ejecuta ESET Inspect On-Prem, puede ver y administrar las detecciones de ESET Inspect.

Puede generar informes personalizados a petición o mediante una tarea programada para ver datos sobre los clientes en su red. Las plantillas de informe predefinidas ofrecen una forma rápida de juntar información importante o puede crear sus propias plantillas nuevas. Los ejemplos de informes incluyen información agregada sobre equipos, detecciones, cuarentena y actualizaciones necesarias.

> Un usuario solo puede utilizar plantillas de informe para las que tiene permisos suficientes. Por defecto, todas las plantillas se almacenan en el grupo **Todos**. Un informe solo puede incluir información sobre equipos y eventos dentro del alcance del permiso del usuario. Incluso si una plantilla de informe se comparte entre más usuarios, el informe de cada usuario solo contendrá información sobre los dispositivos sobre los que el usuario tiene permisos. Consulte la lista de permisos para obtener más información sobre los derechos de acceso.

Servicio de notificaciones de empuje de ESET

ESET Push Notification Service (EPNS) sirve para recibir mensajes del servidor de ESET PROTECT si el servidor tiene una notificación para el cliente. La conexión se está ejecutando, por lo que ESET PROTECT On-Prem puede enviar una notificación a un cliente inmediatamente. Cuando la conexión se interrumpe, el cliente intenta volver a conectarse. El motivo principal de la conexión permanente es poner los clientes a disposición de recibir mensajes.

Un usuario de la consola web puede enviar llamadas de activación a través de EPNS entre el servidor de ESET PROTECT y los agentes ESET Management. EL servidor ESET PROTECT envía llamadas de **Wake on LAN**. Puede configurar direcciones multidifusión para **Wake-On-LAN** en **Más** > Configuración.

Detalles de la conexión

Para configurar su red local y permitir comunicaciones con EPNS, tanto el agente ESET Management como el servidor de ESET PROTECT deben poder conectarse al servidor EPNS. Si no puede establecer una conexión con EPNS para sus agentes, solo se verán afectadas las llamadas de Wake-Up. Asegúrese de que su firewall permita la conexión con el servidor EPNS (consulte la tabla siguiente).

Protocolo de seguridad criptográfica	TLS: la versión TLS más reciente compatible con el sistema operativo del equipo administrado
Protocolo	MQTT (protocolo de conexión equipo a equipo)
Puerto	• principal: 8883 • reserva: 443 y el puerto proxy definidos en la política del agente ESET Management Se prefiere el puerto 8883, ya que se trata de un puerto MQTT. El 443 solo es un puerto de reserva y está compartido con otros servicios. Además, un firewall puede anular la conexión en el puerto 443 debido a inactividad o al máximo de conexiones abiertas para el servidor proxy HTTP.
Dirección del host	*epns.eset.com*
Compatibilidad del proxy	Si utiliza el proxy HTTP para reenviar comunicaciones, las llamadas de Wake-Up también se envían a través del proxy HTTP. La autenticación no es compatible. Asegúrese de configurar el proxy HTTP en la política del agente de los equipos a los que quiere enviar las llamadas de Wake-Up. En caso de que el proxy HTTP no funcione, las llamadas de Wake-Up se envían directamente.

Solución de problemas

• Asegúrese de que su firewall está configurado para permitir la conexión a EPNS, (vea los detalles arriba o consulte el artículo de la base de conocimiento).

• Asegúrese de que el agente y el servidor puedan conectarse directamente al servidor EPNS en los puertos 443 y 8883 (para verificar la conexión, use el comando `telnet`).

IEV, clonación y detección de hardware

iESET PROTECT On-Prem es compatible con los entornos VDI, la clonación de máquinas y los sistemas de almacenamiento no persistentes. Esta característica es necesaria para configurar un indicador para el ordenador maestro o para resolver una pregunta que aparezca después de clonar o hacer un cambio de hardware.

• Hasta que la pregunta esté resuelta, el equipo del cliente no podrá replicarse en el servidor de ESET PROTECT. El cliente solo verifica si la pregunta está resuelta.

• Deshabilitar la detección de hardware es irreversible, ¡use esta función con máxima precaución y únicamente en equipos físicos!

• Al resolver múltiples preguntas, use el recuadro Información general de estado - **Preguntas**.

¿Qué sistemas operativos e hipervisores son compatibles?

⚠ Antes de comenzar a usar VDI con ESET PROTECT On-Prem, obtenga más información acerca de las características compatibles y no compatibles con diversos entornos de VDI en nuestro artículo de la base de conocimiento.

• Solo se admiten los sistemas operativos Windows.

• Se puede utilizar ESET Full Disk Encryption en un entorno virtual, pero ESET Full Disk Encryption no se debe clonar

• Los dispositivos móviles administrados a través de MDM no son compatibles

- Los clones enlazados en Virtual Box no pueden distinguirse entre sí
- En casos muy raros, la detección puede ser desactivada automáticamente por ESET PROTECT On-Prem; esto sucede cuando ESET PROTECT On-Prem no es capaz de analizar el hardware de forma fiable
- Consulte la lista de configuraciones compatibles:
  - Citrix PVS 7.15+ con máquinas físicas
  - Citrix PVS 7.15+ con máquinas virtuales en Citrix XenServer 7.15+
  - Citrix PVS 7.15+ y Citrix XenDesktop con Citrix XenServer 7.15+
  - Servicios de creación de máquinas Citrix
  - (sin PVS) Citrix XenDesktop con Citrix XenServer 7.15+
  - VMware Horizon 8.0+ con VMware ESXi
  - Microsoft SCCM (para volver a representar)
- ESET PROTECT On-Prem es compatible con los patrones de nomenclatura de VDI para todos los hipervisores compatibles.

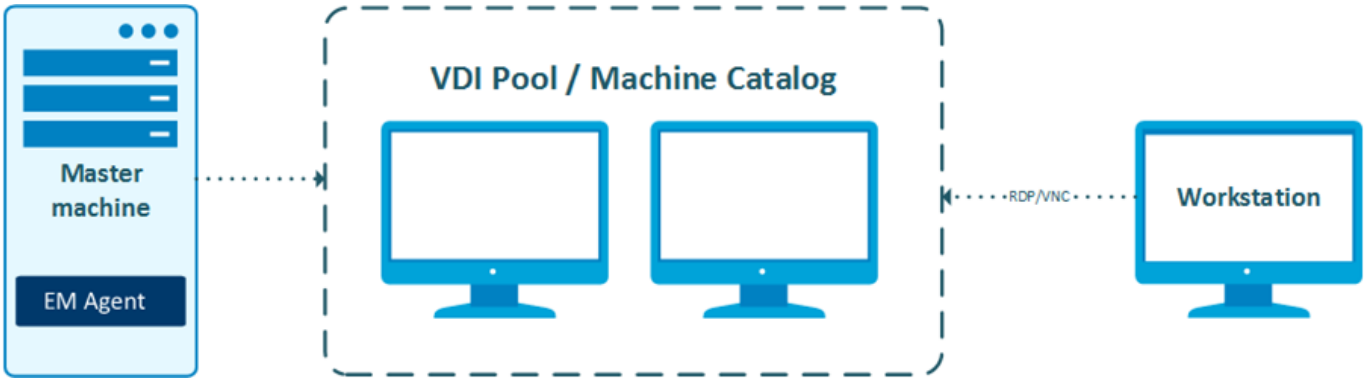
Entornos VDI

Puede usar un equipo maestro con el Agente ESET Management para un grupo IEV. No es necesario ningún conector IEV; todas las comunicaciones se hacen a través del Agente ESET Management. ESET Management Agent debe instalarse en el equipo maestro antes de que se configure el grupo IEV (catálogo de equipo).

- Si desea crear un grupo IEV, ponga un indicador en el equipo maestro en Detalles del equipo > **Virtualización** antes de crearlo; luego, seleccione **Marcar como maestro para clonar** > **Hacer coincidir con el equipo existente)**
- Si el equipo maestro se quita de ESET PROTECT On-Prem, se prohíbe la recuperación de su identidad (clonación) y los nuevos equipos del grupo obtendrán una nueva identidad cada vez (se crea una nueva entrada de equipo en la consola web)
- Cuando se conecta por primera vez un equipo del grupo IEV, tiene un intervalo de conexión obligatorio de 1 minuto; luego de las primeras replicaciones, el intervalo de conexión se hereda del equipo maestro
- Nunca deshabilite la detección del hardware cuando utilice el grupo IEV.
- Puede ejecutar al equipo maestro junto con los equipos clonados, para que pueda mantenerlo actualizado.

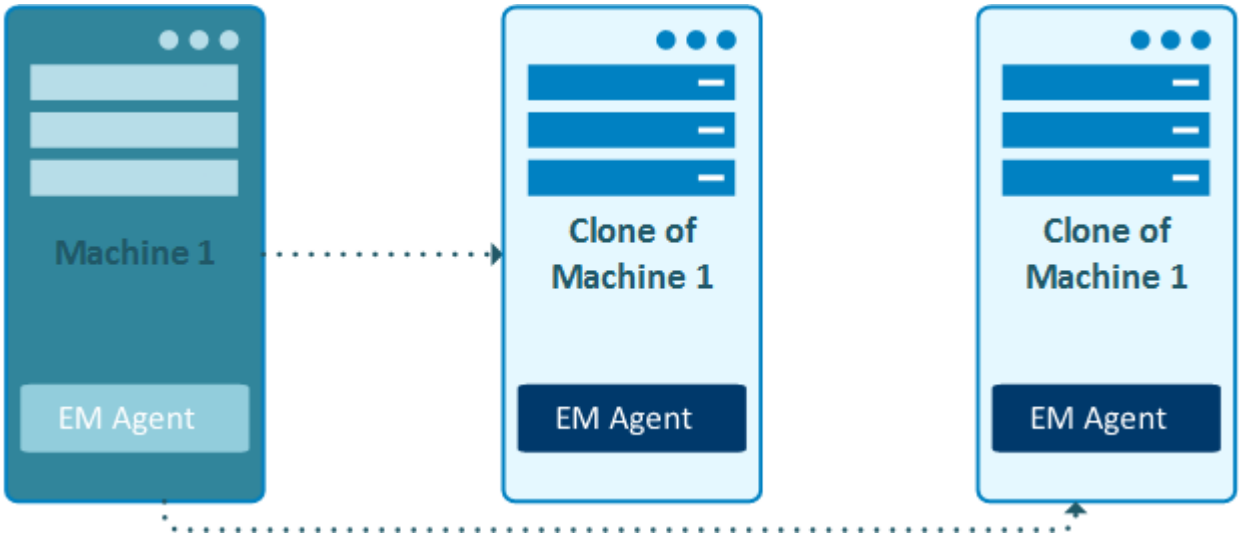
Grupo predeterminado para máquinas VDI

Las nuevas máquinas clonadas desde el maestro aparecen en el grupo estático establecido en el **grupo de pertenencia Equipos clonados** de la ventana Maestro para clonación.



Clonación de equipos en el hipervisor

Puede crear un clon a partir de un equipo normal. Únicamente espere a que aparezca la Pregunta y resuélvala al seleccionar **Crear un nuevo equipo sólo esta vez**



Imágenes de sistemas a equipos físicos

Puede usar una imagen maestra con ESET Management Agent instalado e implementado en equipos físicos. Hay dos formas de hacerlo:

Crear un nuevo equipo

Cree un nuevo equipo en ESET PROTECT On-Prem después de cada implementación de imagen.

Cuando se detecta un clon, el sistema puede reaccionar de dos maneras:

- Manual: resuelva manualmente cada nuevo equipo en Preguntas y seleccione **Crear un nuevo equipo cada vez**.
- Automático: indique el equipo maestro antes de la clonación y seleccione **Marcar como Maestro para la clonación** > **Crear nuevos equipos**.

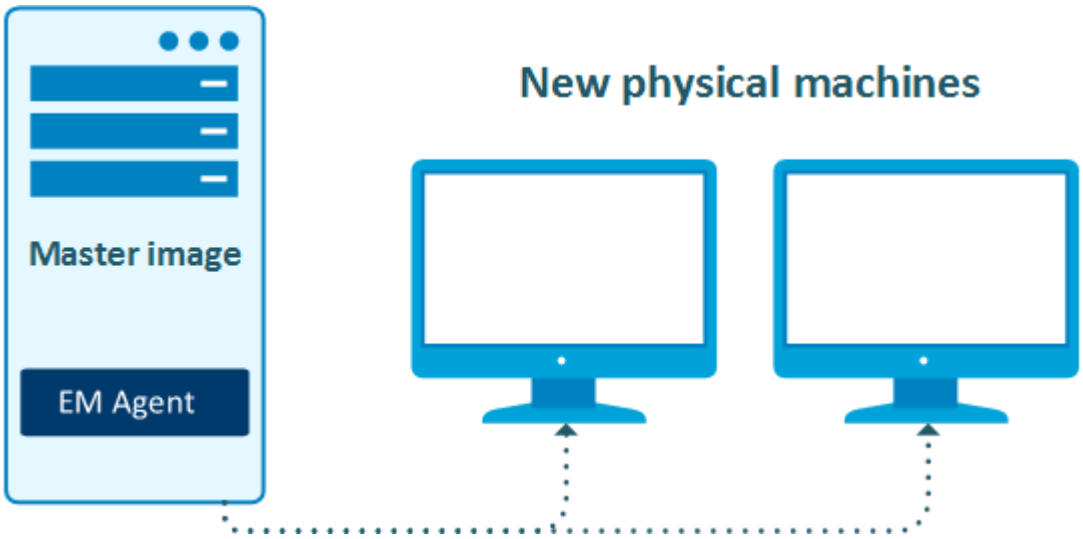
Vincular con equipo existente

Si la imagen vuelve a implementarse en un equipo con historial anterior en ESET PROTECT On-Prem (que ya ESET Management tenía implementado el Agente), este equipo está conectado a su identidad anterior en ESET PROTECT On-Prem. Si no hay identidades previas que coincidan, el sistema crea un nuevo equipo en ESET PROTECT On-Prem después de cada implementación de imagen en el equipo nuevo.

Cuando se detecta un clon, el sistema puede reaccionar de dos maneras:

- Manual: resuelva manualmente cada nuevo equipo en Preguntas y seleccione **Emparejar con un equipo existente cada vez**.
- Automático: indique el equipo maestro antes de la clonación y seleccione **Marcar como Maestro para la clonación** > **Establecer coincidencia con los existentes equipos**.

Si tiene una imagen (o plantilla) de su equipo principal, asegúrese de mantenerla actualizada. Actualice siempre la imagen después de actualizar o reinstalar cualquier componente de ESET en el equipo maestro.



Replicación paralela

El Servidor ESET PROTECTpuede reconocer y resolver casos de replicación paralela en múltiples equipos a una única identidad en ESET PROTECT On-Prem. Este tipo de evento se informa en Detalles del equipo > **Alertas** ('**Conexiones múltiples con la misma identificación de agente**'). Hay dos formas de resolver este problema:

- Use la acción de un clic disponible en la alerta; los equipos se dividen y la detección de hardware es apaga de manera permanente.
- En raras ocasiones, incluso los equipos con detección de hardware desactivado pueden entrar en conflicto; si esto sucede, la tarea Restablecer agente clonado es la única opción.
- Ejecute la tarea Restablecer agente clonado en el equipo, y esto evitará que tenga que deshabilitar la detección de hardware.

Solución de problemas

Si tiene problemas con un clon de VDI, siga los pasos de resolución de problemas de VDI.

Resolver preguntas de clonación

Cada vez que una máquina se conecta al ESET PROTECT On-Prem, se crea una entrada en función de dos huellas digitales:

- un agente UUID (identificador único universal) de ESET Management: cambia cuando se vuelve a instalar el agente ESET Management en una máquina (consulte la situación de doble agente).
- una huella digital de hardware del equipo: cambia si la máquina se clona o se vuelve a implementar.

Se mostrará una pregunta si el Servidor de ESET PROTECT detecta una de las siguientes cuestiones:

- un dispositivo clonado que está siendo conectado
- un cambio de hardware en un dispositivo existente con el Agente ESET Management instalado

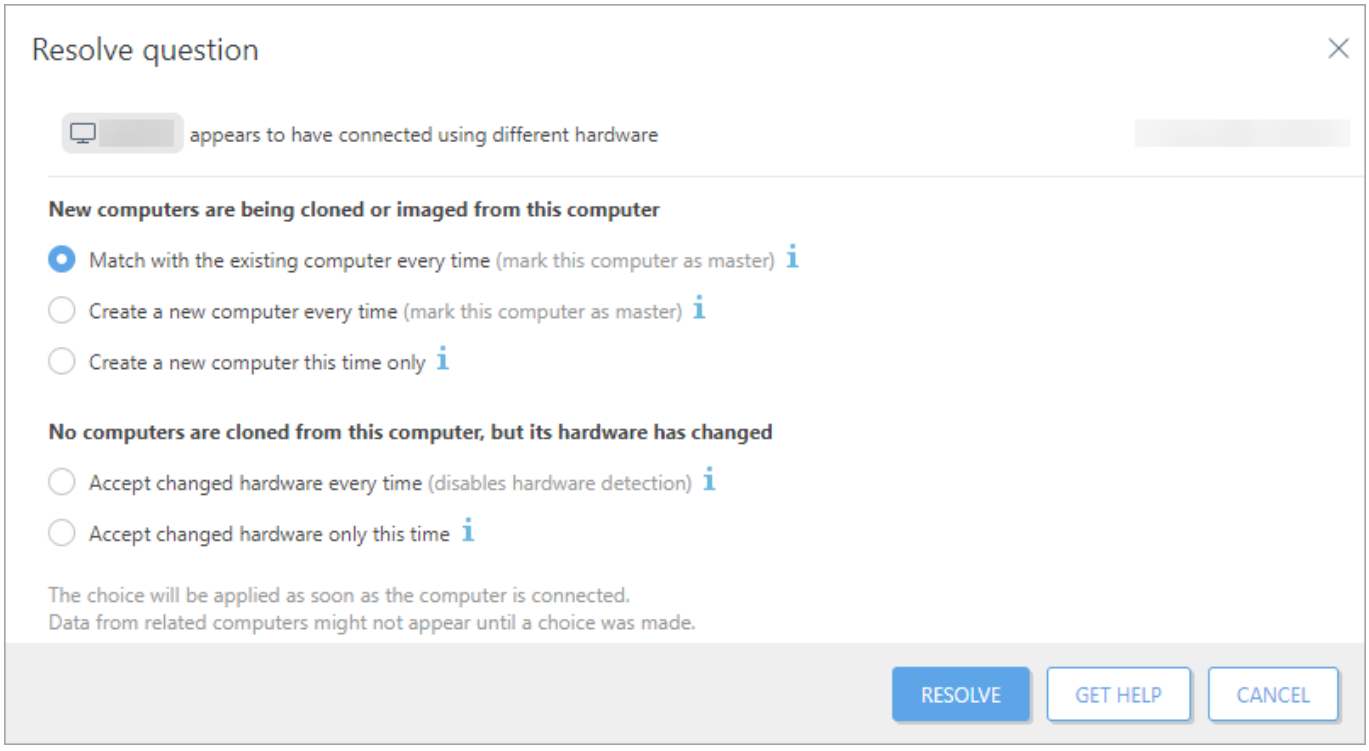
La detección de huella digital de equipos no es compatible con:
- Linux, macOS, Android, iOS
- equipo sin ESET Management Agente

Haga clic en la pregunta y seleccione **Resolver pregunta** para que se muestre un menú con las siguientes opciones:

Se han hecho clonaciones o imágenes de nuevos ordenadores desde este equipo	Acción	Más información
Se hace un emparejamiento con el equipo existente cada vez	Seleccione esta opción cuando: • Use el equipo como el maestro y todas sus imágenes deben conectarse a la entrada existente en el equipo en ESET PROTECT On-Prem. • Use el equipo como el maestro para configurar un entorno IEV y el equipo esté en el grupo IEV, y se espera que recupere su identidad basándose en un ID de huella digital del hardware.	Artículo KB
Crear un nuevo equipo cada vez	Seleccione esta opción cuando use este equipo como una imagen maestra y desee que ESET PROTECT On-Prem reconozca automáticamente todos los clones de este equipo como nuevos equipos. No lo utilice con entornos IEV.	Artículo KB
Crear un nuevo equipo solo esta vez	El equipo se clona solo una vez. Seleccione esta opción para crear una nueva instancia para el dispositivo clonado.	Artículo KB

No se han clonado ordenadores desde este equipo, pero el hardware ha cambiado	Acción
Aceptar el hardware cambiado cada vez	Deshabilitar permanentemente la detección de hardware para este dispositivo. Usar solo si se informan cambios de hardware inexistentes. **¡Esta acción es irreversible!** Si desactiva la detección de hardware, tanto el agente como el servidor almacenan esta configuración. La nueva instalación del agente no restaura la detección de hardware desactivada. Las máquinas con detección de hardware desactivada no son adecuadas para los escenarios VDI de ESET PROTECT On-Prem.
Aceptar el hardware cambiado solo esta vez	Seleccione para renovar la huella digital del hardware del dispositivo. Use esta opción después de cambiar el hardware del equipo del cliente. Se reportarán nuevamente las futuras modificaciones del hardware.

Haga clic en **Resolver** para enviar la opción seleccionada. La pregunta de clonación se resolverá la próxima vez que el equipo clonado se conecte a ESET PROTECT On-Prem.



Si no resuelve una pregunta en 30 días, la opción **Crear un nuevo equipo solo esta vez** se seleccionará automáticamente.

Situación de Agente doble

Si el Agente de ESET Management no está instalado (pero el equipo no se elimina de la Consola Web) en el equipo del cliente y vuelve a instalarse, entonces hay dos equipos iguales en la Consola Web. Uno de ellos está conectado al ESET PROTECT On-Prem y el otro no. La ventana de diálogo **Preguntas** no controla esta situación. Esta situación es causada por un procedimiento de eliminación del agente inadecuado. La única solución es quitar manualmente el equipo sin conexión desde la consola web. Después de esto se perderán el historial y los registros creados antes de la reinstalación.

Uso de la tarea Eliminar equipos sin conexión

Si tiene un grupo IEV de equipos y no resolvió el problema (consulte arriba) correctamente, la consola web crea una nueva instancia del equipo después de volver a cargar el equipo desde el grupo. Las instancias del equipo se agrupan en la consola web y las licencias pueden usarse de manera excesiva. No recomendamos resolverlo mediante la configuración de una tarea para eliminar los equipos sin conexión. Un procedimiento tal elimina el historial (registros) para los equipos eliminados y las licencias también pueden usarse de manera excesiva.

Licencias usadas de manera excesiva

Cuando se clona un equipo cliente con ESET Management Agent instalado y el producto de seguridad de ESET activado, cada máquina clonada puede reclamar otro puesto de licencia. Este proceso puede usar sus licencias de manera excesiva. En entornos IEV, use un archivo de licencia sin conexión para activar los productos de ESET y póngase en contacto con ESET para modificar la licencia.

Notificaciones para equipos clonados

Un usuario puede elegir entre tres notificaciones preparadas para acciones relacionadas con la clonación. Para configurar una notificación, seleccione el menú de **Notificaciones** en la consola web.

- **Nuevo equipo inscrito** – Notifica si un equipo está conectado por primera vez al grupo estático seleccionado (el grupo **Todos** está seleccionado de forma predeterminada).
- **Identidad del equipo recuperada**: notifique si se identificó un equipo en función de su hardware; el equipo se clonó desde un equipo maestro u otro origen conocido
- **Detección de posibles clonaciones de equipos** – Notifica sobre una modificación o clonación de hardware importante si el equipo fuente no ha sido marcado como maestro antes.

Solución de problemas

Si tiene problemas con un clon de VDI, siga los pasos de resolución de problemas de VDI.

Identificación del hardware

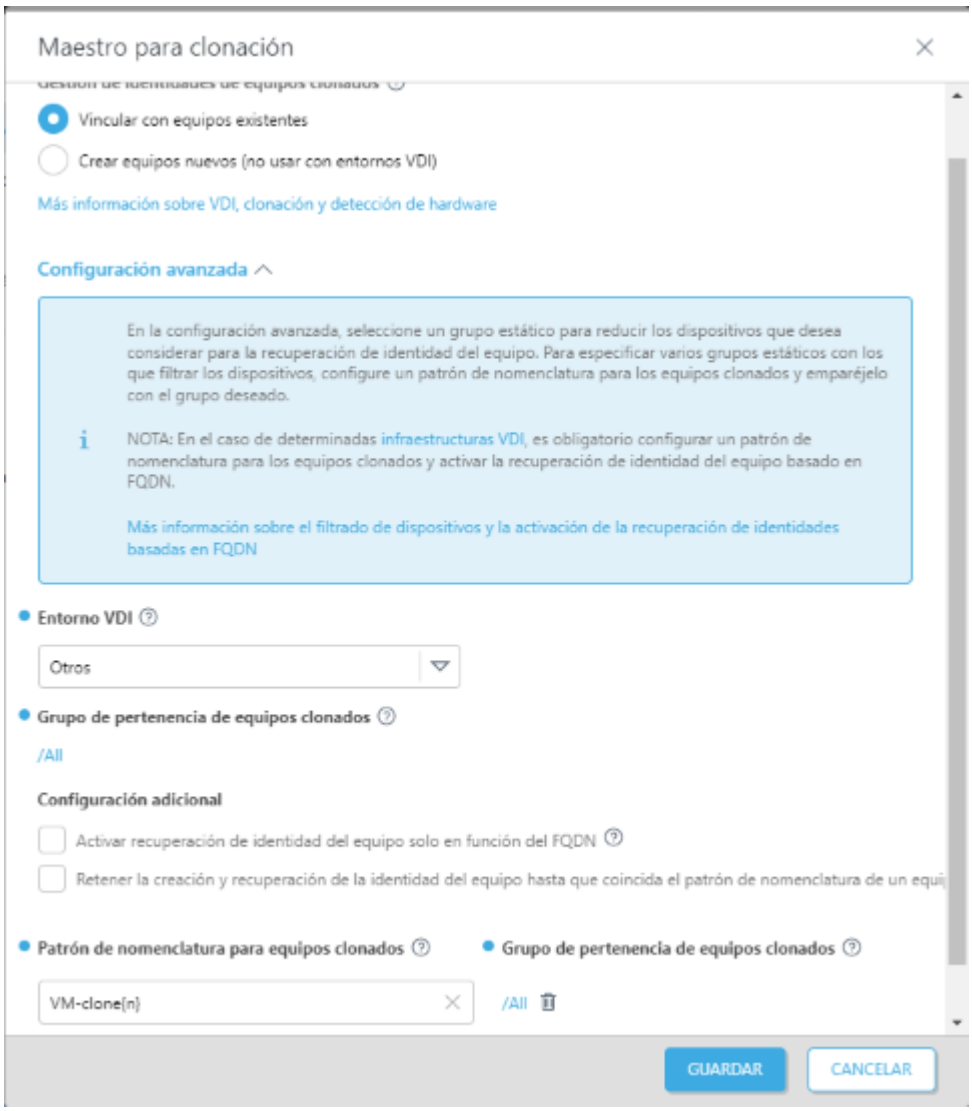
ESET PROTECT On-Prem está recopilando detalles de hardware sobre cada dispositivo administrado e intenta identificarlo. Cada dispositivo conectado a ESET PROTECT On-Prem pertenece a una de las siguientes categorías, como se muestra en la columna **Identificación del hardware**, en la ventana **Ordenador**.

- **Detección de hardware habilitada** – La detección está habilitada y funciona correctamente.
- **Detección de hardware deshabilitada** – La detección está deshabilitada por el usuario o automáticamente por ESET PROTECT On-Prem.
- **Sin información de hardware** - no hay información de hardware disponible, ya sea que el dispositivo cliente esté ejecutando un sistema operativo no compatible o una versión antigua del Agente ESET Management.
- **Detección de hardware poco fiable** – el usuario informa que la detección no es fiable y que va a ser

desactivada. Este estado solo puede ocurrir durante el intervalo de replicación única antes de deshabilitar la detección.

Maestro para clonación

Al hacer clic en **Virtualización** > **Marcar como maestro para clonación** en Detalles del equipo se muestra la siguiente notificación:



Seleccionar una de las opciones de **Gestión de identidades de equipos clonados** antes de crear el grupo IEV:

- **Emparejar con equipos existente**: ver la opción Emparejar con un equipo existente siempre.
- **Crear nuevos equipos**: consulte la opción Crear un nuevo equipo cada vez.

Para buscar los equipos marcados como equipo Maestro para clonación, vaya a **Equipos** > haga clic en **Agregar filtro** > seleccione **Maestro para clonación**, seleccione la casilla de verificación situada junto al filtro **Maestro para clonación**.
Puede cambiar la configuración del **Maestro para clonación** más adelante en los detalles del equipo:
- Haga clic en el ícono de engranaje del mosaico **Virtualización** para ajustar la configuración.
- Para quitar la configuración, haga clic en **Virtualización** > **Desmarcar como maestro para clonación**.

Configuración avanzada

1. Seleccione el tipo de **entorno VDI** para rellenar la configuración necesaria para el entorno.

- Máquinas virtuales Citrix MCS/PVS Gen1
- Máquinas virtuales Citrix PVS Gen2
- Clones vinculados de VMware Horizon
- Clones instantáneos de VMware Horizon
- SCCM
- Otros

2. **Grupo de pertenencia de equipos clonados**: seleccione un grupo estático para limitar los dispositivos que desea considerar para la recuperación de identidad del ordenador. El grupo estático seleccionado también sirve como destino de las máquinas virtuales recién creadas.

3. **Configuración adicional**:

- **Activar la recuperación de identidad del equipo basada solo en FQDN**: seleccione la casilla de verificación para habilitar la recuperación de identidad del equipo basada en FQDN (nombre de dominio calificado completo) si los atributos de hardware de los equipos clonados generados por su infraestructura VDI no son fiables para el proceso de recuperación.

- **Retener la creación y recuperación de la identidad del equipo hasta que se coincida el patrón de nomenclatura de un equipo**: marque la casilla para asegurarse de que el nombre del equipo clonado coincida con uno de los patrones de nomenclatura proporcionados. La creación y la recuperación de la identidad del equipo no finalizarán si no se encuentra un patrón que coincida.

> En función del entorno VDI seleccionado, la configuración recomendada se selecciona previamente (puede ser obligatoria o no disponible).

4. **Patrón de nomenclatura para equipos clonados**: haga clic en **Agregar nuevo** y escriba el patrón de nomenclatura para filtrar dispositivos.

> **Patrón de nomenclatura IEV**
> ESET PROTECT On-Prem solo reconoce clones con nombres que coincidan con el patrón de nomenclatura establecido en el entorno IEV:
> - **VMware**: el patrón de nomenclatura VDI es obligatorio para los clones instantáneos de VMware. El patrón de nomenclatura IEV debe tener un marcador de posición especificado para un número `{n}` exclusivo generado por la infraestructura IEV, por ejemplo, `VM-instant-clone-{n}`. Consulte la documentación de VMware para obtener más información sobre los patrones de nomenclatura.
> - **Citrix XenCenter/XenServer**: utilice el hash `#` en el esquema de nomenclatura del catálogo de equipo, por ejemplo, `VM-office-##`. Consulte la documentación de Citrix para obtener más información sobre los esquemas de nomenclatura.

5. Haga clic en **Seleccionar** y seleccione el **Grupo de pertenencia de equipos clonados**: seleccione el grupo estático asociado como grupo de pertenencia de los dispositivos que coincidan con el patrón de nomenclatura de VDI.

6. Haga clic en **Agregar nuevo** para agregar más grupos de pertenencia y patrones de nomenclatura de VDI.

7. Haga clic en **Guardar**.

Para buscar los equipos marcados como equipo Maestro para clonación, vaya a **Equipos** > haga clic en **Agregar filtro** > seleccione **Maestro para clonación**, seleccione la casilla de verificación situada junto al filtro **Maestro para clonación**.
Puede cambiar la configuración del **Maestro para clonación** más adelante en los detalles del equipo:
- Haga clic en el ícono de engranaje del mosaico **Virtualización** para ajustar la configuración.
- Para quitar la configuración, haga clic en **Virtualización** > **Desmarcar como maestro para clonación**.

Solución de problemas

Si tiene problemas con un clon de VDI, siga los pasos de resolución de problemas de VDI.

Implementación del agente ESET Management

En esta sección se describen todos los métodos disponibles que puede usar para implementar el agente ESET Management en equipos cliente de su red. Es muy importante debido a que las soluciones de seguridad de ESET que se ejecutan en los equipos cliente se comunican con el servidor ESET PROTECT exclusivamente a través del agente.

Agregar equipos cliente a la estructura de ESET PROTECT On-Prem

Antes de comenzar a administrar equipos de clientes en su red, deberá agregarlos a ESET PROTECT On-Prem. Use uno de los siguientes métodos para agregarlos:

- Sincronización con Active Directory
- RD Sensor
- Agregar nuevos dispositivos en forma manual

Implementación del agente ESET Management

La implementación del agente ESET Management puede realizarse de varias maneras diferentes. Puede implementar el agente a nivel local o remoto:

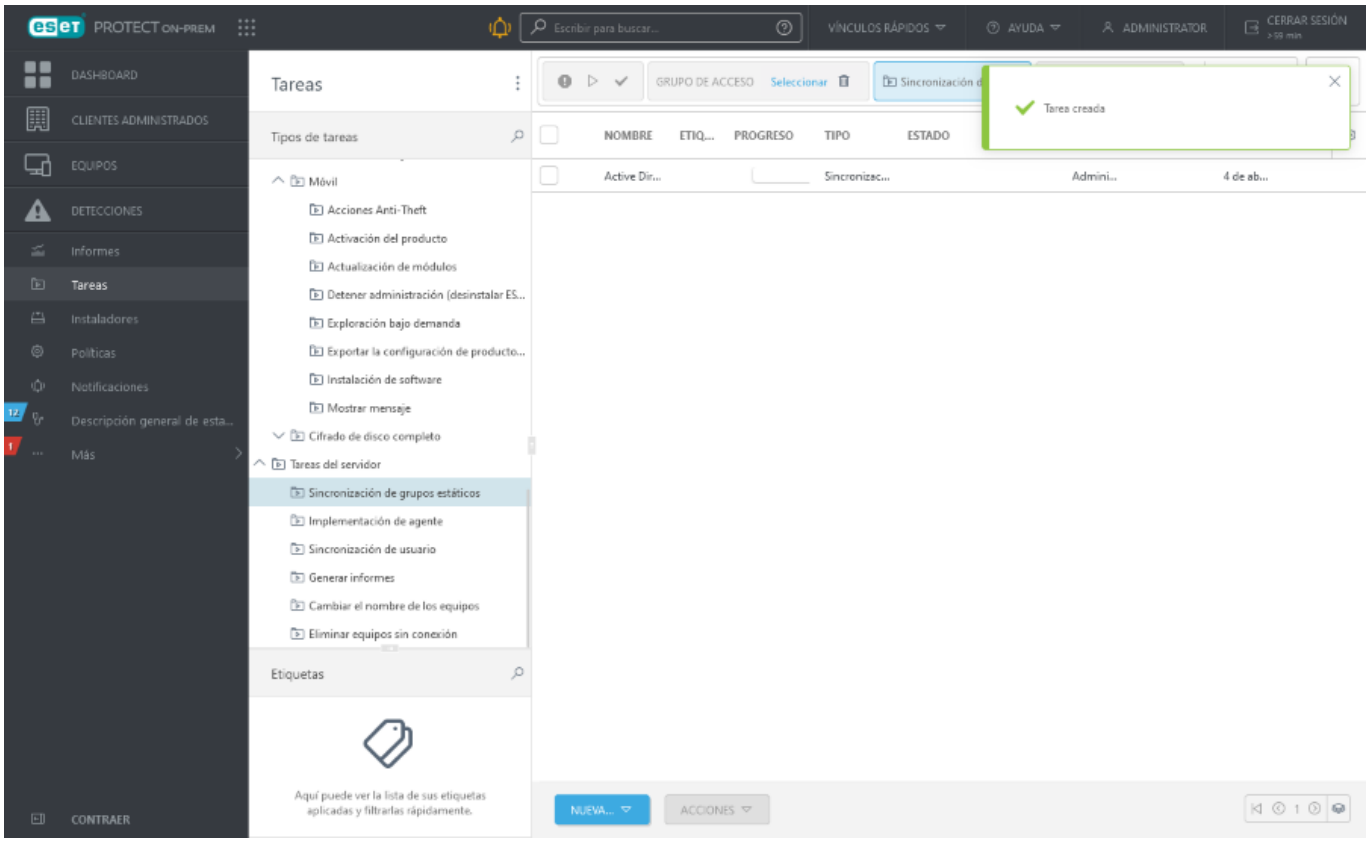
- Instalación local: instale el agente ESET Management y el producto de seguridad ESET en un equipo cliente.

Le recomendamos usar la implementación local solo si tiene una red pequeña (hasta 50 equipos). Para redes más grandes, puede Implementar el agente ESET Management mediante GPO o SCCM.

- Implementación remota: le recomendamos usar este método para implementar el agente ESET Management en una gran cantidad de equipos de clientes.

Agregar equipos mediante la sincronización con Active Directory

La sincronización con AD se realiza al ejecutar la tarea del servidor **Sincronización de grupos estáticos**. Es una tarea predeterminada y predefinida que puede elegir para ejecutar automáticamente durante la instalación de ESET PROTECT On-Prem. Si el equipo se encuentra en un dominio, la sincronización se realizará y los equipos del AD se colocarán en una lista en el grupo predeterminado **Todos**.



Para iniciar el proceso de sincronización, haga clic en la tarea y elija **Ejecutar ahora**.

- Si necesita crear una nueva tarea de sincronización con AD, seleccione un grupo al que desee agregar los equipos nuevos desde AD.
- Seleccione los objetos en el AD desde donde desea realizar la sincronización y qué hacer con los duplicados.
- Ingrese la configuración de su conexión al servidor AD y establezca el Modo de sincronización para el **Active Directory/Open Directory/LDAP**. Siga las instrucciones paso a paso de este artículo de la base de conocimiento de ESET.

> Puede ejecutar la tarea del servidor Instalación de agente para instalar el ESET Management agente a los equipos sincronizados desde Active Directory.

Agregar nuevos dispositivos en forma manual

Esta función le permite agregar manualmente **Equipos** o Dispositivos móviles que no se encuentran o agregan automáticamente. La pestaña **Equipos** o **Grupo** le permite agregar nuevos equipos o dispositivos móviles.

1. Para agregar un nuevo equipo, haga clic en **Equipos** > **Agregar dispositivo** y, luego, seleccione **Equipos** (también puede hacer clic en el ícono del engranaje junto al **Grupo estático** existente y, luego, hacer clic en **Agregar nuevo**).

2. **Agregar equipos**: puede usar varias opciones:

   - Escriba la **dirección IP** o **nombre de host** del equipo que quiera agregar y ESET PROTECT On-Prem lo buscará en la red. De manera opcional, ingrese una **Descripción** de los equipos.

   - **+Agregar dispositivo** para agregar dispositivos adicionales. Si desea eliminar un equipo de la lista de dispositivos, haga clic en el icono **Papelera** o en **Eliminar todos**.

   - **Importar CSV** para cargar un archivo *.csv* que contenga una lista de equipos para agregar. Para más información, consulte Importar carga de CSV.

   - **Copiar y pegar** una lista personalizada de equipos separados por delimitadores personalizados. La función se usa de manera similar a la importación de *.csv*.

3. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.

4. **Grupo primario**: seleccione un grupo primario existente y, luego, haga clic en **Acepar**.

5. **Usar la resolución FQDN**:

   - Seleccione la casilla de verificación y ESET PROTECT Server traduce la dirección IP proporcionada o el nombre de host del equipo por un nombre de dominio totalmente calificado.

   - Quite la marca de la casilla de verificación para importar los nombres de equipo proporcionados. Con esta opción, la importación por lotes de los equipos es mucho más rápida con nombres en formato FQDN (por ejemplo, importar desde *.csv*).

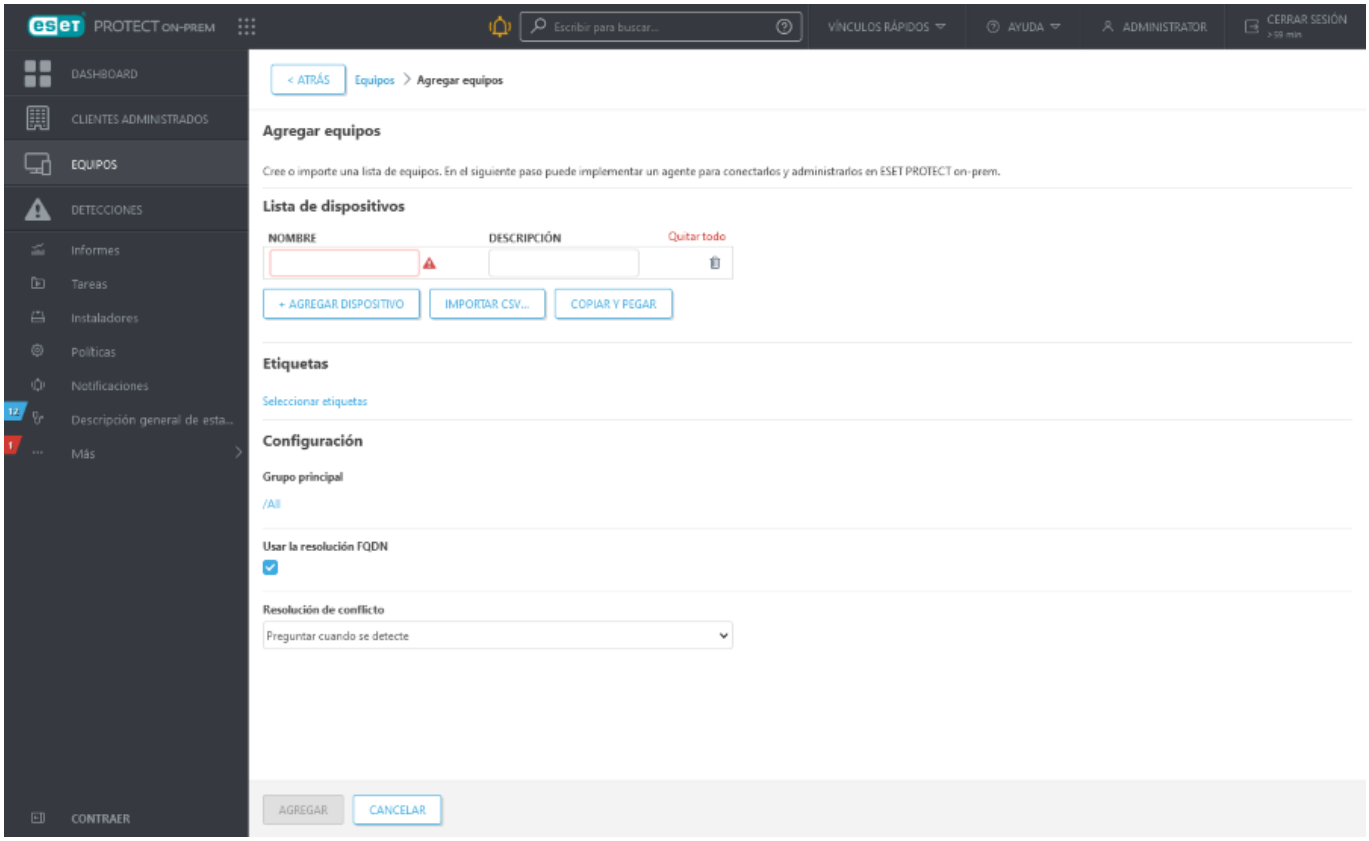
6. Use el menú desplegable **Resolución de conflictos** para seleccionar la acción que se debe realizar si el equipo agregado ya se encuentra en ESET PROTECT On-Prem:

   - **Preguntar cuando se detectan conflictos**: cuando se detecta un conflicto, el programa le solicitará que seleccione una acción (vea las siguientes opciones).

   - **Omitir dispositivos duplicados**: no se agregarán equipos duplicados.
   - **Crear dispositivos duplicados**: los equipos nuevos se agregarán, pero con nombres diferentes.

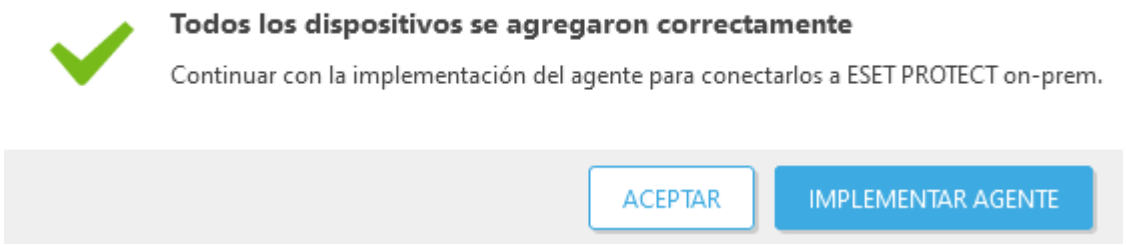
   - **Mover dispositivos duplicados al grupo**: los equipos en conflicto se moverán al grupo principal.

7. Haga clic en **Agregar** cuando haya finalizado con los cambios.



Agregar múltiples equipos puede tardar más tiempo (es posible realizar una búsqueda DNS en reverso. Consulte **Cómo usar la resolución FQDN** arriba).

8. Aparecerá una ventana **Todos los dispositivos agregados correctamente**.



• Haga clic en **Implementar agente**: en Crear instalador, seleccione el sistema operativo y el tipo de implementación del agente.

• Haga clic en **Aceptar** para implementar el agente más adelante. Los equipos agregados aparecerán en **Equipos**. Haga clic en el equipo > **Soluciones** para implementar el agente:

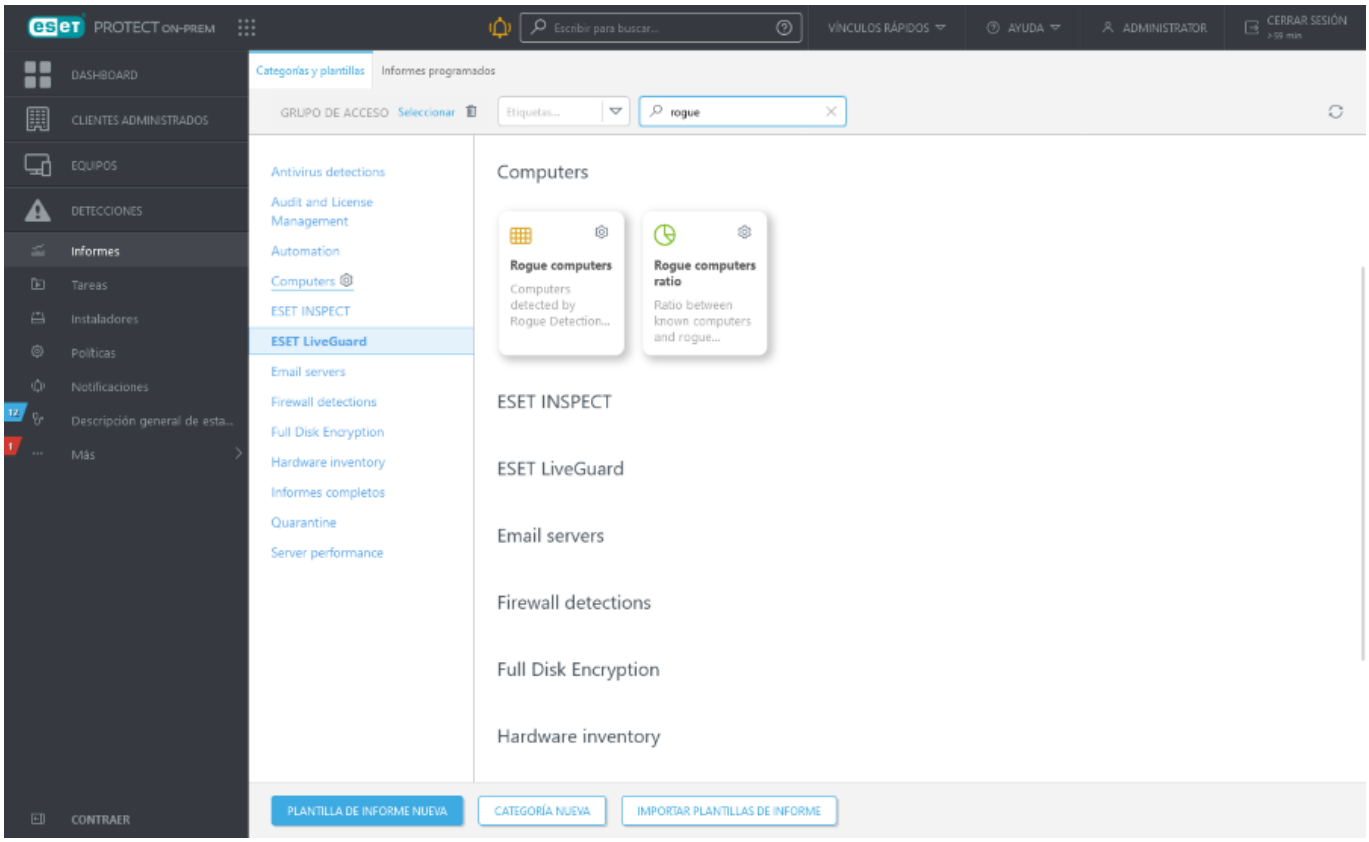
o **Implementar agente con un instalador**: en Crear instalador, seleccione el sistema operativo y el tipo de implementación del agente.

o **Implementar agente con una tarea de servidor**: utilice la tarea de servidor Implementación de agente para implementar el agente.

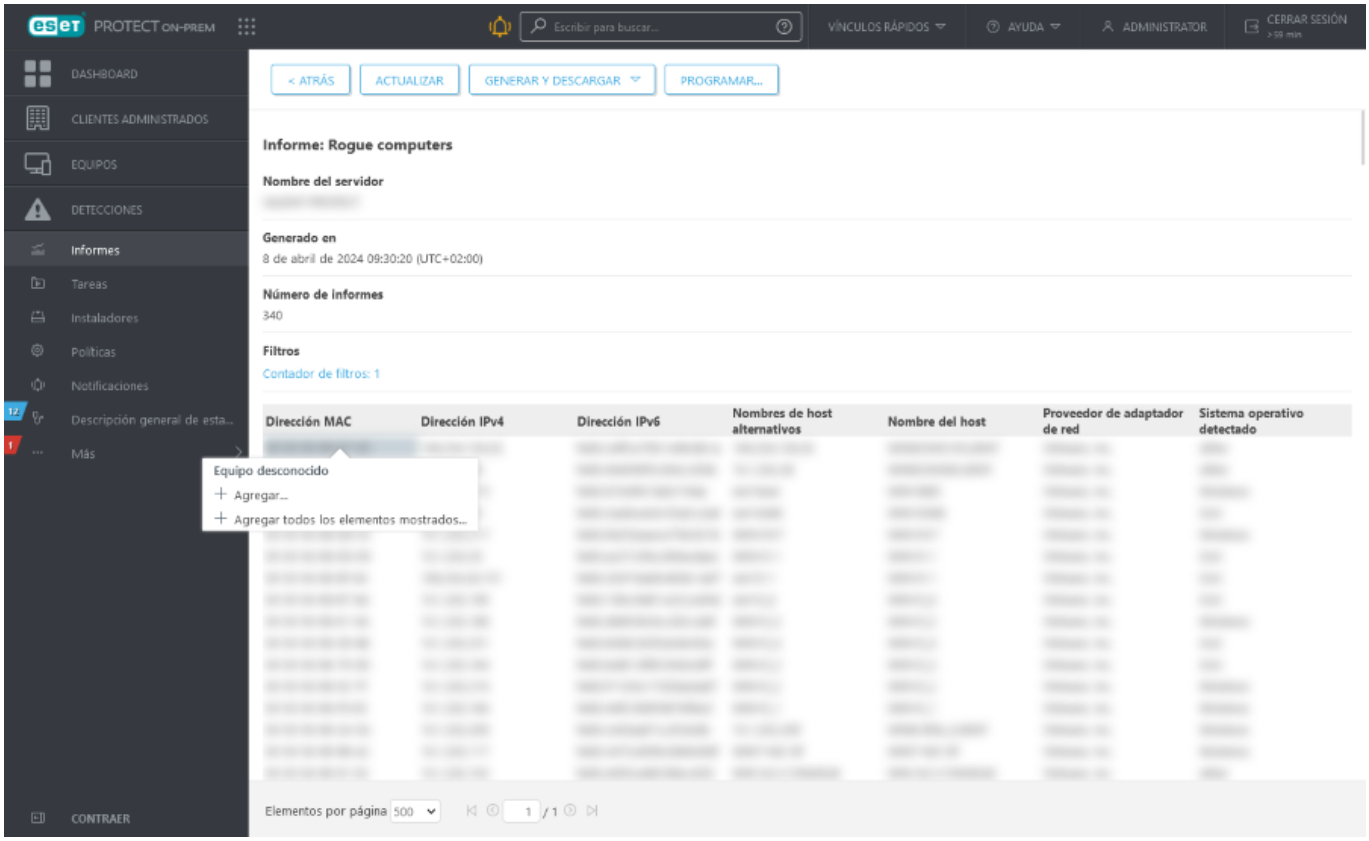
Agregar equipos con RD Sensor

Si no usa la sincronización de AD, la forma más fácil de encontrar un equipo no administrado en su estructura de red es mediante el RD Sensor. El RD Sensor supervisa la red en la que se encuentra instalado y, cuando se conecta un nuevo dispositivo sin un agente a la red, envía esta información a ESET PROTECT On-Prem.

En **Informes**, vaya a la sección **Equipos** y haga clic en el informe **Equipos no autorizados**.



El informe Equipos no autorizados muestra los equipos detectados por el sensor RD. Puede ajustar la información que brinda el RD Sensor con la Política del RD Sensor. Puede agregar equipos al hacer clic en el equipo que quiere Agregar, o bien, puede Agregar todos los elementos que se muestran.



Si va a agregar un único equipo, puede usar un nombre preconfigurado o especificar su propio nombre (es un nombre de visualización que se usará únicamente en la consola web ESET PROTECT, no un nombre de host real).

- También puede agregar una descripción si lo desea. Si este equipo ya existe en su directorio de ESET PROTECT On-Prem, recibirá una notificación y podrá decidir qué hacer con el duplicado. Las opciones disponibles son: **Implementar el agente**, **Omitir**, **Volver a intentar**, **Mover**, **Duplicar** o **Cancelar**.

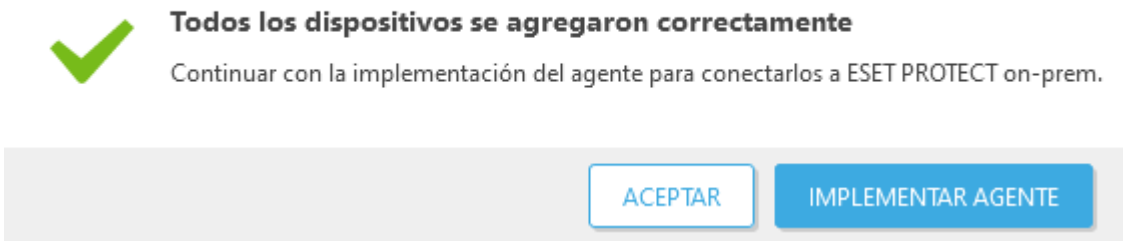
- Una vez que se agrega el equipo, se abrirá una ventana con una opción para **Implementar el agente**.

Si hace clic en **Agregar todos los elementos mostrados**, aparecerá una lista de los equipos que se agregarán.

1.Haga clic en junto al nombre de un equipo específico si no desea incluirlo en su directorio de ESET PROTECT On-Prem en este momento. Una vez que finalice de eliminar equipos de la lista, haga clic en **Agregar**.

2.Seleccione la acción a realizar cuando se detecta un duplicado (tenga en cuenta que puede haber una breve demora dependiendo del número de equipos en su lista): **Omitir, Volver a intentar, Mover**, **Duplicar** o **Cancelar**.

3.Aparecerá una ventana **Todos los dispositivos agregados correctamente**.



- Haga clic en **Implementar agente**: en Crear instalador, seleccione el sistema operativo y el tipo de implementación del agente.

- Haga clic en **Aceptar** para implementar el agente más adelante. Los equipos agregados aparecerán en **Equipos**. Haga clic en el equipo > **Soluciones** para implementar el agente:

  o **Implementar agente con un instalador**: en Crear instalador, seleccione el sistema operativo y el tipo de implementación del agente.

  o **Implementar agente con una tarea de servidor**: utilice la tarea de servidor Implementación de agente para implementar el agente.

Los resultados de la exploración del RD Sensor se inscriben en un archivo de registro llamado `detectedMachines.log`. Contiene una lista de los equipos que se descubrieron en su red. Puede encontrar el archivo `detectedMachines.log` aquí:

- Windows
C:\ProgramData\ESET\Rogue Detection Sensor\Logs\detectedMachines.log

- Linux
/var/log/eset/RogueDetectionSensor/detectedMachines.log

Ajustes de política de ESET Rogue Detection Sensor

Es posible cambiar el comportamiento de ESET RD Sensor con una política. Esto se usa principalmente para cambiar el filtrado de direcciones. Puede, por ejemplo, incluir ciertas direcciones en la lista negra para que no sean detectadas.

Haga clic en **Políticas** y expanda **Políticas personalizadas para** editar una política existente o crear una nueva.

Filtros

IPv4 Filtro

Habilitar IPv4 filtrado de direcciones: al permitir el filtrado, solo se detectarán los equipos cuyas direcciones IP sean parte de la lista blanca en la lista de filtrado IPv4 o solo aquellas que no estén en la lista negra.

Filtros: especifican si la lista será una **lista blanca** o **lista negra**.

IPv4 lista de direcciones: haga clic en Editar **IPv4** lista para agregar o eliminar direcciones de la lista.

MAC filtro de prefijo de dirección

Habilitar MAC filtrado de direcciones: al permitir el filtrado, solo se detectarán los equipos cuyos prefijos de dirección MAC (xx:xx:xx) sean parte de la lista blanca en la lista de direcciones MAC o solo aquellos que no estén en la lista negra.

Modo de filtrado: especifican si la lista será una **lista blanca** o **lista negra**.

MAC lista de prefijos de direcciones: haga clic en **Editar MAC lista** para agregar o eliminar un prefijo de la lista.

Detección

Detección activa: habilitar esta opción le permitirá al Sensor RD buscar equipos de forma activa en la red local. Esto puede mejorar los resultados de búsqueda, pero también desencadenar advertencias del firewall en algunos equipos.

Puerto de detección del OS : el Sensor RD utiliza una lista preconfigurada de puertos para buscar equipos en la red local. Puede editar esta lista de puertos.

Configuración avanzada

Participar en el programa de mejora del producto: habilite o deshabilite el envío de 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).

Asignar

Especifica los clientes que recibirán esta política. Haga clic en **Asignar** para visualizar todos los Grupos estáticos y dinámicos y a sus miembros. Seleccione el equipo donde quiere aplicar la política y haga clic en **Aceptar**.

Resumen

Revise la configuración de esta política y haga clic en **Finalizar**.

Implementación local

Este método de implementación ha sido diseñado para instalaciones en el sitio. Cree o descargue un paquete de instalación y permita el acceso a él a través de una carpeta compartida, unidad flash o correo electrónico.

El administrador o un usuario con privilegios de administrador debe instalar el paquete del instalador.

Le recomendamos usar la implementación local solo si tiene una red pequeña (hasta 50 equipos). Para redes más grandes, puede Implementar el agente ESET Management mediante GPO o SCCM.

La implementación local se puede realizar de tres maneras:

- Crear instalador de agente (y producto de seguridad ESET) (Solo Windows)
- Crear instalador de scripts del agente (Windows, Linux, macOS)
- Descargar el agente desde el sitio Web de ESET (Windows, Linux, macOS)

Implementación local y permisos

Para más información sobre cómo permitir a un usuario implementar el agente ESET Management localmente, siga las instrucciones en este ejemplo.

Tenga en cuenta que el usuario será capaz de trabajar con Certificados al crear instaladores. El usuario debe tener el permiso de **Uso** para **Certificados** con acceso al grupo estático donde se contienen los certificados. Si un usuario desea implementar el agente ESET Management, es necesario asignar permiso de **Uso** para la autoridad de certificación a la que se encuentra asignado el servidor real. Para información sobre cómo dividir el acceso a los certificados y la autoridad de certificación lea este ejemplo. Consulte la lista de permisos para obtener más información sobre los derechos de acceso.

Crear instalador de agente y producto de seguridad ESET - Creación de Windows

Puede crear el instalador para el agente y el producto de seguridad de ESET para Windows de varias maneras:

- **Enlaces rápidos** > **Implementar agente** > **Windows**
- **Instaladores** > **Crear instalador**.
- Recorrido por ESET PROTECT On-Prem

Haga clic en **Windows** > **Descargar el instalador o utilizar Remote Deployment Tool de ESET**

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

1. **Distribución:** seleccione **Descargar o enviar instalador o usar ESET Remote Deployment Tool**.

Si ha seleccionado otro tipo de instalador, siga las instrucciones correspondientes:
- Implementar agente primero (instalador de scripts del agente)
- Usar GPO o SCCM para la implementación

2. **Componentes**: seleccione la(s) casilla(s) de verificación a partir de las siguientes opciones:

- **Management Agent**: si no selecciona otros elementos en el **Componentes**, el instalador incluirá solo el agente ESET Management. Seleccione esta opción si desea instalar el Producto de seguridad ESET en el equipo cliente más tarde, o si el equipo cliente ya tiene un Producto de seguridad ESET instalado.
- **Producto de seguridad**: incluye el producto de seguridad ESET con el agente ESET Management. Seleccionar esta opción si el equipo cliente no tiene ningún Producto de seguridad ESET instalado y desea instalarlo con el agente ESET Management.
- **Cifrado de disco completo**: ESET Full Disk Encryption incluya el instalador. La opción está visible solo con una licencia ESET Full Disk Encryption activa.
- **Conector ESET Inspect**: incluya el conector ESET Inspect en el instalador. La opción está visible solo con una licencia ESET Inspect On-Prem activa.

Casilla de verificación del producto de ESET que falta

Si la casilla de verificación del producto de ESET (**Full Disk Encryption** o **ESET Inspect Conector**) falta o no se selecciona automáticamente después de seleccionar el grupo principal, no tiene la licencia del producto o la licencia del producto no se asigna al ESET Business Account sitio o la ESET MSP Administrator empresa para la que ha seleccionado el grupo principal, incluso si tiene derechos de acceso a la licencia. Asigne la licencia del producto de ESET al sitio (en ESET Business Account) o a la empresa (en ESET MSP Administrator). A continuación, estará disponible la casilla de verificación del producto de ESET y podrá incluir el producto de ESET en el instalador.

3. Seleccione la casilla de verificación **Participar en el programa de mejora del producto** para 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).

4. **Grupo principal:** seleccione el grupo principal en el que la consola web de ESET PROTECT colocará el equipo la instalación de un agente.

- Puede seleccionar un grupo estático existente o crear uno nuevo al que se le asignará el dispositivo luego de implementar el instalador.
- Si selecciona un grupo principal, se agregarán al instalador todas las políticas aplicadas al grupo.
- La selección del grupo principal no afecta a la ubicación del instalador. Después de crear el instalador, se coloca en el grupo de acceso del usuario actual. El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario.
- El grupo principal es obligatorio si utiliza ESET Business Account con sitios o ESET MSP Administrator y opcional si utiliza ESET Business Account sin sitios.

5. **Nombre de host del servidor (opcional)**: escriba el nombre de host o la dirección IP del servidor de ESET PROTECT. De ser necesario, especifique el número de **Puerto** (el predeterminado es 2222).

El campo **Nombre de host del servidor** no admite caracteres especiales, por ejemplo, letras con signos diacríticos.

6. **Certificado de pares**:

- **certificado ESET PROTECT**: se seleccionan automáticamente un certificado de pares para la instalación del agente y la autoridad de certificación de ESET PROTECT. Para utilizar un certificado diferente, haga clic en **Descripción del certificado de ESET PROTECT** para seleccionarlo en el menú desplegable de los certificados disponibles.
- **Certificado personalizado**: si utiliza un certificado personalizado para la autenticación, haga clic en **Certificado personalizado** > **Seleccionar**, cargue el certificado .pfx y selecciónelo al instalar el agente. Para obtener más información, consulte Certificados.

Frase de contraseña del certificado: escriba la frase de contraseña del certificado si es necesario: si especificó la contraseña durante la instalación del servidor ESET PROTECT (en el paso en el que creó una autoridad certificadora) o si utiliza un certificado personalizado con contraseña. De lo contrario, deje el campo **Frase de contraseña del certificado** en blanco.

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

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

7. Personalizar más ajustes

- Escriba el **Nombre del instalador** y la **Descripción** (opcional).
- **Instalación de componentes**: marque la casilla **Instalar siempre la versión más reciente disponible de los productos y componentes** y el instalador instalará siempre la versión más reciente de los productos y componentes seleccionados en los dispositivos conectados a Internet. Si un dispositivo no tiene acceso a Internet, se instalará la versión que seleccione en el siguiente paso de este asistente. Se recomienda marcar esta casilla de verificación si desea utilizar el instalador durante más tiempo, para asegurarse de que instala siempre la versión más reciente de los productos y componentes.
- Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
- **Configuración inicial (opcional):** utilice esta opción para aplicar una política de configuración al agente de ESET Management. Haga clic en **Seleccionar** dentro de **Configuración del agente** y elija entre la lista de políticas disponibles. Si ninguna de las políticas definidas previamente son adecuadas, puede crear una nueva política o personalizar las existentes.
- Si usa un proxy HTTP (recomendamos usar ESET Bridge), seleccione la casilla de verificación **Habilitar la configuración del proxy HTTP** y especifique la configuración del proxy (**Host**, **Puerto**, **Nombre de usuario** y **Contraseña**) para descargar el instalador a través del proxy y definir la conexión del agente ESET Management al proxy para habilitar el reenvío de comunicaciones entre el agente ESET Management y el servidor ESET PROTECT. El campo **Host** es la dirección del equipo que ejecuta el proxy HTTP. ESET Bridge usa el puerto 3128 de forma predeterminada. Puede definir otro puerto, de ser necesario. Asegúrese de configurar el mismo puerto también en la configuración del proxy de HTTP (consulta la ESET Bridge Política).

  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.

La casilla de verificación **Utilice una conexión directa si el proxy HTTP no está disponible** está preseleccionada. El asistente aplica la configuración como alternativa para el instalador: no puede anular la selección de la casilla de verificación. Puede deshabilitar la configuración mediante una política de agente de ESET Management:

- Durante la creación del instalador: incluya la política en la **Configuración inicial**.
- Tras la ESET Management instalación del agente: asigne la política al equipo.

8. Haga clic en **Finalizar** o en **Configuración del producto**.

9. Producto de seguridad

a.Haga clic en el producto de seguridad de ESET seleccionado previamente y cambie sus detalles:
oSeleccione otro producto de seguridad de ESET compatible.
o Seleccione el idioma en el menú desplegable **Idioma**.
oMarque la casilla de verificación **Avanzada**. De forma predeterminada, se selecciona previamente la versión más reciente (recomendada). Puede seleccionar una versión anterior.

> Si no ve los archivos de instalación de ningún producto, asegúrese de establecer el repositorio en **AUTOSELECT**. Para más información, consulte la sección de **Configuración avanzada** de la Configuración.

b. Marque la casilla de verificación que se encuentra junto a la configuración para habilitarla para el instalador:
oHabilite el sistema de respuesta ESET LiveGrid® (recomendado)
oHabilite la detección de aplicaciones potencialmente no deseadas: obtenga más información en nuestro artículo de la base de conocimiento.
o**Permitir cambiar la configuración de protección durante la instalación**: le recomendamos que no marque esta casilla.

c.Seleccione la casilla de verificación **Acepto el Acuerdo de licencia de usuario final y confirmo estar de acuerdo con la Política de privacidad**. Consulte el Acuerdo de licencia de usuario final (EULA), los Términos de uso y la Política de privacidad de los productos ESET.
d.**Personalizar más ajustes**:
o**Licencia**: Seleccione la licencia adecuada del producto de la lista de licencias disponibles. La licencia activará el producto de seguridad de ESET durante la instalación. La lista de licencias disponibles no muestra las licencias vencidas o sobreusadas (aquellas que están en estado **Error** u **Obsoleto**). Si no selecciona una licencia, puede instalar el producto de seguridad de ESET sin la licencia y activar el producto más tarde. Puede agregar una licencia a través de uno de los métodos que se describen en Administración de licencias. La adición o eliminación de licencias está restringida al administrador cuyo grupo de pertenencia sea **Todo** y que tenga el permiso de **Escritura** en las licencias.
o**Configuración** De manera opcional, puede seleccionar una **Política** que se aplicará en el producto de ESET Security durante su instalación.
o **Ejecutar ESET AV Remover**: seleccione la casilla de verificación si desea desinstalar o quitar por completo otros programas de antivirus del dispositivo de destino.
o**Instalación de módulos**: es posible que la opción no esté disponible, en función del producto de seguridad de ESET seleccionado. De forma predeterminada, el instalador del producto contiene solo los módulos esenciales de ESET. El resto de los módulos se descargan durante el primer inicio del producto. Marque la casilla de verificación **Usar instalador del producto de seguridad con un conjunto completo de módulos de ESET** para crear el instalador con todos los módulos (para instalaciones sin conexión).

Si ha seleccionado Full Disk Encryption en ESET Inspect en el paso 2, también puede definir su configuración.

Cifrado de disco completo

a.Haga clic en la opción preseleccionada **ESET Full Disk Encryption** y cambie sus detalles:
o Seleccione el idioma en el menú desplegable **Idioma**.
oMarque la casilla de verificación **Avanzada**. De forma predeterminada, se selecciona previamente la versión más reciente (recomendada). Puede seleccionar una versión anterior.
b.Seleccione la casilla de verificación **Acepto el Acuerdo de licencia de usuario final y confirmo estar de acuerdo con la Política de privacidad**. Consulte el Acuerdo de licencia de usuario final (EULA), los Términos de uso y la Política de privacidad de los productos ESET.
c.**Configuración**: seleccione la política que se aplicará a ESET Full Disk Encryption durante la instalación.
d.**Personalizar más ajustes**:
o**Licencia**: Seleccione la licencia adecuada del producto de la lista de licencias disponibles. La licencia activará el producto de seguridad de ESET durante la instalación. La lista de licencias disponibles no muestra las licencias vencidas o sobreusadas (aquellas que están en estado **Error** u **Obsoleto**). Si no selecciona una licencia, puede instalar el producto de seguridad de ESET sin la licencia y activar el producto más tarde. Puede agregar una licencia a través de uno de los métodos que se describen en Administración de licencias. La adición o eliminación de licencias está restringida al administrador cuyo grupo de pertenencia sea **Todo** y que tenga el permiso de **Escritura** en las licencias.

ESET Inspect Connector

Requisitos del conector ESET Inspect:
- Debe tener una licencia ESET Inspect On-Prem para activar el conector ESET Inspect.
- Un producto de seguridad ESET compatible instalado en el equipo administrado.

a.Haga clic en la opción preseleccionada conector **ESET Inspect** y cambie sus detalles:
o Seleccione el idioma en el menú desplegable **Idioma**.
oMarque la casilla de verificación **Avanzada**. De forma predeterminada, se selecciona previamente la versión más reciente (recomendada). Puede seleccionar una versión anterior.

b.Seleccione la casilla de verificación **Acepto el Acuerdo de licencia de usuario final y confirmo estar de acuerdo con la Política de privacidad**. Consulte el Acuerdo de licencia de usuario final (EULA), los Términos de uso y la Política de privacidad de los productos ESET.
c.**Personalizar más ajustes**:
o**Licencia**: Seleccione la licencia adecuada del producto de la lista de licencias disponibles. La licencia activará el producto de seguridad de ESET durante la instalación. La lista de licencias disponibles no muestra las licencias vencidas o sobreusadas (aquellas que están en estado **Error** u **Obsoleto**). Si no selecciona una licencia, puede instalar el producto de seguridad de ESET sin la licencia y activar el producto más tarde. Puede agregar una licencia a través de uno de los métodos que se describen en Administración de licencias. La adición o eliminación de licencias está restringida al administrador cuyo grupo de pertenencia sea **Todo** y que tenga el permiso de **Escritura** en las licencias.
o**Configuración**: haga clic en **Seleccionar** para seleccionar una política existente del conector ESET Inspect o **Crear** para crear una nueva política del conector ESET Inspect. El instalador aplicará la configuración de la política durante la instalación del conector ESET Inspect.
oEscriba el **nombre de host del servidor** ESET Inspect On-Prem y el **puerto** de conexión especificado durante la instalación del servidor ESET Inspect (el puerto predeterminado es 8093).
oSeleccione la **autoridad de certificación** para la conexión al servidor ESET Inspect.

10. Haga clic en **Finalizar**.
11. Descargue el paquete de instalación todo en uno generado. Seleccione la versión que desee instalar:

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

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

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

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

12. Luego de crear y descargar el paquete instalador todo en uno, hay dos opciones para implementar el agente ESET Management:

- Localmente en un equipo cliente Ejecute el archivo del paquete de instalación en un equipo del cliente. Se instalará el agente de ESET Management y el producto de ESET Security en el dispositivo, y podrá conectarse a ESET PROTECT On-Prem. El instalador de ESET Endpoint Antivirus/Security creado en ESET PROTECT On-Prem 8.1 y versiones posteriores es compatible con Windows 10 Enterprise para escritorios virtuales y el modo de varias sesiones de Windows 10. Para obtener instrucciones paso a paso, consulte el asistente de configuración. Puede ejecutar el paquete de instalación en un modo silencioso para ocultar la ventana del asistente de configuración.

- Utilizando la Herramienta de implementación remota de ESET para implementar los ESET Management Agent en diferentes equipos cliente al mismo tiempo.

Crear instalador de scripts del agente - Windows/Linux/macOS

Este tipo de implementación del Agente es útil cuando las opciones de implementación local y remota no son adecuadas para usted. Puede distribuir el instalador del script del agente por correo electrónico y dejar que el usuario lo instale. También puede ejecutar el instalador del script del agente desde un medio extraíble (una unidad de memoria USB, por ejemplo).

El equipo cliente necesita una conexión a Internet para descargar el paquete de instalación del agente y conectarse al ESET PROTECT On-Prem.

Puede crear el instalador de scripts del agente para Windows/macOS/Linux de diferentes formas:

- **Enlaces rápidos** > **Implementar agente**

- **Instaladores** > **Crear instalador** > **Windows/macOS//Linux** > **Implemente primero el agente (instalador de scripts del agente)**

- Recorrido por ESET PROTECT On-Prem

1. Seleccione la casilla de verificación **Participar en el programa de mejora del producto** para 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).

2. **Grupo principal:** seleccione el grupo principal en el que la consola web de ESET PROTECT colocará el equipo la instalación de un agente.

- Puede seleccionar un grupo estático existente o crear uno nuevo al que se le asignará el dispositivo luego de implementar el instalador.
- Si selecciona un grupo principal, se agregarán al instalador todas las políticas aplicadas al grupo.
- La selección del grupo principal no afecta a la ubicación del instalador. Después de crear el instalador, se coloca en el grupo de acceso del usuario actual. El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario.
- El grupo principal es obligatorio si utiliza ESET Business Account con sitios o ESET MSP Administrator y opcional si utiliza ESET Business Account sin sitios.

3. **Nombre de host del servidor (opcional)**: escriba el nombre de host o la dirección IP del servidor de ESET PROTECT. De ser necesario, especifique el número de **Puerto** (el predeterminado es 2222).

> ⚠ El campo **Nombre de host del servidor** no admite caracteres especiales, por ejemplo, letras con signos diacríticos.

4. **Certificado de pares**:

- **certificado ESET PROTECT**: se seleccionan automáticamente un certificado de pares para la instalación del agente y la autoridad de certificación de ESET PROTECT. Para utilizar un certificado diferente, haga clic en **Descripción del certificado de ESET PROTECT** para seleccionarlo en el menú desplegable de los certificados disponibles.
- **Certificado personalizado**: si utiliza un certificado personalizado para la autenticación, haga clic en **Certificado personalizado** > **Seleccionar**, cargue el certificado .pfx y selecciónelo al instalar el agente. Para obtener más información, consulte Certificados.

Frase de contraseña del certificado: escriba la frase de contraseña del certificado si es necesario: si especificó la contraseña durante la instalación del servidor ESET PROTECT (en el paso en el que creó una autoridad certificadora) o si utiliza un certificado personalizado con contraseña. De lo contrario, deje el campo **Frase de contraseña del certificado** en blanco.

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

5. Personalizar más ajustes

- Escriba el **Nombre del instalador** y la **Descripción** (opcional).
- Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
- **Configuración inicial (opcional):** utilice esta opción para aplicar una política de configuración al agente de ESET Management. Haga clic en **Seleccionar** dentro de **Configuración del agente** y elija entre la lista de políticas disponibles. Si ninguna de las políticas definidas previamente son adecuadas, puede crear una nueva política o personalizar las existentes.
- Si usa un proxy HTTP (recomendamos usar ESET Bridge), seleccione la casilla de verificación **Habilitar la configuración del proxy HTTP** y especifique la configuración del proxy (**Host**, **Puerto**, **Nombre de usuario** y **Contraseña**) para descargar el instalador a través del proxy y definir la conexión del agente ESET Management al proxy para habilitar el reenvío de comunicaciones entre el agente ESET Management y el servidor ESET PROTECT. El campo **Host** es la dirección del equipo que ejecuta el proxy HTTP. ESET Bridge usa el puerto 3128 de forma predeterminada. Puede definir otro puerto, de ser necesario. Asegúrese de configurar el mismo puerto también en la configuración del proxy de HTTP (consulta la ESET Bridge Política).

> 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.

La casilla de verificación **Utilice una conexión directa si el proxy HTTP no está disponible** está preseleccionada. El asistente aplica la configuración como alternativa para el instalador: no puede anular la selección de la casilla de verificación. Puede deshabilitar la configuración mediante una política de agente de ESET Management:

- Durante la creación del instalador: incluya la política en la **Configuración inicial**.
- Tras la ESET Management instalación del agente: asigne la política al equipo.

6. Haga clic en **Guardar y descargar**.

7. Extraiga el archivo comprimido descargado en el equipo del cliente en el que desea implementar el agente ESET Management.

8. Ejecute el script *PROTECTAgentInstaller.bat* (Windows) o *PROTECTAgentInstaller.sh* (Linux o macOS) para instalar el agente. Siga las instrucciones detalladas de instalación del agente:

- Instalación del agente: Windows
- Instalación del agente – Linux
- Instalación del agente: macOS

> ESET PROTECT On-Prem admite la actualización automática de agentes ESET Management en equipos administrados.

Instalación desde una ubicación remota personalizada

Para implementar el agente desde una ubicación que no sea el repositorio de ESET, modifique el script de instalación para especificar la nueva URL donde se encuentra el paquete del agente. También puede usar la dirección IP del nuevo paquete.
Busque y modifique las siguientes líneas:
Windows:

```
set url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent_x64.msi
set url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent_x86.msi
set url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent_arm64.msi
```

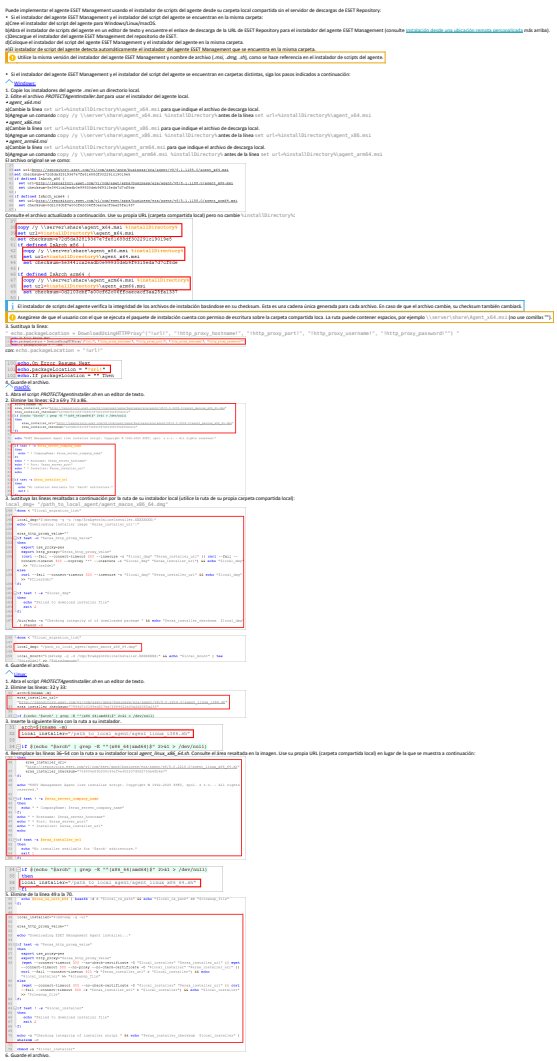
Linux:

```
eraa_installer_url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent-linux-i386.sh
eraa_installer_url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent-linux-x86_64.sh
```

macOS:

```
eraa_installer_url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent_macosx_x86_64.dmg
eraa_installer_url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent-macosx-x86_64_arm64.dmg
```

Instalación desde una carpeta compartida local



Instalación del agente: Windows

1. Descargue el script instalador del agente en el equipo cliente.

2. Extraiga el archivo *PROTECTAgentinstaller.bat* del archivo: *PROTECTAgentinstaller.zip*.

3. Haga doble clic en el archivo por lotes extraído para instalar el agente ESET Management.

4. Compruebe el archivo de registro *status.html* en el equipo cliente que se encuentra en *C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html* para asegurarse de que el agente ESET Management funcione correctamente.

5. El equipo con el agente instalado aparecerá en su consola web de ESET PROTECT y podrá administrarlo con ESET PROTECT On-Prem.

- Si hay problemas con el Agente (por ejemplo, si no se conecta con el servidor de ESET PROTECT), consulte la Resolución de problemas.
- ESET PROTECT On-Prem admite la actualización automática de agentes ESET Management en equipos administrados.

Instalación del agente – Linux

Requisitos previos

- Debe poder acceder al equipo desde la red.
- Le recomendamos **usar la versión más reciente de OpenSSL1.1.1**. El agente ESET Management admite OpenSSL 3.x. 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`

> **OpenSSL 3.x soporte**
> - ESET Management El agente admite OpenSSL 3.x.
> - El servidor/la administración de dispositivos móviles (MDM) de ESET PROTECT no admite OpenSSL 3.x de forma nativa, pero puede habilitar la compatibilidad con OpenSSL 3.x para ESET PROTECT On-Prem.

- Instale el paquete `lshw` en el equipo Linux cliente/servidor para que el agente ESET Management informe correctamente el 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

Realice la instalación del componente del agente ESET Management en Linux usando un comando en el terminal.

> 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.

Siga los pasos a continuación para instalar el Agente en la estación de trabajo Linux.

1. Descargue el script instalador del agente en el equipo cliente.
2. Extraiga el archivo *.sh* del archivo *.gz*: `tar -xvzf PROTECTAgentInstaller.tar.gz`

3. Configure el archivo de instalación del Agente ESET Management *.sh* como ejecutable: `chmod +x PROTECTAgentInstaller.sh`

4. Ejecute el archivo *.sh* o ejecute el comando de terminal: `sudo ./PROTECTAgentInstaller.sh`

5. Cuando se le indique, escriba la contraseña del administrador local y pulse **Intro**.

6. Una vez completada la instalación del agente, ejecute el siguiente comando en la ventana de terminal para verificar que el agente se esté ejecutando: `sudo systemctl status eraagent`

7. El equipo con el agente instalado aparecerá en su consola web de ESET PROTECT y podrá administrarlo con ESET PROTECT On-Prem.

Si el equipo con el agente instalado no aparece en su ESET PROTECT On-Prem, lleve a cabo la resolución de problemas.

ESET PROTECT On-Prem admite la actualización automática de agentes ESET Management en equipos administrados.

Instalación del agente: macOS

1. Descargue el script instalador del agente en el equipo cliente.

2. Haga doble clic en *PROTECTAgentInstaller.tar.gz* para extraer el archivo *PROTECTAgentInstaller.sh* en su escritorio.

3. Haga clic en **Ir** > **Utilidades** y, a continuación, haga doble clic en Terminal para abrir una nueva ventana de terminal.

4. Habilitar acceso total al terminal:

   a)Abra las **Preferencias del sistema** > **Seguridad y privacidad** > **Privacidad**.

   b)Desbloquee la configuración en la esquina inferior izquierda.

   c)Haga clic en **Acceso total al disco**.

   d)Haga clic en **+** > **Aplicación** > y agregue el **Terminal** a la lista de aplicaciones en la carpeta **Acceso total al disco**.

   e)Bloquee la configuración en la esquina inferior izquierda.

5. En la nueva ventana de terminal, escriba los siguientes comandos:

```
cd Desktop

sudo bash PROTECTAgentInstaller.sh
```

6. Cuando se le solicite, escriba la contraseña de la cuenta de usuario y pulse **Volver** para continuar con la instalación.

7. Habilite el acceso total al disco para el agente ESET Management:

Localmente:

a)Abra las **Preferencias del sistema** > **Seguridad y privacidad** > **Privacidad**.

b)Desbloquee la configuración en la esquina inferior izquierda.

c)Haga clic en **Acceso total al disco**.

d)Haga clic en **+** > **Aplicación** > **ESET** > **Abrir** y agregue el agente de ESET Management a la lista de aplicaciones en la carpeta **Acceso total al disco**.

e)Bloquee la configuración en la esquina inferior izquierda.

Remotamente:

a)Descargue el archivo de configuración .plist.

b)Genere dos UUID con un generador de UUID de su elección y use un editor de texto para sustituir cadenas con el texto. Introduzca su UUID 1 y UUID 2 en el perfil de configuración descargado.

c)Implemente el archivo de perfil de configuración .plist con el servidor de administración de dispositivos móviles. Su equipo debe estar inscrito en el servidor de administración de dispositivos móviles para implementar perfiles de configuración en equipos.

8. El equipo con el agente instalado aparecerá en su consola web de ESET PROTECT y podrá administrarlo con ESET PROTECT On-Prem.

Se instalará un agente ARM64 ESET Management nativo (versión 9.1 y posteriores) en los sistemas ARM64macOS.
ESET PROTECT On-Prem admite la actualización automática de agentes ESET Management en equipos administrados.

Resolución de problemas de Instalación del agente

Compruebe que el agente esté en ejecución: Haga clic en **Ir** > **Utilidades** y, a continuación, haga doble clic en **Monitor de actividad**. Haga clic en la pestaña **Energía** o en la pestaña **CPU** y localice el proceso llamado **ERAAgent**.

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.

Descargar desde el sitio web de ESET

Descargue el paquete de instalación del agente ESET Management desde el sitio web de ESET. Seleccione el paquete adecuado en función del SO de su equipo cliente:

- Linux instalación asistida por el servidor y fuera de línea
- macOS
- Windows

  - Instalación asistida del servidor: mediante el paquete de instalación del agente, este método descarga certificados desde el servidor ESET PROTECT de forma automática (se recomienda para implementación local).

> - No puede usar un usuario con autenticación de dos factores para instalaciones asistidas por el servidor.
> - Si decide permitir la instalación asistida por servidor por parte de otro usuario, asegúrese de tener configurados los siguientes permisos:
>
> El usuario debe tener permisos de Uso para la autoridad de certificación que firmó el certificado de pares del servidor y permisos de Uso para, al menos, un certificado de pares. Si no existe dicho certificado, el usuario deberá contar con permisos de Escritura para crear uno nuevo.
>
> Permisos de **Escritura** para el grupo estático al que el usuario desea agregar el equipo.

  - Instalación fuera de línea: con el paquete de instalación del agente. Debe exportar manualmente los certificados y aplicarlos en este método de implementación.

Compruebe el registro de estado en un equipo cliente (ubicado en *C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.html*) para comprobar si el agente ESET Management funciona adecuadamente.

> En caso de que hubiera problemas con el agente (por ejemplo, si no se conecta al servidor ESET PROTECT), consulte la sección Solución de problemas: implementación del agente.

Implementación remota

La implementación remota se puede realizar de las siguientes maneras:

- ESET Remote Deployment Tool: esta herramienta le permite implementar los paquetes del instalador del agente ESET Management (y el producto de seguridad de ESET) creados en la consola web de ESET PROTECT.
- Objeto de política de grupo (GPO) y Administrador de configuración del centro de sistema (SCCM) - Utilice esta opción para la instalación masiva del agente ESET Management en equipos del cliente.
- Tarea del servidor Instalación del agente: una alternativa al método GPO y SCCM.

Si tiene problemas al implementar el agente ESET Management en forma remota (la tarea de servidor **Implementación del agente** falla), consulte los siguientes:

- Resolución de problemas: implementación del Agente
- Resolución de problemas: conexión del Agente
- Escenarios de ejemplo de implementación del agente ESET Management

Implementación remota y permisos

Si desea permitir a un usuario crear instaladores GPO o scripts SCCM, configure sus permisos para que sean iguales a los de nuestro ejemplo.

Se necesitan los siguientes permisos para la implementación de agente de tarea del servidor:

- Permiso de **Escritura** para **Grupos y equipos** donde se ejecute la implementación
- Permisos de **Uso** para **Certificados** con acceso al grupo estático donde se contienen los certificados
- Permisos de **Uso** para **Implementación de agente** en la sección **Tareas del servidor y desencadenadores**

Instalación del agente con GPO o SCCM

Además de la implementación local, también puede usar herramientas de administración como Objetivo de política de grupo (GPO), Software Center Configuration Manager (SCCM), Symantec Altiris o Puppet para la instalación remota del agente.

Utilice esta opción para la instalación masiva del agente ESET Management en equipos del cliente.

Puede crear un script de GPO/SCCM para la instalación del agente en Windows desde **Enlaces rápidos** > **Implementar agente** o **Instaladores** > **Crear instalador**.

1. Haga clic en **Windows** > **Usar GPO o SCCM para la instalación**.

2. Seleccione la casilla de verificación **Participar en el programa de mejora del producto** para 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).

3. **Grupo principal:** seleccione el grupo principal en el que la consola web de ESET PROTECT colocará el equipo la instalación de un agente.

   - Puede seleccionar un grupo estático existente o crear uno nuevo al que se le asignará el dispositivo luego de implementar el instalador.
   - Si selecciona un grupo principal, se agregarán al instalador todas las políticas aplicadas al grupo.
   - La selección del grupo principal no afecta a la ubicación del instalador. Después de crear el instalador, se coloca en el grupo de acceso del usuario actual. El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario.
   - El grupo principal es obligatorio si utiliza ESET Business Account con sitios o ESET MSP Administrator y

opcional si utiliza ESET Business Account sin sitios.

4. **Nombre de host del servidor (opcional)**: escriba el nombre de host o la dirección IP del servidor de ESET PROTECT. De ser necesario, especifique el número de **Puerto** (el predeterminado es 2222).

> ⚠ El campo **Nombre de host del servidor** no admite caracteres especiales, por ejemplo, letras con signos diacríticos.

5. **Certificado de pares**:

- **certificado ESET PROTECT**: se seleccionan automáticamente un certificado de pares para la instalación del agente y la autoridad de certificación de ESET PROTECT. Para utilizar un certificado diferente, haga clic en **Descripción del certificado de ESET PROTECT** para seleccionarlo en el menú desplegable de los certificados disponibles.

- **Certificado personalizado**: si utiliza un certificado personalizado para la autenticación, haga clic en **Certificado personalizado** > **Seleccionar**, cargue el certificado .pfx y selecciónelo al instalar el agente. Para obtener más información, consulte Certificados.

Frase de contraseña del certificado: escriba la frase de contraseña del certificado si es necesario: si especificó la contraseña durante la instalación del servidor ESET PROTECT (en el paso en el que creó una autoridad certificadora) o si utiliza un certificado personalizado con contraseña. De lo contrario, deje el campo **Frase de contraseña del certificado** en blanco.

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

6. Personalizar más ajustes

- Escriba el **Nombre del instalador** y la **Descripción** (opcional)
- Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
- **Configuración inicial (opcional):** utilice esta opción para aplicar una política de configuración al agente de ESET Management. Haga clic en **Seleccionar** dentro de **Configuración del agente** y elija entre la lista de políticas disponibles. Si ninguna de las políticas definidas previamente son adecuadas, puede crear una nueva política o personalizar las existentes.
- Si usa un proxy HTTP (recomendamos usar ESET Bridge), seleccione la casilla de verificación **Habilitar la configuración del proxy HTTP** y especifique la configuración del proxy (**Host**, **Puerto**, **Nombre de usuario** y **Contraseña**) para descargar el instalador a través del proxy y definir la conexión del agente ESET Management al proxy para habilitar el reenvío de comunicaciones entre el agente ESET Management y el servidor ESET PROTECT. El campo **Host** es la dirección del equipo que ejecuta el proxy HTTP. ESET Bridge usa el puerto 3128 de forma predeterminada. Puede definir otro puerto, de ser necesario. Asegúrese de configurar el mismo puerto también en la configuración del proxy de HTTP (consulta la ESET Bridge Política).

> ⚠ 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.

La casilla de verificación **Utilice una conexión directa si el proxy HTTP no está disponible** está preseleccionada. El asistente aplica la configuración como alternativa para el instalador: no puede anular la selección de la casilla de verificación. Puede deshabilitar la configuración mediante una política de agente de ESET Management:
- Durante la creación del instalador: incluya la política en la **Configuración inicial**.
- Tras la ESET Management instalación del agente: asigne la política al equipo.

7. Haga clic en **Finalizar**.

8. Descargue el script de GPO/SCCM y los instaladores del agente (32 bits, 64 bits, ARM64). Descargue el archivo del instalador del **agente** *.msi* de la página de descarga de ESET, sección instaladores independientes.

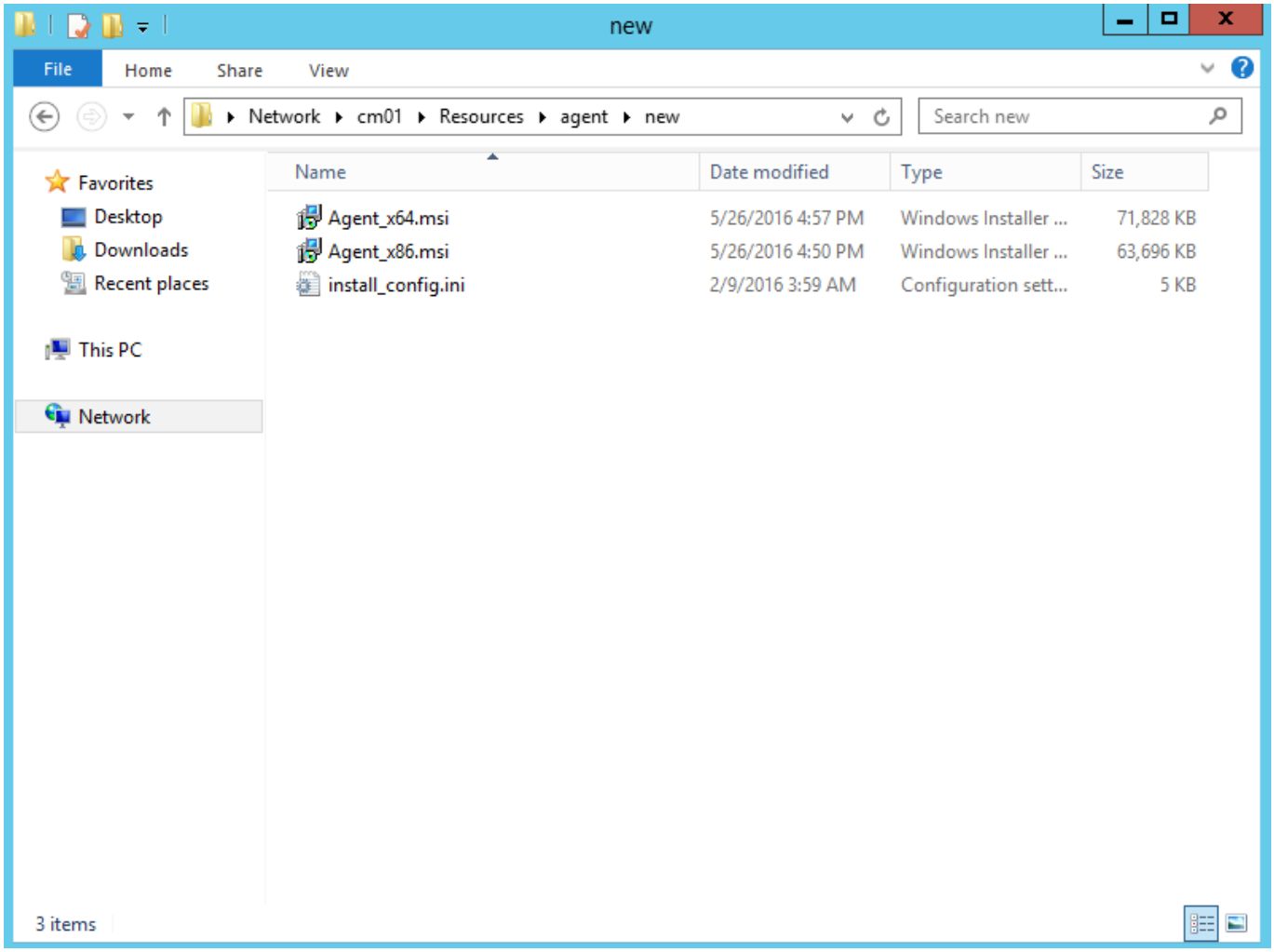
Haga clic en el enlace adecuado a continuación para acceder a las instrucciones paso a paso para dos métodos de instalación remota populares del agente ESET Management:

- Instalación del agente de ESET Management por medio del Objeto de política de grupo (GPO). Es posible que este artículo de la base de conocimiento no esté disponible en su idioma.
- Instalación del agente de ESET Management por medio de System Center Configuration Manager (SCCM)

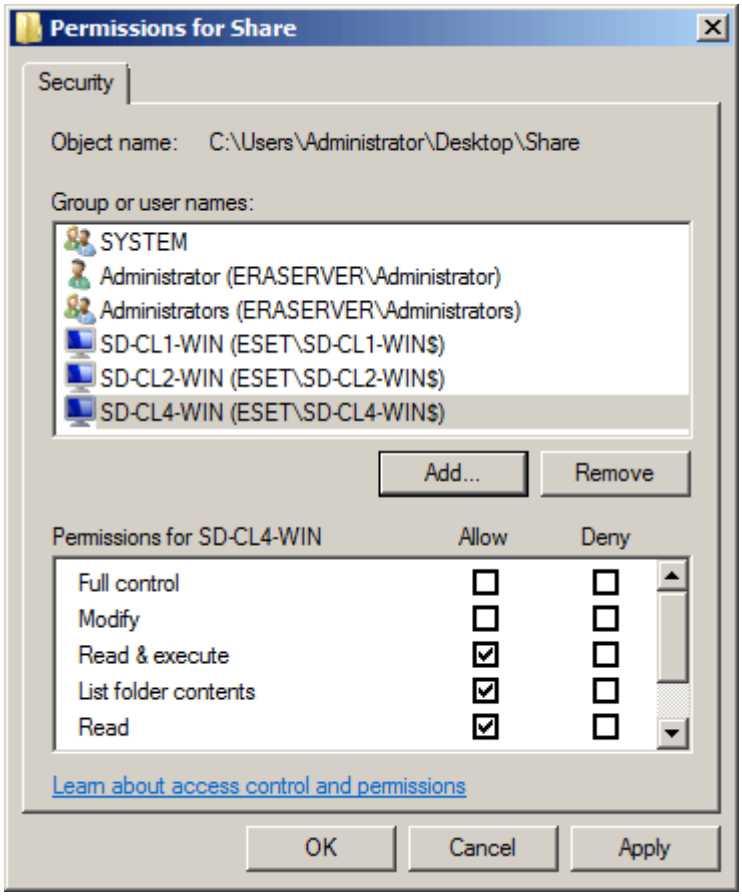
Pasos de la implementación: SCCM

Para implementar el agente ESET Management usando SCCM, siga los siguientes pasos:

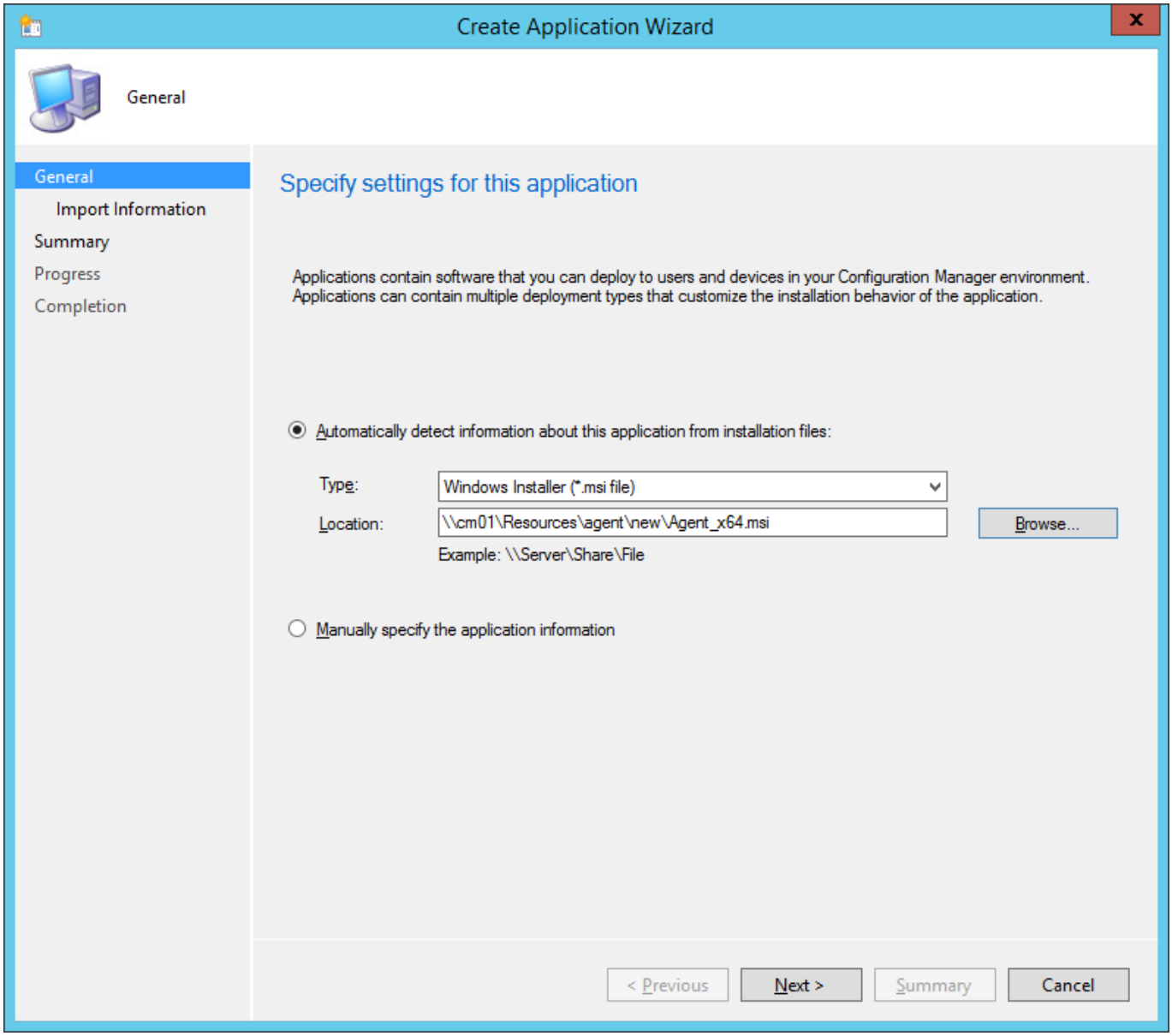
1. Guarde el archivo *.msi* del instalador del agente ESET Management y el archivo *install_config.ini* en una carpeta compartida.



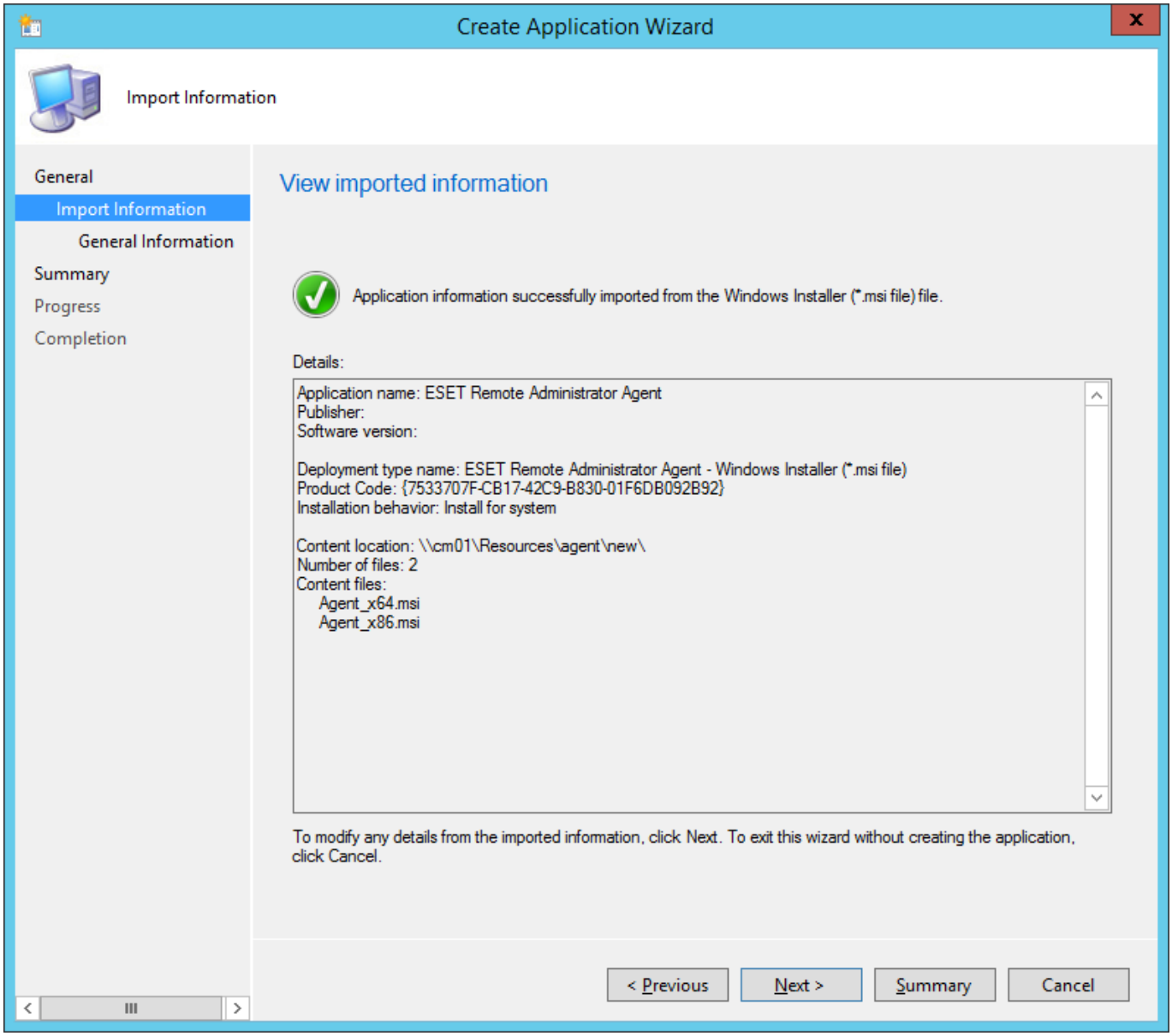
Los equipos cliente necesitarán acceso de lectura/ejecución para acceder a esta carpeta compartida.



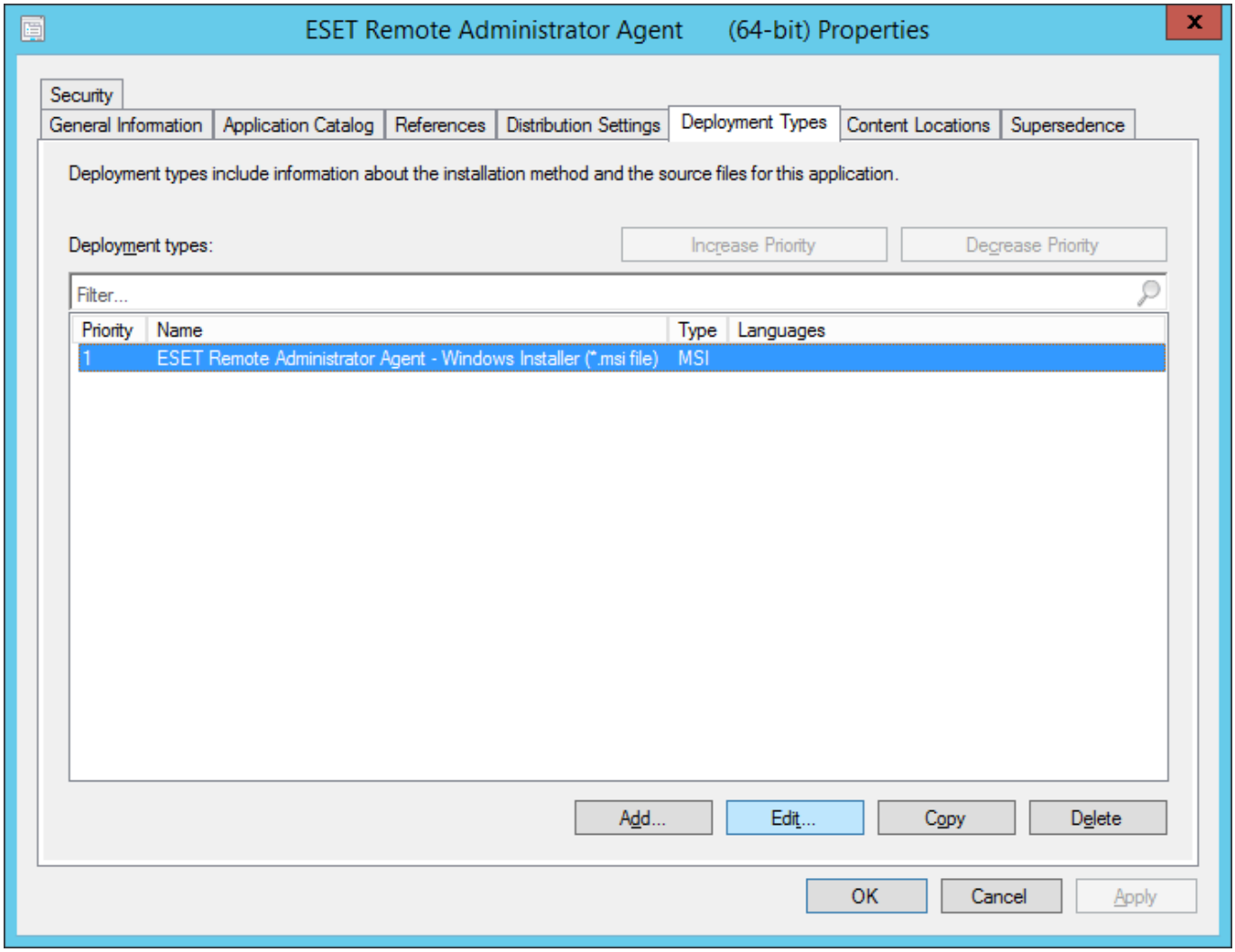
2. Abra la consola SCCM y haga clic en **Biblioteca de software**. En **Administración de aplicaciones** haga clic con el botón secundario en **Aplicaciones** y seleccione **Crear aplicación**. Elija **Windows Installer (*archivo .msi)**.



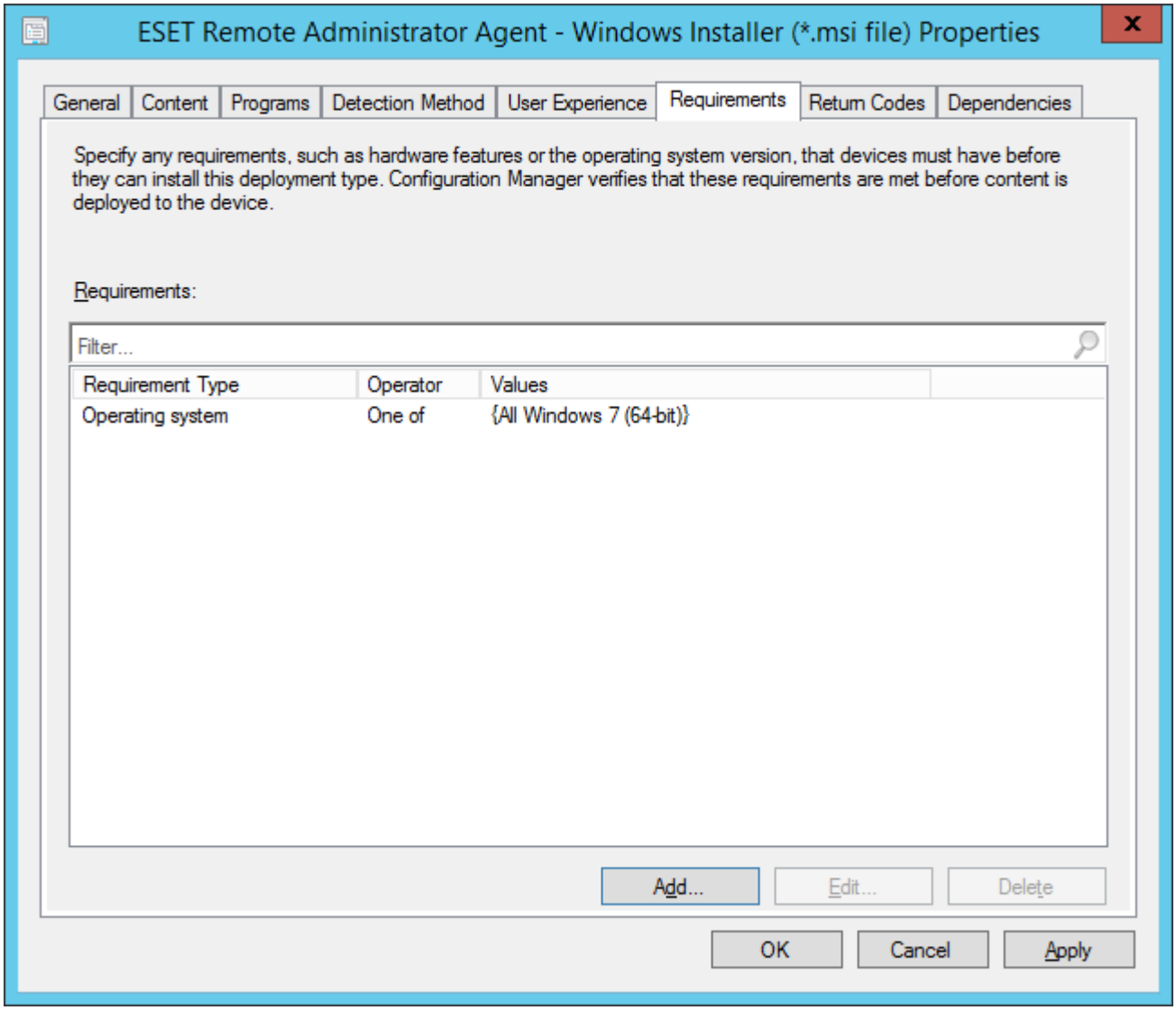
3. Especifique toda la información necesaria sobre la aplicación y haga clic en **Siguiente**.

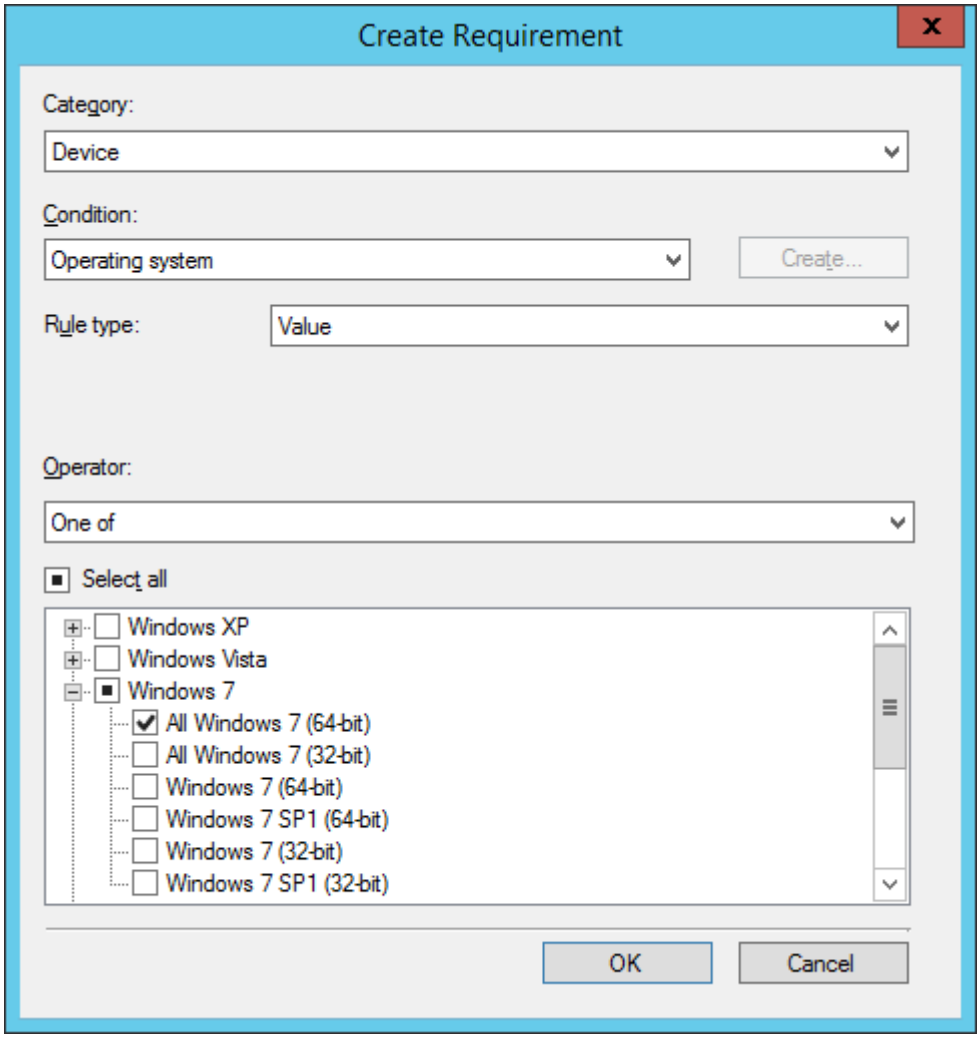


4. Haga clic con el botón secundario en la aplicación del agente ESET Management, haga clic en la pestaña **Tipos de implementación**, seleccione la única implementación disponible y haga clic en **Editar**.

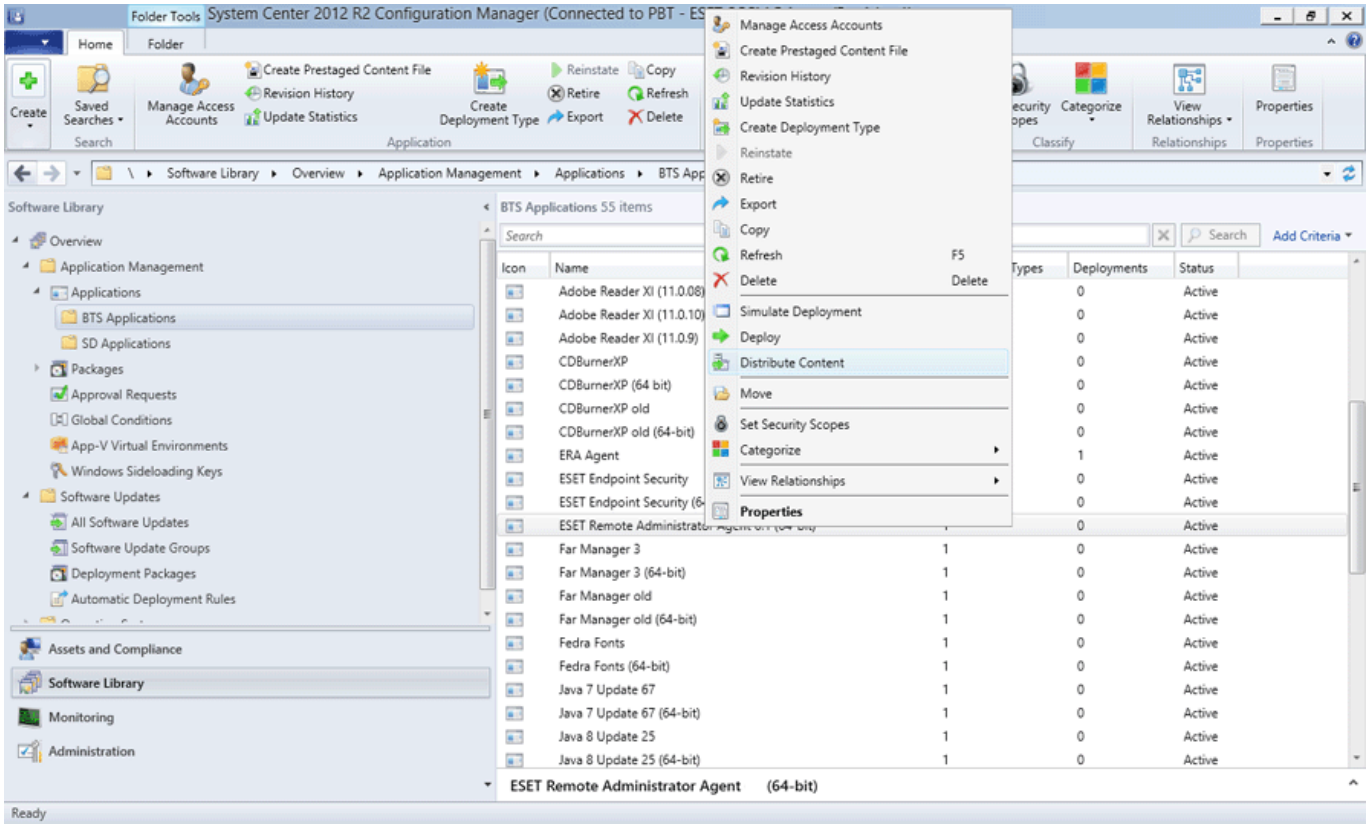


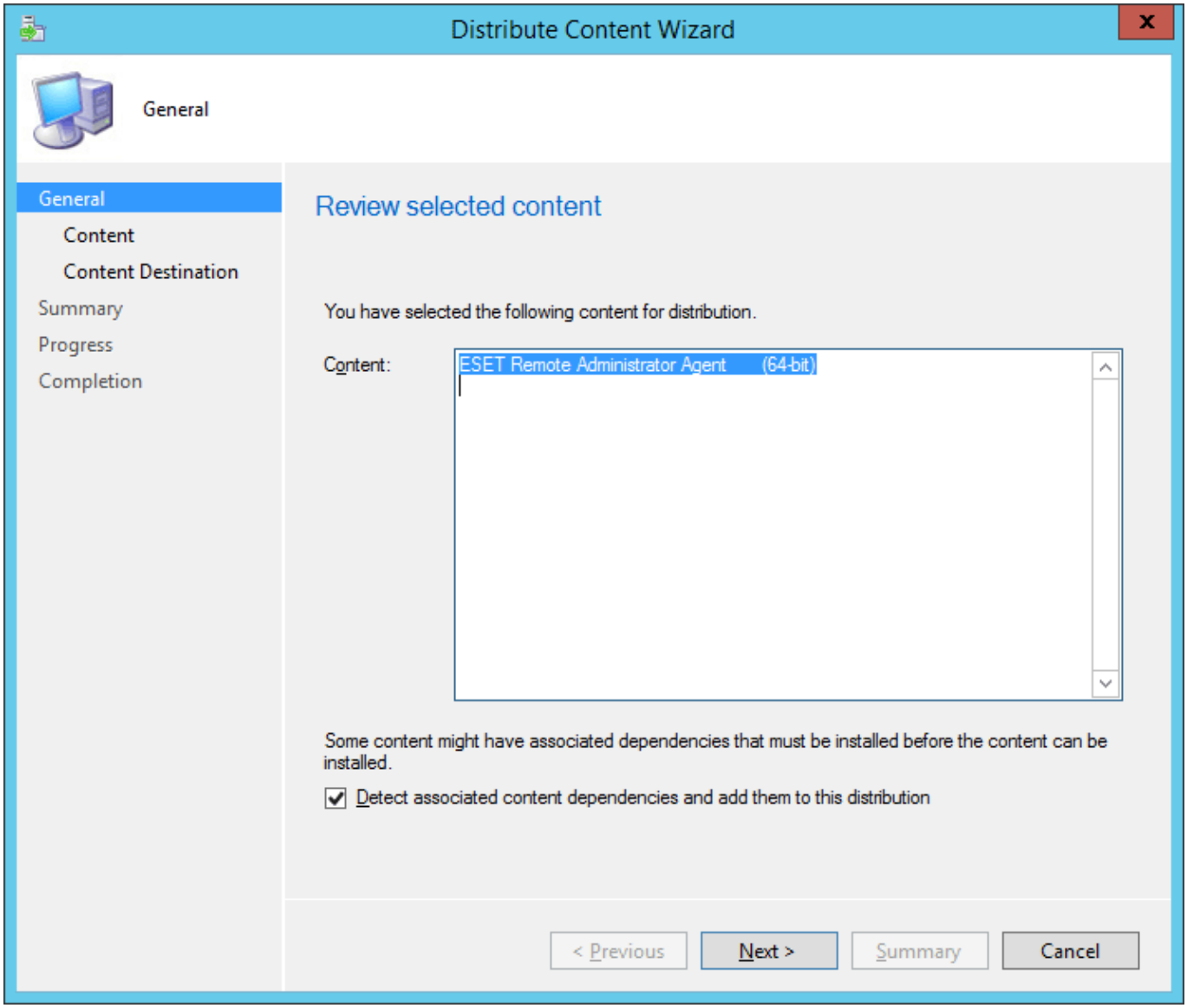
5. Haga clic en la pestaña **Requisitos** y luego haga clic en **Agregar**. Seleccione **Sistema operativo** en el menú desplegable **Condición**, seleccione **Uno de** del menú desplegable **Operador** y especifique los sistemas operativos que instalará al seleccionar las casillas de verificación correspondientes. Haga clic en **Aceptar** una vez finalizado y, luego, en **Aceptar** para cerrar cualquier ventana restante y guardar los cambios.

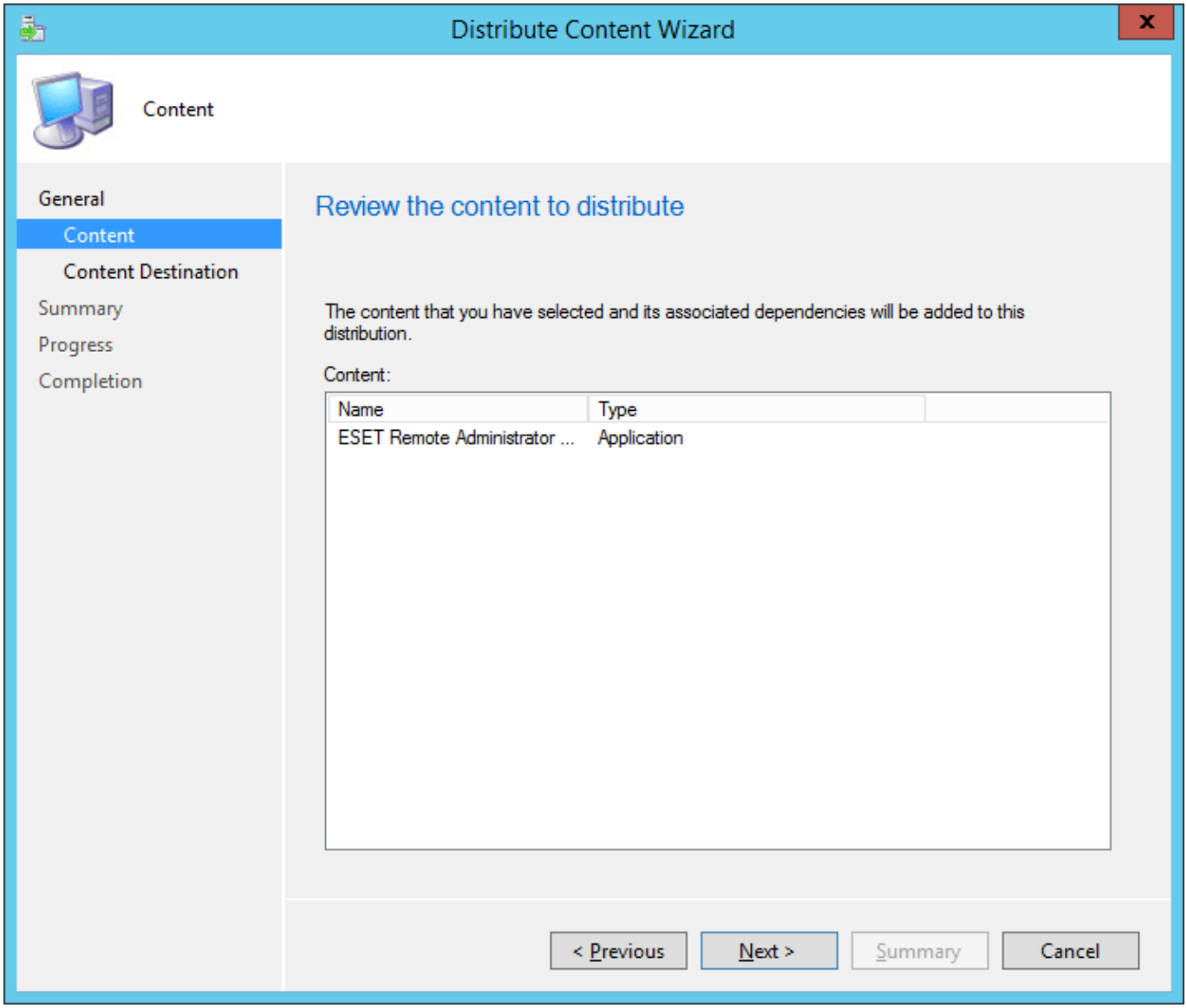

ESET Remote Administrator Agent - Windows Installer (*.msi file) Properties
General
Content
Programs
Detection Method
User Experience
Requirements
Return Codes
Dependencies
Specify any requirements, such as hardware features or the operating system version, that devices must have before they can install this deployment type. Configuration Manager verifies that these requirements are met before content is deployed to the device.
Requirements:
Filter...
Requirement Type
Operator
Values
Operating system
One of
{All Windows 7 (64-bit)}
Add...
Edit...
Delete
OK
Cancel
Apply



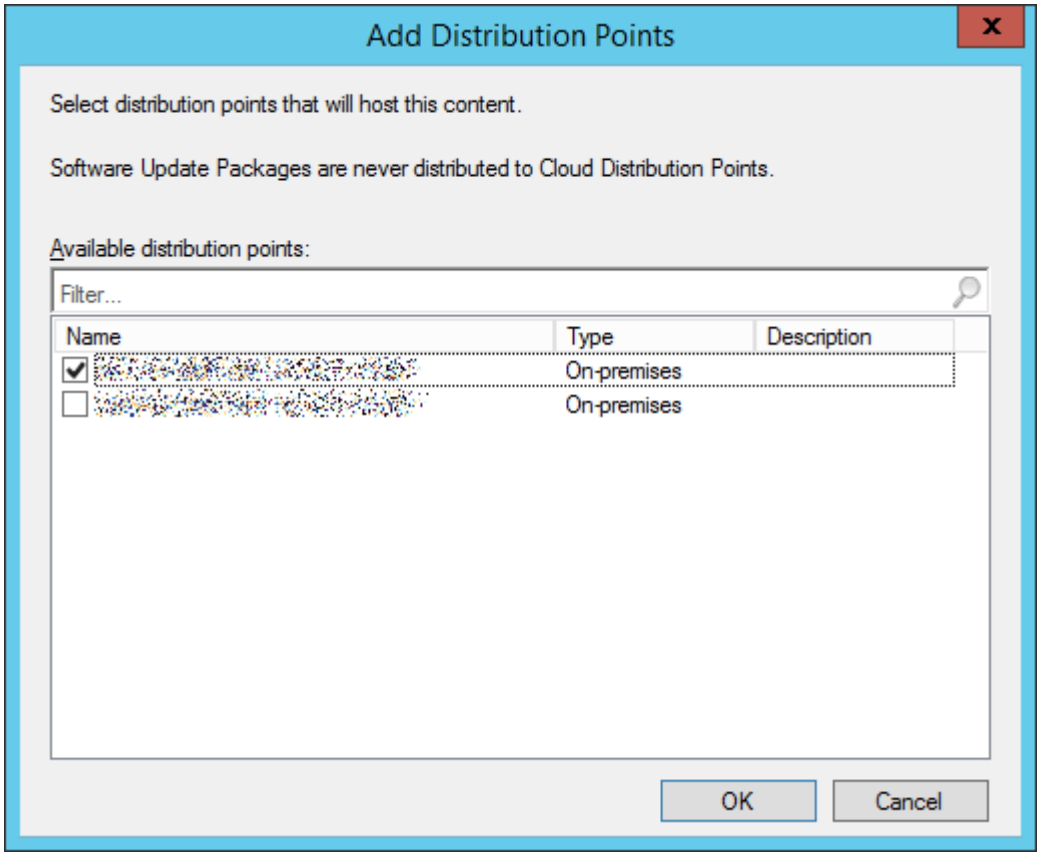
6. En la biblioteca de software del centro del sistema, haga clic con el botón secundario en su nueva aplicación y seleccione **Distribuir contenido** en el menú desplegable. Siga las indicaciones del Asistente de implementación de software para finalizar la implementación de la aplicación.

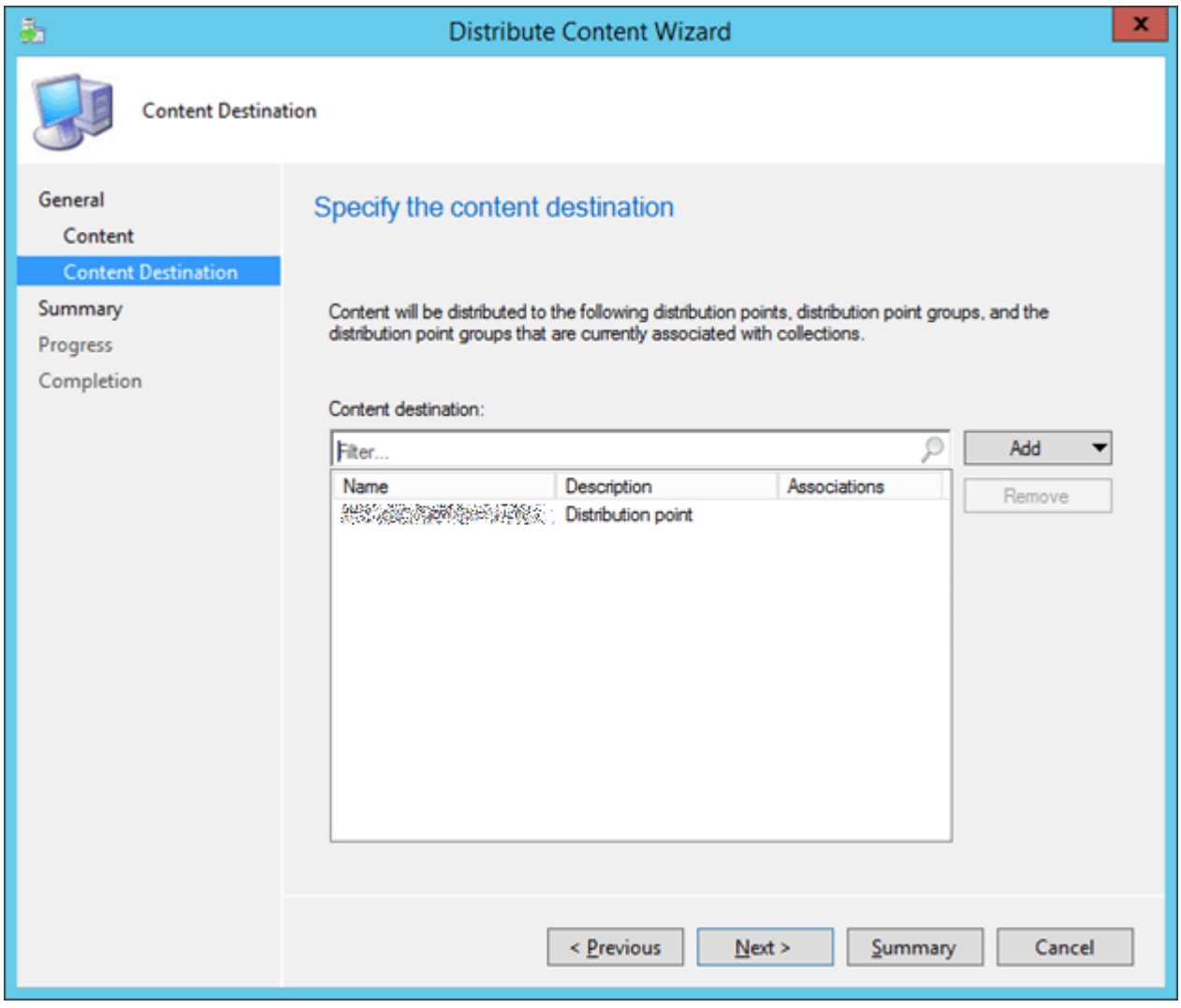

Folder Tools
System Center 2012 R2 Configuration Manager (Connected to PBT - ES
Home
Folder
Create
Saved Searches
Manage Access Accounts
Create Prestaged Content File
Revision History
Update Statistics
Create Deployment Type
Reinstate
Retire
Export
Copy
Refresh
Delete
Search
Application
Categorize
View Relationships
Properties
Classify
Relationships
Properties
Software Library ▸ Overview ▸ Application Management ▸ Applications ▸ BTS App
Software Library
Overview
Application Management
Applications
BTS Applications
SD Applications
Packages
Approval Requests
Global Conditions
App-V Virtual Environments
Windows Sideloading Keys
Software Updates
All Software Updates
Software Update Groups
Deployment Packages
Automatic Deployment Rules
Assets and Compliance
Software Library
Monitoring
Administration
BTS Applications 55 items
Search
Add Criteria
Icon
Name
Types
Deployments
Status
Adobe Reader XI (11.0.08) 0 Active
Adobe Reader XI (11.0.10) 0 Active
Adobe Reader XI (11.0.9) 0 Active
CDBurnerXP 0 Active
CDBurnerXP (64 bit) 0 Active
CDBurnerXP old 0 Active
CDBurnerXP old (64-bit) 0 Active
ERA Agent 1 Active
ESET Endpoint Security 0 Active
ESET Endpoint Security (6 0 Active
ESET Remote Administrator 0 Active
Far Manager 3 1 0 Active
Far Manager 3 (64-bit) 1 0 Active
Far Manager old 1 0 Active
Far Manager old (64-bit) 1 0 Active
Fedra Fonts 1 0 Active
Fedra Fonts (64-bit) 1 0 Active
Java 7 Update 67 1 0 Active
Java 7 Update 67 (64-bit) 1 0 Active
Java 8 Update 25 1 0 Active
Java 8 Update 25 (64-bit) 1 0 Active
ESET Remote Administrator Agent (64-bit)
Ready
Manage Access Accounts
Create Prestaged Content File
Revision History
Update Statistics
Create Deployment Type
Reinstate
Retire
Export
Copy
Refresh F5
Delete Delete
Simulate Deployment
Deploy
Distribute Content
Move
Set Security Scopes
Categorize
View Relationships
Properties

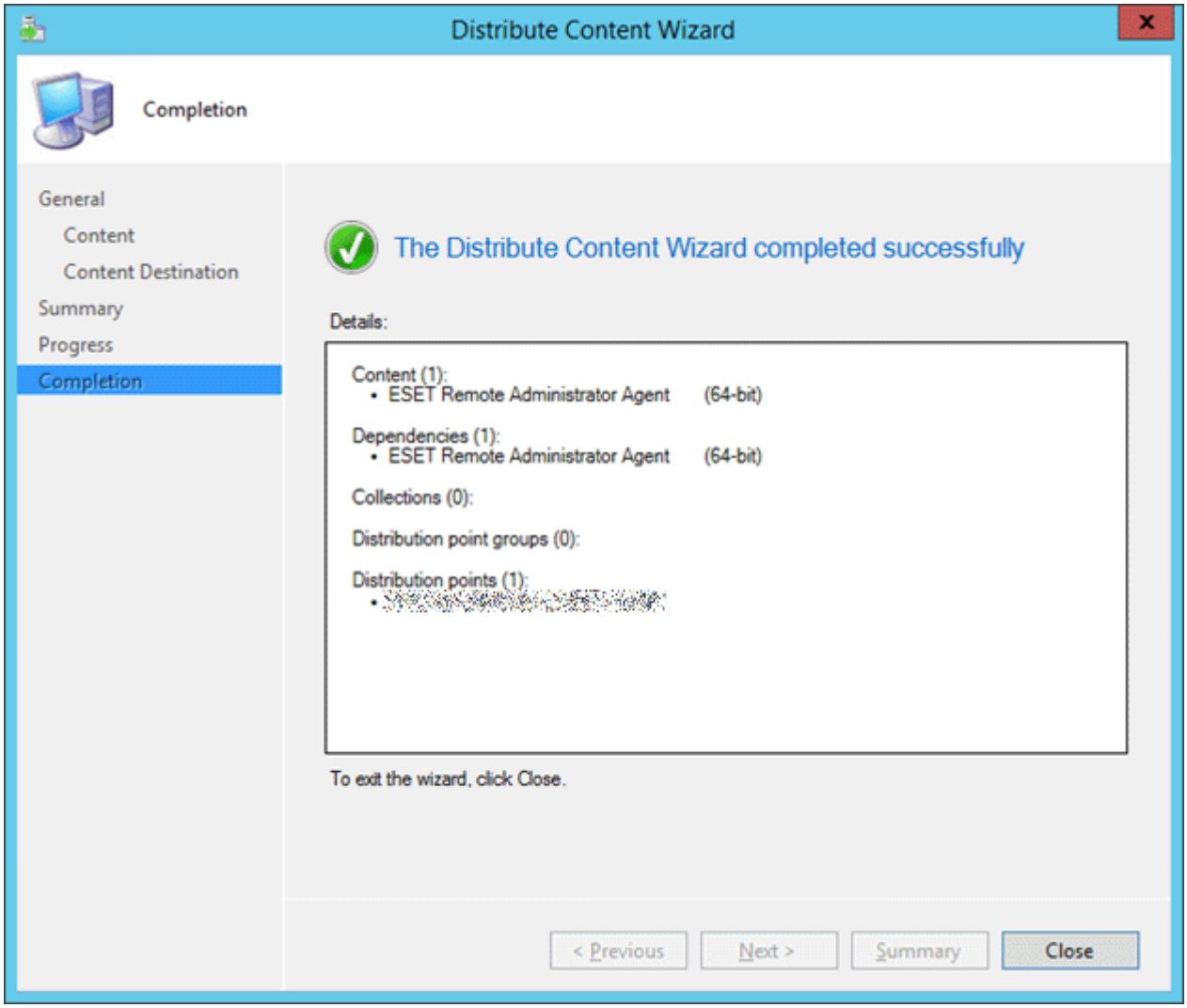

Distribute Content Wizard
General
General
Content
Content Destination
Summary
Progress
Completion
Review selected content
You have selected the following content for distribution.
Content:
ESET Remote Administrator Agent (64-bit)
Some content might have associated dependencies that must be installed before the content can be installed.
Detect associated content dependencies and add them to this distribution
< Previous
Next >
Summary
Cancel

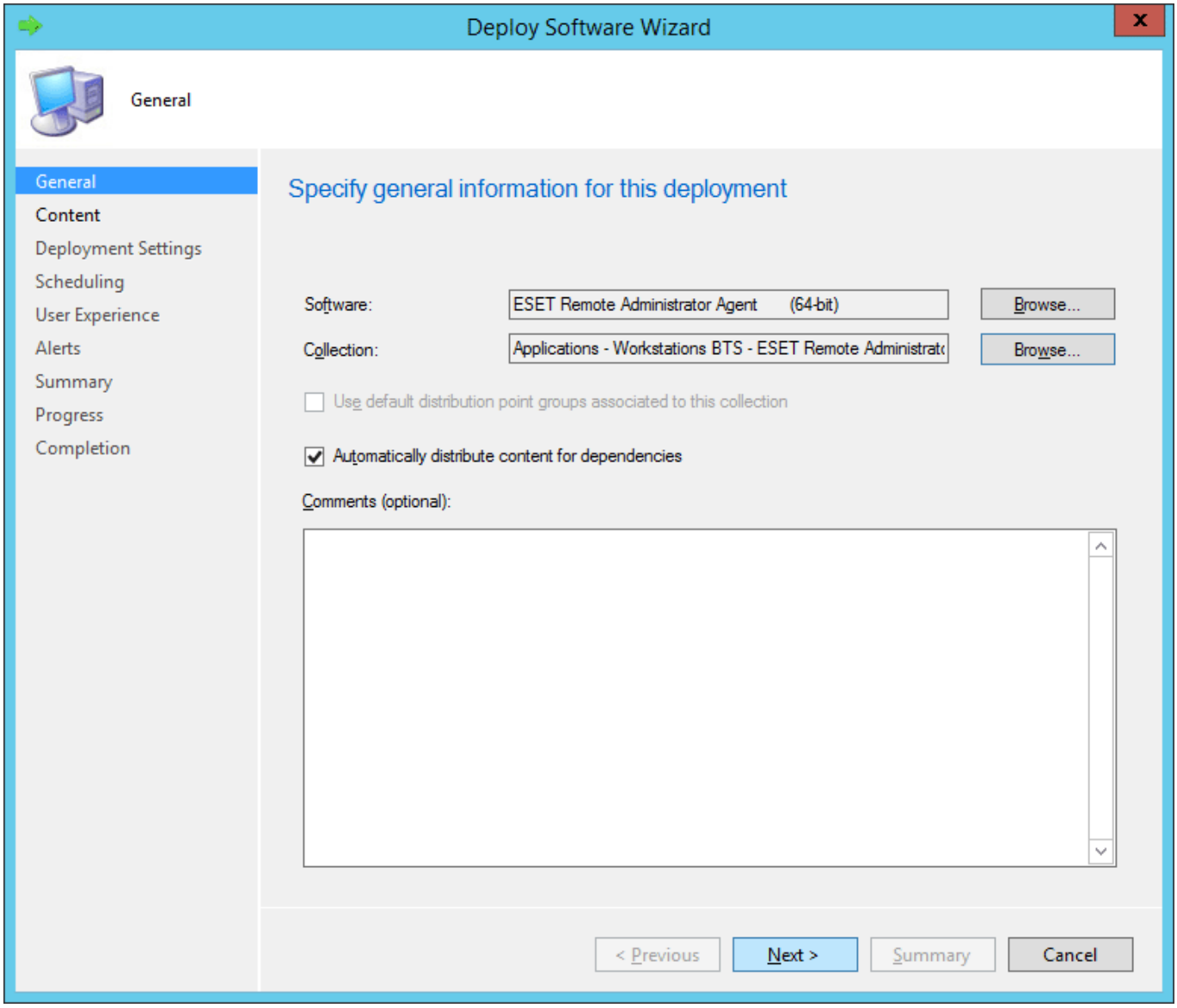


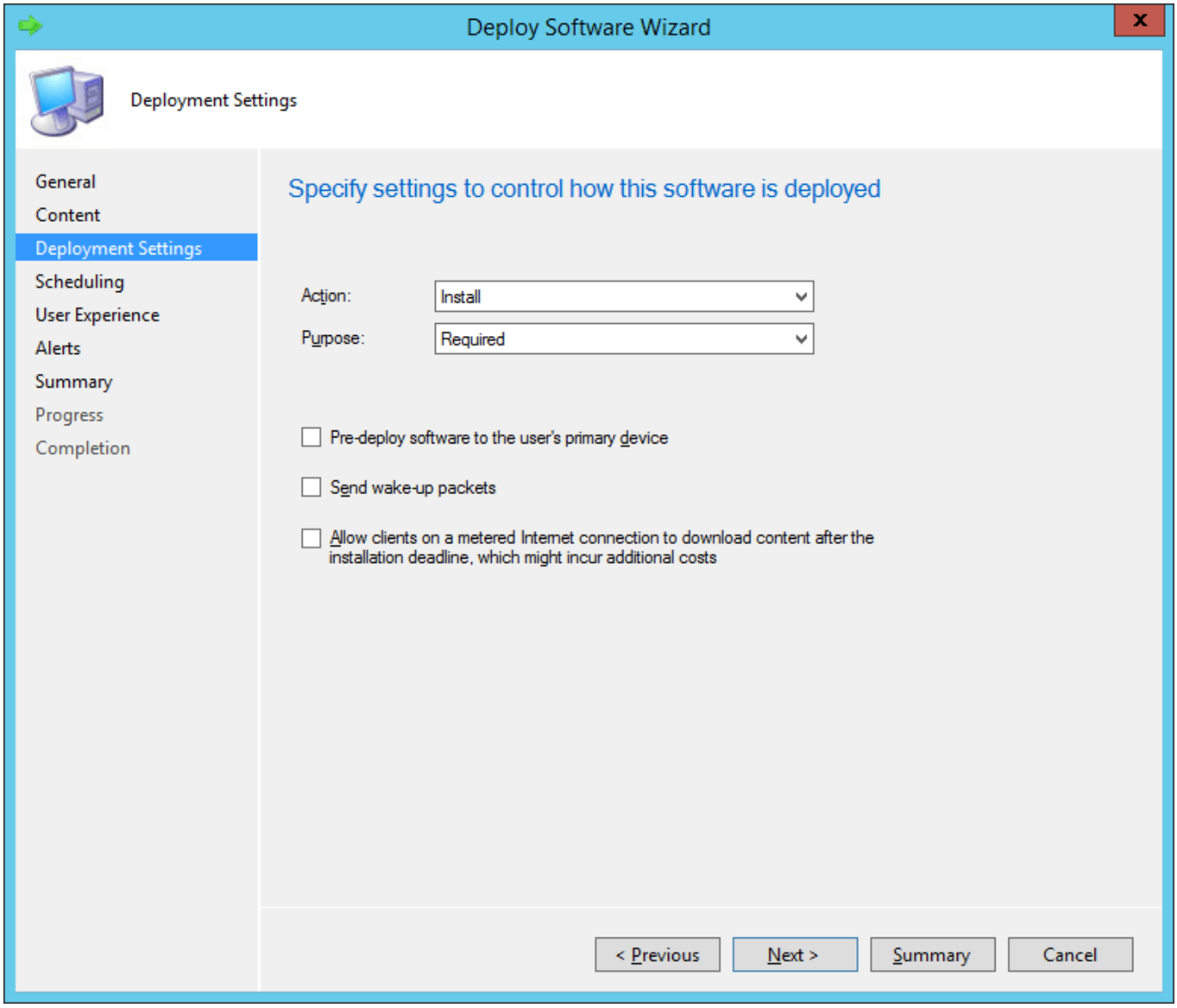
7. Haga clic con el botón secundario en la aplicación y seleccione **Implementar**. Siga las instrucciones del asistente y seleccione la colección y el destino donde desea implementar el agente.

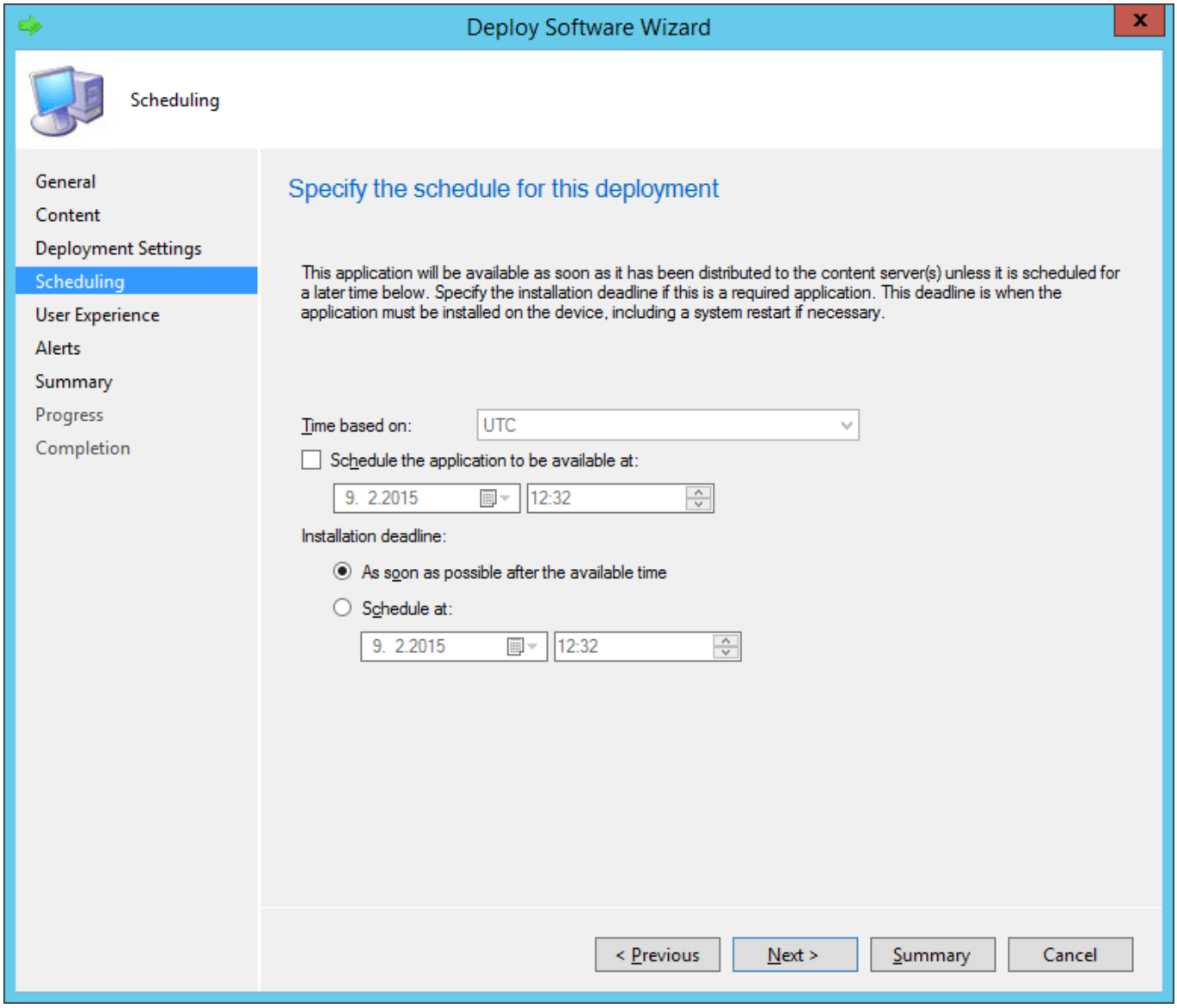

Add Distribution Points
Select distribution points that will host this content.
Software Update Packages are never distributed to Cloud Distribution Points.
Available distribution points:
Filter...
Name
Type
Description
On-premises
On-premises
OK
Cancel

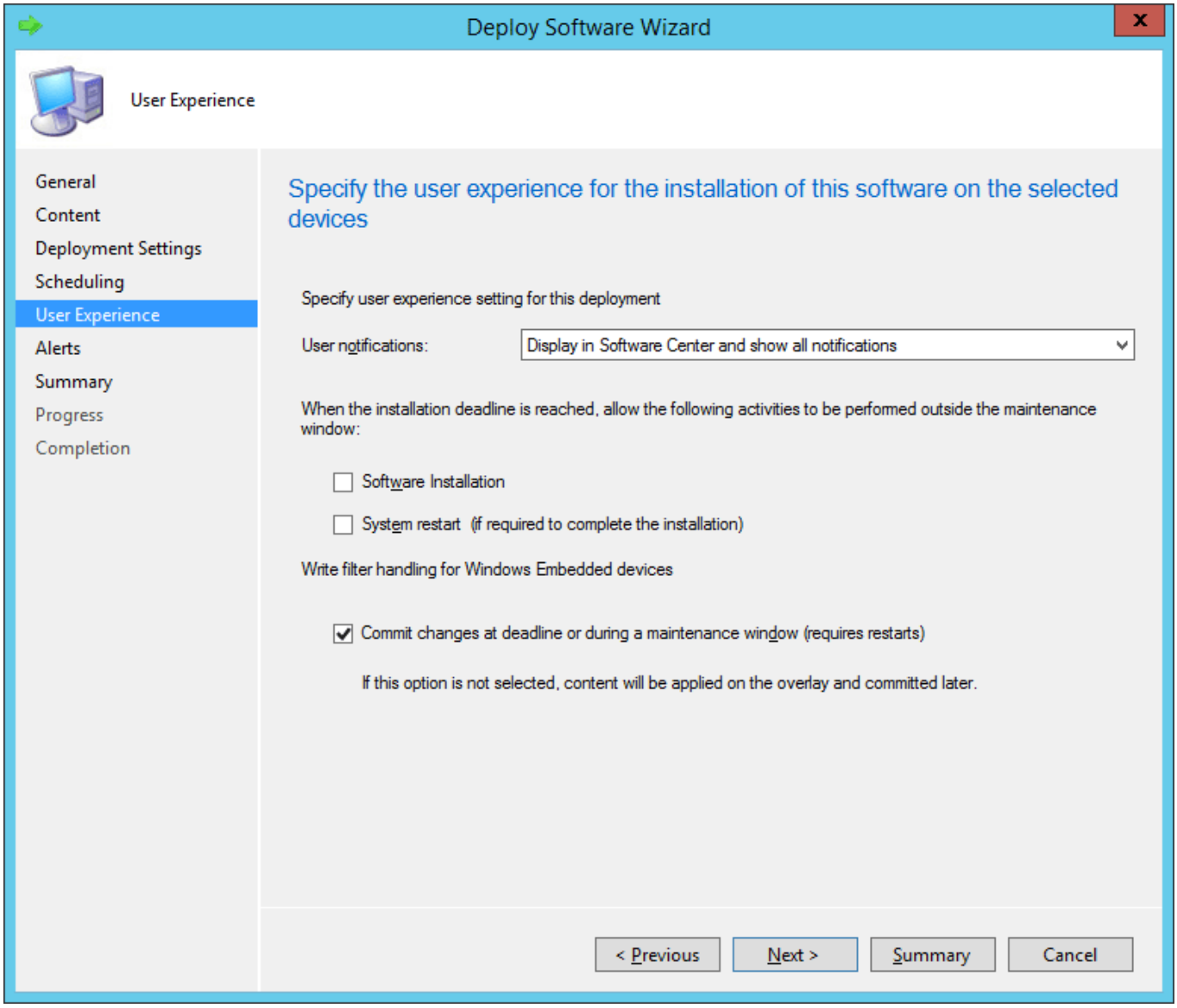

Distribute Content Wizard
Content Destination
General
Content
Content Destination
Summary
Progress
Completion
Specify the content destination
Content will be distributed to the following distribution points, distribution point groups, and the distribution point groups that are currently associated with collections.
Content destination:
Filter...
Add
Remove
Name
Description
Associations
Distribution point
< Previous
Next >
Summary
Cancel

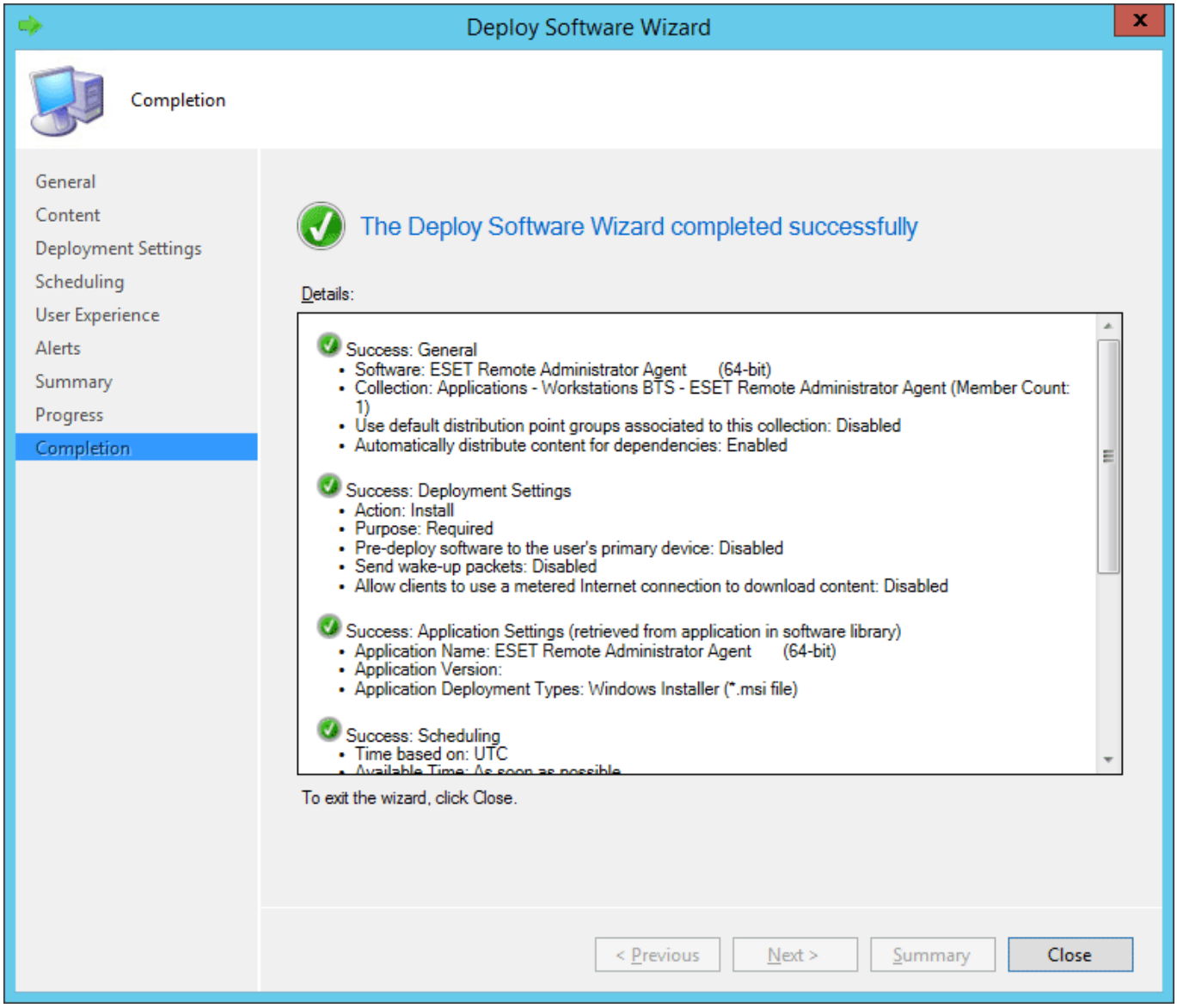

Distribute Content Wizard
Completion
General
Content
Content Destination
Summary
Progress
Completion
The Distribute Content Wizard completed successfully
Details:
Content (1):
• ESET Remote Administrator Agent (64-bit)
Dependencies (1):
• ESET Remote Administrator Agent (64-bit)
Collections (0):
Distribution point groups (0):
Distribution points (1):
To exit the wizard, click Close.
< Previous
Next >
Summary
Close


Deploy Software Wizard
General
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify general information for this deployment
Software:
ESET Remote Administrator Agent (64-bit)
Browse...
Collection:
Applications - Workstations BTS - ESET Remote Administrat
Browse...
Use default distribution point groups associated to this collection
Automatically distribute content for dependencies
Comments (optional):
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Deployment Settings
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify settings to control how this software is deployed
Action:
Install
Purpose:
Required
Pre-deploy software to the user's primary device
Send wake-up packets
Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Scheduling
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify the schedule for this deployment
This application will be available as soon as it has been distributed to the content server(s) unless it is scheduled for a later time below. Specify the installation deadline if this is a required application. This deadline is when the application must be installed on the device, including a system restart if necessary.
Time based on:
UTC
Schedule the application to be available at:
9. 2.2015
12:32
Installation deadline:
As soon as possible after the available time
Schedule at:
9. 2.2015
12:32
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
User Experience
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify the user experience for the installation of this software on the selected devices
Specify user experience setting for this deployment
User notifications:
Display in Software Center and show all notifications
When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:
Software Installation
System restart (if required to complete the installation)
Write filter handling for Windows Embedded devices
Commit changes at deadline or during a maintenance window (requires restarts)
If this option is not selected, content will be applied on the overlay and committed later.
< Previous
Next >
Summary
Cancel



ESET Remote Deployment Tool

La ESET Remote Deployment Tool es una manera conveniente de distribuir el paquete del instalador creado por ESET PROTECT On-Prem 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 On-Prem. La herramienta de instalación está pensada principalmente para la instalación en redes pequeñas o medianas, y se ejecuta conforme a los privilegios de administración.

> La Remote Deployment Tool de ESET está dedicada a implementar el agente ESET Management solo en equipos cliente con sistemas operativos Microsoft Windows compatibles.

Para implementar el agente de ESET Management y el producto de seguridad de ESET con este método, siga los pasos que se mencionan a continuación:

1. Descargue ESET Remote Deployment Tool desde el sitio Web de ESET.

2. Asegúrese de que se cumplen todos los requisitos previos.

3. Ejecutar ESET Remote Deployment Tool en el equipo del cliente.

4. Seleccione una de las siguientes opciones de instalación:

   • Active Directory: necesitará proporcionar credenciales de Active Directory. Esta opción incluye una estructura de exportación de Active Directory para la importación subsecuente a ESET PROTECT On-Prem.

   • Red de escaneo: deberá proporcionar rangos de IP para escanear equipos en la red.

   • Importar lista: necesitará proporcionar una lista de nombres de host o direcciones IP.

   • Agregar equipos manualmente: necesitará proporcionar una lista de nombres de host o direcciones IP manualmente.

> La implementación puede fallar por varios motivos. En caso de problemas con la implementación, lea el capítulo sobre Resolución de problemas o los escenarios de ejemplo verificados de la implementación del agente ESET Management.

Requisitos previos de la herramienta de implementación remota de ESET

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

• Debe instalar el servidor de ESET PROTECT y la consola web de ESET PROTECT (en un equipo del servidor).

• Se deben abrir los puertos adecuados. Consulte los puertos usados para la implementación remota del Agente ESET Management en un equipo de destino con sistema operativo Windows.

• Los nombres de paquetes de instalación deben incluir la cadena "x86" o "x64". De lo contrario, no funcionará la implementación.

• Se debe crear y descargar un paquete instalador todo en uno en su unidad local.

• Es necesario contar con permisos para crear un instalador todo en uno.

> La implementación puede fallar por varios motivos. En caso de problemas con la implementación, lea el capítulo sobre Resolución de problemas o los escenarios de ejemplo verificados de la implementación del agente ESET Management.

Seleccionar equipos del Active Directory

Para continuar con la instalación del Agente ESET Management del producto de seguridad de ESET del capítulo anterior:

1. Lea y acepte el **Contrato de licencia de usuario final** y haga clic en **Siguiente**.

2. Ingrese al **Servidor de Active Directory** con la dirección IP o el nombre de host y el **Puerto** al que desea conectarse.

3. Ingrese el **Nombre de usuario** y la **Contraseña** para iniciar sesión en el Servidor de Active Directory. Si selecciona la casilla de verificación junto a **Usar las credenciales de usuario actuales**, y se completarán automáticamente las credenciales.

4. De manera opcional, seleccione la casilla de verificación junto a **Exportar lista de equipos para ESET PROTECT** si desea exportar la estructura del Active Directory para luego importarla en ESET PROTECT On-Prem.

Si un equipo forma parte del Active Directory, haga clic en **Siguiente** y se realizará el inicio de sesión predeterminado del Controlador de dominio.

5. Seleccione la casilla de verificación junto a los equipos que desea agregar y haga clic en **Siguiente**. Seleccione la casilla de verificación **Incluir subgrupos** para enumerar todos los equipos dentro de un grupo seleccionado.

6. Se mostrarán equipos seleccionados para implementación remota. Asegúrese de que se hayan agregado todos los equipos y luego haga clic en **Siguiente**.

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

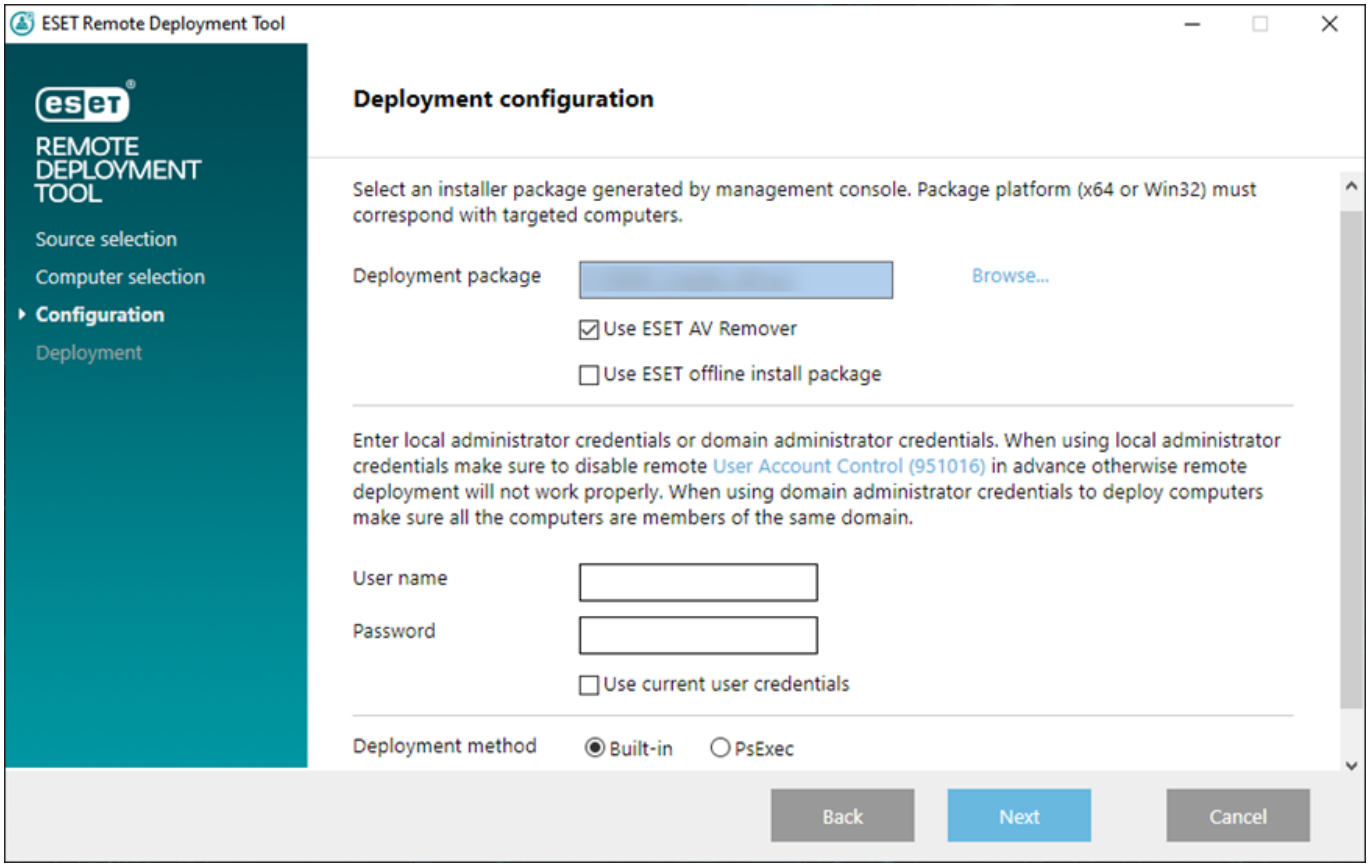
7. Haga clic en **Examinar** y seleccione el paquete de instalación de paquetes que creó en la consola web de ESET PROTECT (on-prem o nube).

- También puede seleccionar **Usar el paquete de instalación sin conexión de ESET** (archivo *.dat*) creado desde Live Installer (solo ESET PROTECT en la nube).

- Si no tiene ninguna aplicación de seguridad adicional instalada en su equipo local, quite la selección de la casilla de verificación junto a **Usar ESET AV Remover**. ESET AV Remover puede quitar ciertas aplicaciones.

8. Ingrese las credenciales de inicio de sesión para los equipos objetivos. Si los equipos son miembros de un dominio, ingrese las **credenciales de administrador de dominio**. Si inicia sesión con **credenciales de administrador de dominio**, es necesario desactivar UAC remoto en los equipos objetivos. De manera opcional, puede seleccionar la casilla de verificación junto a **Usar credenciales de usuario actuales**.

9. Se utiliza el **método de instalación** para ejecutar programas en máquinas remotas. El método **Incorporado** es una configuración predeterminada que admite mensajes de error de Windows. **PsExec** es una herramienta de terceros y una alternativa al método Incorporado. Seleccione una de estas opciones y haga clic en **Siguiente**.



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

10. Cuando se inicia la instalación, se mostrará "Éxito". Haga clic en **Finalizar** para completar la implementación. Si la implementación falla, haga clic en **Más información** en la columna **Estado** para ver más detalles. Puede exportar una lista de equipos fallidos. Haga clic en **Buscar** junto al campo **Exportar equipos fallidos**, seleccione un archivo *.txt* en el que quiere guardar la lista y haga clic en **Exportar equipos fallidos**.

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

La implementación puede fallar por varios motivos. En caso de problemas con la implementación, lea el capítulo sobre Resolución de problemas o los escenarios de ejemplo verificados de la implementación del agente ESET Management.

Explorar la red local en busca de equipos

Para continuar con la instalación del Agente ESET Management del producto de seguridad de ESET del capítulo anterior:

1. Lea y acepte el **Contrato de licencia de usuario final** y haga clic en **Siguiente**.

2. Ingrese el **rango de IP** de la red en el formato *10.100.100.10-10.100.100.250*

3. Seleccione uno de las siguientes **Métodos de escaneo**:

- **Escaneo de ping** - Busca los equipos cliente con comando `ping`.

> Algunos equipos cliente en esta red no necesitan enviar una respuesta al comando `ping` ya que el firewall bloquea la conexón.

- **Escaneo de puerto** - Usa el número de puerto para explorar la red. Consulte los puertos compatibles usados para la implementación remota de Agentes ESET Management. El número de puerto predeterminado es 445.

4. Para encontrar equipos en la red, haga clic en **Iniciar escaneo**.

5. Seleccione la casilla de verificación junto a los equipos que desea agregar y haga clic en **Siguiente**.

6. Se mostrarán equipos seleccionados para implementación remota. Asegúrese de que se hayan agregado todos los equipos y luego haga clic en **Siguiente**.

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

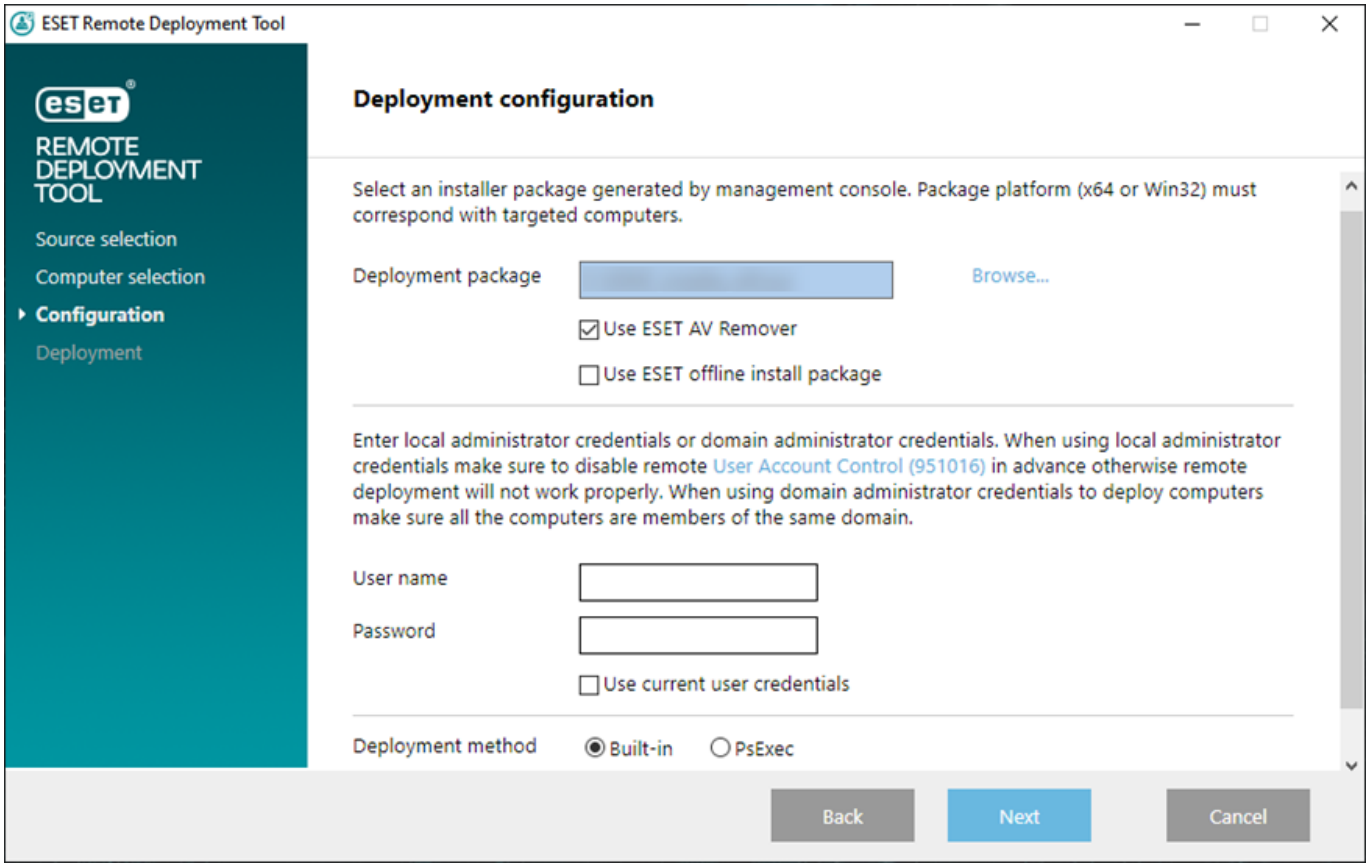
7. Haga clic en **Examinar** y seleccione el paquete de instalación de paquetes que creó en la consola web de ESET PROTECT (on-prem o nube).

- También puede seleccionar **Usar el paquete de instalación sin conexión de ESET** (archivo *.dat*) creado desde Live Installer (solo ESET PROTECT en la nube).

- Si no tiene ninguna aplicación de seguridad adicional instalada en su equipo local, quite la selección de la casilla de verificación junto a **Usar ESET AV Remover**. ESET AV Remover puede quitar ciertas aplicaciones.

8. Ingrese las credenciales de inicio de sesión para los equipos objetivos. Si los equipos son miembros de un dominio, ingrese las **credenciales de administrador de dominio**. Si inicia sesión con **credenciales de administrador de dominio**, es necesario desactivar UAC remoto en los equipos objetivos. De manera opcional, puede seleccionar la casilla de verificación junto a **Usar credenciales de usuario actuales**.

9. Se utiliza el **método de instalación** para ejecutar programas en máquinas remotas. El método **Incorporado** es una configuración predeterminada que admite mensajes de error de Windows. **PsExec** es una herramienta de terceros y una alternativa al método Incorporado. Seleccione una de estas opciones y haga clic en **Siguiente**.



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

10. Cuando se inicia la instalación, se mostrará "Éxito". Haga clic en **Finalizar** para completar la implementación. Si la implementación falla, haga clic en **Más información** en la columna **Estado** para ver más detalles. Puede exportar una lista de equipos fallidos. Haga clic en **Buscar** junto al campo **Exportar equipos fallidos**, seleccione un archivo *.txt* en el que quiere guardar la lista y haga clic en **Exportar equipos fallidos**.

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

La implementación puede fallar por varios motivos. En caso de problemas con la implementación, lea el capítulo sobre Resolución de problemas o los escenarios de ejemplo verificados de la implementación del agente ESET Management.

Importar un listado de equipos

Para continuar con la instalación del Agente ESET Management del producto de seguridad de ESET del capítulo anterior:

1. Lea y acepte el **Contrato de licencia de usuario final** y haga clic en **Siguiente**.

2. Seleccione una de las siguientes opciones:

   • **Archivo de texto (un equipo por línea)**: Un archivo con nombres de host o direcciones IP. Cada dirección IP o nombre de host debe estar en una línea nueva.

   • **Exportar desde la consola de administración**: Un archivo con nombres de host o direcciones IP exportado desde la Consola web ESET PROTECT.

3. Haga clic en **Examinar** y seleccione el archivo que le gustaría cargar y, luego, haga clic en **Siguiente**.

4. Se mostrarán equipos seleccionados para implementación remota. Asegúrese de que se hayan agregado todos los equipos y luego haga clic en **Siguiente**.

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

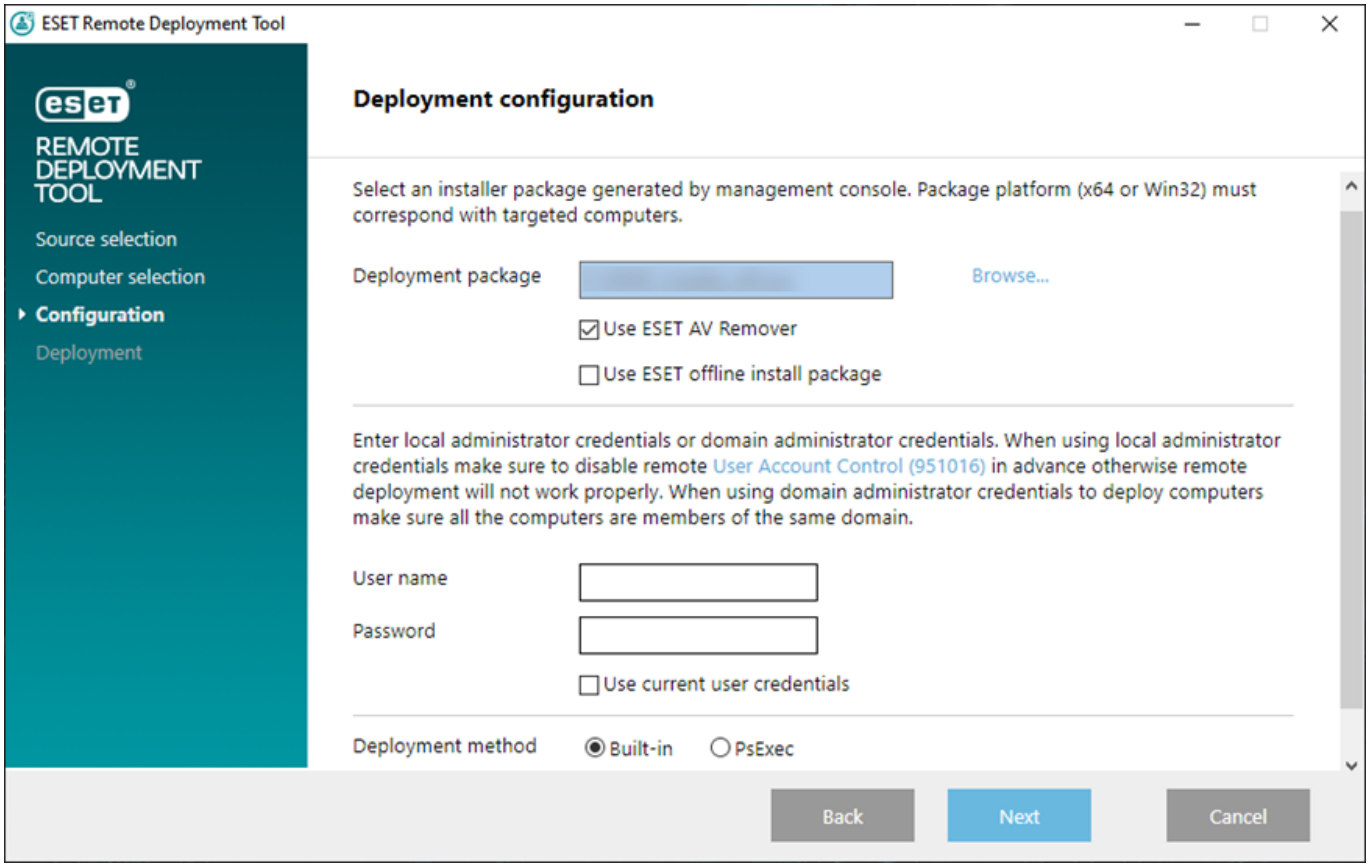
5. Haga clic en **Examinar** y seleccione el paquete de instalación de paquetes que creó en la consola web de ESET PROTECT (on-prem o nube).

   • También puede seleccionar **Usar el paquete de instalación sin conexión de ESET** (archivo *.dat*) creado desde Live Installer (solo ESET PROTECT en la nube).

   • Si no tiene ninguna aplicación de seguridad adicional instalada en su equipo local, quite la selección de la casilla de verificación junto a **Usar ESET AV Remover**. ESET AV Remover puede quitar ciertas aplicaciones.

6. Ingrese las credenciales de inicio de sesión para los equipos objetivos. Si los equipos son miembros de un dominio, ingrese las **credenciales de administrador de dominio**. Si inicia sesión con **credenciales de administrador de dominio**, es necesario desactivar UAC remoto en los equipos objetivos. De manera opcional, puede seleccionar la casilla de verificación junto a **Usar credenciales de usuario actuales**.

7. Se utiliza el **método de instalación** para ejecutar programas en máquinas remotas. El método **Incorporado** es una configuración predeterminada que admite mensajes de error de Windows. **PsExec** es una herramienta de terceros y una alternativa al método Incorporado. Seleccione una de estas opciones y haga clic en **Siguiente**.



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

8. Cuando se inicia la instalación, se mostrará "Éxito". Haga clic en **Finalizar** para completar la implementación. Si la implementación falla, haga clic en **Más información** en la columna **Estado** para ver más detalles. Puede exportar una lista de equipos fallidos. Haga clic en **Buscar** junto al campo **Exportar equipos fallidos**, seleccione un archivo *.txt* en el que quiere guardar la lista y haga clic en **Exportar equipos fallidos**.

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

La implementación puede fallar por varios motivos. En caso de problemas con la implementación, lea el capítulo sobre Resolución de problemas o los escenarios de ejemplo verificados de la implementación del agente ESET Management.

Agregar equipos manualmente

Para continuar con la instalación del Agente ESET Management del producto de seguridad de ESET del capítulo anterior:

1. Lea y acepte el **Contrato de licencia de usuario final** y haga clic en **Siguiente**.

2. Ingresar los nombres de host o direcciones IP manualmente y luego hacer clic en **Siguiente**. Cada dirección IP o nombre de host debe estar en una línea nueva.

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

3. Se mostrarán equipos seleccionados para implementación remota. Asegúrese de que se hayan agregado todos los equipos y luego haga clic en **Siguiente**.

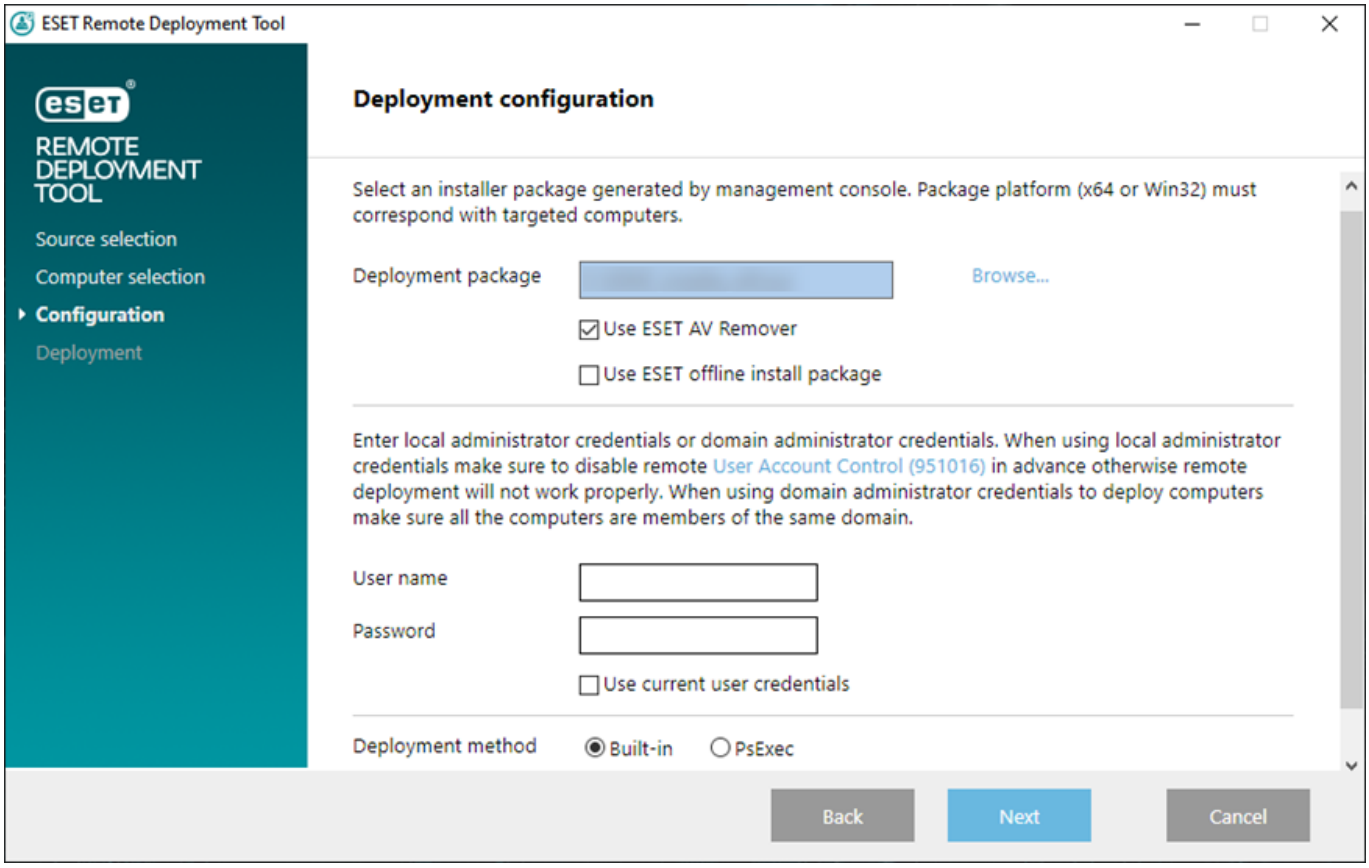
4. Haga clic en **Examinar** y seleccione el paquete de instalación de paquetes que creó en la consola web de ESET PROTECT (on-prem o nube).

- También puede seleccionar **Usar el paquete de instalación sin conexión de ESET** (archivo *.dat*) creado desde Live Installer (solo ESET PROTECT en la nube).

- Si no tiene ninguna aplicación de seguridad adicional instalada en su equipo local, quite la selección de la casilla de verificación junto a **Usar ESET AV Remover**. ESET AV Remover puede quitar ciertas aplicaciones.

5. Ingrese las credenciales de inicio de sesión para los equipos objetivos. Si los equipos son miembros de un dominio, ingrese las **credenciales de administrador de dominio**. Si inicia sesión con **credenciales de administrador de dominio**, es necesario desactivar UAC remoto en los equipos objetivos. De manera opcional, puede seleccionar la casilla de verificación junto a **Usar credenciales de usuario actuales**.

6. Se utiliza el **método de instalación** para ejecutar programas en máquinas remotas. El método **Incorporado** es una configuración predeterminada que admite mensajes de error de Windows. **PsExec** es una herramienta de terceros y una alternativa al método Incorporado. Seleccione una de estas opciones y haga clic en **Siguiente**.



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

7. Cuando se inicia la instalación, se mostrará "Éxito". Haga clic en **Finalizar** para completar la implementación. Si la implementación falla, haga clic en **Más información** en la columna **Estado** para ver más detalles. Puede exportar una lista de equipos fallidos. Haga clic en **Buscar** junto al campo **Exportar equipos fallidos**, seleccione un archivo *.txt* en el que quiere guardar la lista y haga clic en **Exportar equipos fallidos**.

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

La implementación puede fallar por varios motivos. En caso de problemas con la implementación, lea el capítulo sobre Resolución de problemas o los escenarios de ejemplo verificados de la implementación del agente ESET Management.

ESET Remote Deployment Tool: resolución de problemas

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

> La Remote Deployment Tool de ESET está dedicada a implementar el agente ESET Management solo en equipos cliente con sistemas operativos Microsoft Windows compatibles.

La implementación puede fallar con algunos mensajes de error y por varios motivos, que se enumeran en la tabla a continuación.

Mensaje de error	Posibles causas
No se encontró la ruta de red (código de error 0x35)	• No se puede localizar el cliente en la red, el firewall bloquea la comunicación • Los puertos de ingreso 135, 137, 138, 139 y 445 no están abiertos en el firewall del cliente o en Windows Firewall: No se usa la excepción de uso compartido de archivo entrante e impresora • No se pudo resolver el nombre de host del cliente, utilice nombres de equipos FQDN válidos
Acceso denegado (código de error 0x5) **El nombre de usuario o la contraseña son incorrectos** (código de error 0x52e)	• Cuando realice una implementación desde un servidor unido al dominio a un cliente unido al dominio, use credenciales de un usuario que sea miembro del grupo Administrador de dominio en formato **Dominio\Admin de dominio** • Cuando realice la implementación desde un servidor a un cliente que no se encuentra en el mismo dominio, deshabilite el filtrado remoto UAC en el equipo de destino. • Cuando realice una implementación desde un servidor a un cliente que no se encuentra en el mismo dominio, use credenciales de un usuario local que sea miembro del grupo Administradores en formato Admin. El nombre del equipo de destino se anexará automáticamente al inicio de sesión. • No se configuró la contraseña para la cuenta del administrador • Permisos de usuarios insuficientes • El recurso compartido administrativo ADMIN$ no está disponible • El recurso compartido administrativo IPC$ no está disponible • La opción Uso compartido simple de archivos está habilitada
El paquete de instalación no es compatible con este tipo de procesador (código de error 1633)	El paquete de instalación no es compatible con esta plataforma. Cree y descargue el paquete de instalación con la plataforma correcta (sistema operativo de 64-bit o 32-bit) en la Consola web ESET PROTECT.
El período de tiempo de espera del semáforo ha expirado	El cliente no puede acceder al recurso compartido de red con el paquete de implementación dado que SMB 1.0 está deshabilitado en el recurso compartido.

Siga los pasos adecuados para la resolución de problemas de acuerdo con la causa posible:

Posibles causas	Pasos para la resolución de problemas
No se puede localizar el cliente en la red	Compruebe la disponibilidad del cliente en el Servidor ESET PROTECT. Si obtiene una respuesta, intente iniciar sesión en el equipo cliente en forma remota (por ejemplo, por medio de un escritorio remoto).
El firewall bloquea la comunicación	Controle la configuración del firewall en el servidor y en el cliente, así como también cualquier otro firewall que exista entre estos dos equipos (si corresponde). Luego de una implementación exitosa, los puertos 2222 y 2223 no están abiertos en el firewall. Asegúrese de que estos puertos estén abiertos en el firewall entre los dos equipos (cliente y servidor).
No se pudo resolver el nombre de host del cliente	Las soluciones posibles para los problemas de DNS pueden incluir, entre otras: • Uso del comando `nslookup` de la dirección IP y el nombre de host del servidor o los clientes que tienen problemas con la implementación del Agente. Los resultados deben coincidir con la información del equipo. Por ejemplo, un `nslookup` de un nombre de host debe resolver en la dirección IP que el comando `ipconfig` muestra en el host en cuestión. El comando `nslookup` tendrá que ejecutarse en los clientes y en el servidor. • Examinar en forma manual si los registros de DNS tienen duplicados.
No se configuró la contraseña para la cuenta del administrador	Configure una contraseña adecuada para la cuenta del administrador (no use una contraseña en blanco).
Permisos de usuarios insuficientes	Intente usar las credenciales del Administrador de dominios al crear la Tarea de implementación del agente. Si el equipo cliente se encuentra en un grupo de trabajo, use la cuenta del Administrador local en ese equipo en particular. La cuenta de usuario Administrador debe estar activada para ejecutar la tarea de implementación de agente. Puede crear un usuario local que sea miembro del grupo Administradores o habilitar una cuenta de Administrador local incorporada. Para activar la cuenta del usuario Administrador: 1.Abra un símbolo del sistema administrativo 2.Tipo el siguiente comando: `net user administrator /active:yes`
El recurso compartido de ADMIN$ no se encuentra disponible	El equipo cliente debe tener el recurso compartido ADMIN$ activado. Asegúrese de que está presente entre los recursos compartidos (**Inicio** > **Panel de control** > **Herramientas administrativas** > **Administración del equipo** > **Carpetas compartidas** > **Recursos compartidos**).
El recurso compartido de IPC$ no se encuentra disponible	Verifique que el cliente pueda acceder al IPC$, al emitir lo siguiente desde el símbolo del sistema en el servidor: `net use \\clientname\IPC$`donde `clientname` es el nombre del equipo de destino.
La opción Uso compartido simple de archivos está habilitada	Si obtiene el mensaje de error **Acceso denegado** y tiene un entorno mixto (contiene tanto un dominio como un grupo de trabajo), deshabilite **Usar intercambio de archivos simple** o **Usar asistente de intercambio** en todos los equipos que tengan problemas con la implementación del Agente. Por ejemplo, en Windows 11 realice lo siguiente: • Haga clic en **Inicio**, escriba `Explorador de archivos` en el cuadro de **búsqueda** y, a continuación, haga clic en **Opciones del Explorador de archivos**. Haga clic en la pestaña **Ver** y, en el cuadro **Configuración avanzada**, desplácese hacia abajo en la lista y quite la selección de la casilla de verificación que está junto a **Usar el asistente de intercambio**.

Protección del agente

El agente ESET Management está protegido por un mecanismo de autodefensa incorporado. Esta característica proporciona lo siguiente:

- Protección contra la modificación de las entradas del registro del agente ESET Management (HIPS)
- Los archivos que pertenecen al agente ESET Management no se pueden modificar, sustituir, eliminar ni alterar (HIPS)
- El proceso del agente ESET Management no se puede finalizar
- El servicio del agente ESET Management no se puede detener, pausar, deshabilitar, desinstalar ni comprometer

Parte de la protección se encuentra cubierta por la función HIPS incluida en su producto ESET.

Para garantizar la plena protección del agente ESET Management, se debe habilitar la característica HIPS en un equipo cliente.

Configuración protegida por contraseña

Además de la autodefensa, podrá proteger con contraseña el acceso al agente ESET Management (disponible solo para Windows). Para establecer una contraseña del agente ESET Management, es necesario crear una política adecuada para el agente ESET Management.

Si el agente ESET Management está protegido por contraseña, debe proporcionar la contraseña para desinstalar, reparar o actualizar (con cambios).

Configuración del agente ESET Management

Puede configurar parámetros específicos para ESET Management Agent con una política de ESET Management Agent.

Existen políticas predefinidas para el agente ESET Management. Por ejemplo **Conexión**: conecta cada (Intervalo de conexión del agente) o **Detección de aplicaciones**: detecta todas las aplicaciones instaladas (incluso las aplicaciones de ESET). Para más información sobre cómo hacer cumplir políticas basadas en la ubicación, lea el ejemplo.

Haga clic en **Directivas** y expanda el **Agente de directivas > ESET Management integrado** luego edite una política existente o cree una nueva.

Conexión

- **Servidores a los que conectarse**: haga clic en Editar lista de servidores para agregar los detalles de conexión (nombre del host/IP y número de puerto) del servidor ESET PROTECT. Se pueden especificar múltiples servidores ESET PROTECT. Esto puede ser útil si, por ejemplo, ha cambiado la dirección IP de su servidor ESET PROTECT o está realizando una migración.
- **Límite de datos**: especifica la cantidad máxima de bytes para enviar datos.
- **Intervalo de conexión**: puede optar por el intervalo regular y especificar el valor de tiempo del intervalo de conexión (o usar la expresión CRON).
- **Certificado**: Puede gestionar los certificados de Pares para el Agente ESET Management. Haga clic en

Cambiar certificado y seleccione el certificado del agente ESET Management que debe usar el agente ESET Management. Para obtener más información, consulte el capítulo Certificados de pares.

Actualizaciones

• **Intervalo de actualización**: intervalo en el que se recibirán las actualizaciones. Puede seleccionar un intervalo regular y configurar los valores (o puede usar una expresión CRON).

• **Actualizar servidor**: actualice el servidor a partir del cual el agente ESET Management recibe las actualizaciones del módulo.

• **Tipo de actualización**: seleccione el tipo de actualizaciones que desea recibir. Elija actualizaciones periódicas o previas a su lanzamiento. No se recomienda que seleccione las actualizaciones previas a su lanzamiento para los sistemas de producción ya que esto implica un riesgo.

• **Habilitar actualización automática**: esta opción se aplica al agente ESET Management 8.1 y versiones posteriores. De forma predeterminada, el agente ESET Management se actualiza automáticamente a la versión compatible más reciente. Puede desactivar esta opción para deshabilitar la actualización automática del agente ESET Management.

Configuración

La Configuración protegida por contraseña es una función de protección del agente ESET Management (solo Windows). Haga clic en **Configurar** junto a **Configuración protegida por contraseña** para habilitar la configuración protegida por contraseña del agente ESET Management.

• La configuración protegida por contraseña se mejoró en la versión 10.1. Establezca la contraseña del agente por separado para la versión 10.0 y anteriores, y la versión 10.1 y posteriores.
• Registre la contraseña en un lugar seguro. Si el agente ESET Management está protegido por contraseña, debe proporcionar la contraseña para desinstalar, reparar o actualizar (con cambios).

Configuración avanzada

• **Proxy HTTP**: Use un servidor proxy para facilitar el tráfico de Internet a clientes en su red y la replicación del Agente al Servidor de ESET PROTECT.

o**Tipo de configuración de proxy**

■**Proxy global**: Use un servidor proxy para replicación del Agente y para caché de servicios de ESET (por ejemplo, actualizaciones).

■**Proxy diferente por servicio**: Use un proxy para replicación del Agente y otro para caché de servicios de ESET (por ejemplo, actualizaciones).

o**Proxy global**: Esta opción solo está disponible si la selecciona en **Tipo de configuración de proxy**. Haga clic en **Editar** y establezca su configuración de proxy.

Las dos opciones a continuación solo están disponibles si selecciona **Proxy diferente por servicio**. También puede usar únicamente una de las configuraciones de proxy, por ejemplo, configurar solamente **Servicios de ESET** y dejar **Replicación** apagado. Marque o demarque la casilla **Utilizar conexión directa si el proxy HTTP no está disponible** para activar o desactivar esta opción alternativa.

- **Replicación (al Servidor de administración ESET):** establezca la configuración de conexión para un proxy que conecte el Agente al Servidor.

- **Servicios de ESET**: Establezca la configuración de conexión para un proxy que almacene servicios de ESET.

• **Llamada de reactivación**: el servidor ESET PROTECT puede ejecutar una replicación instantánea del agente ESET Management en un equipo cliente a través de EPNS. Esto resulta útil cuando no desea esperar el intervalo regular cuando el agente ESET Management se conecta al servidor ESET PROTECT. Por ejemplo, cuando desea que una Tarea se ejecute de inmediato en los clientes o si desea que se aplique una política rápidamente.

• **Compatibilidad**: para permitir la administración de productos ESET versión 5 o anterior por parte del ESET Management Agente, se debe especificar un puerto de escucha específico. Además, se debe configurar los productos de ESET para detectar este puerto y la dirección del Servidor de ESET PROTECT se debe configurar en **localhost**.

• **Sistema operativo**: use los conmutadores para informar determinada información o problemas en el equipo del cliente. Por ejemplo, active **Informar de aplicaciones que no están instaladas de ESET** para activar los informes de las aplicaciones de terceros instaladas.

• **Repositorio**: ubicación del repositorio donde se almacenan todos los archivos de instalación.

El repositorio predeterminado es **AUTOSELECT**.

• **Programa de mejora del producto**: Habilite o deshabilite la transmisión de informes de fallas y datos anónimos de telemetría a ESET.

• **Inicio de sesión**: 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). El archivo de registro más reciente de ESET Management Agent puede encontrarse en un equipo cliente aquí:

Asignar

Especifica los clientes que recibirán esta política. Haga clic en **Asignar** para visualizar todos los Grupos estáticos y dinámicos y a sus miembros. Seleccione el equipo donde quiere aplicar la política y haga clic en **Aceptar**.

Resumen

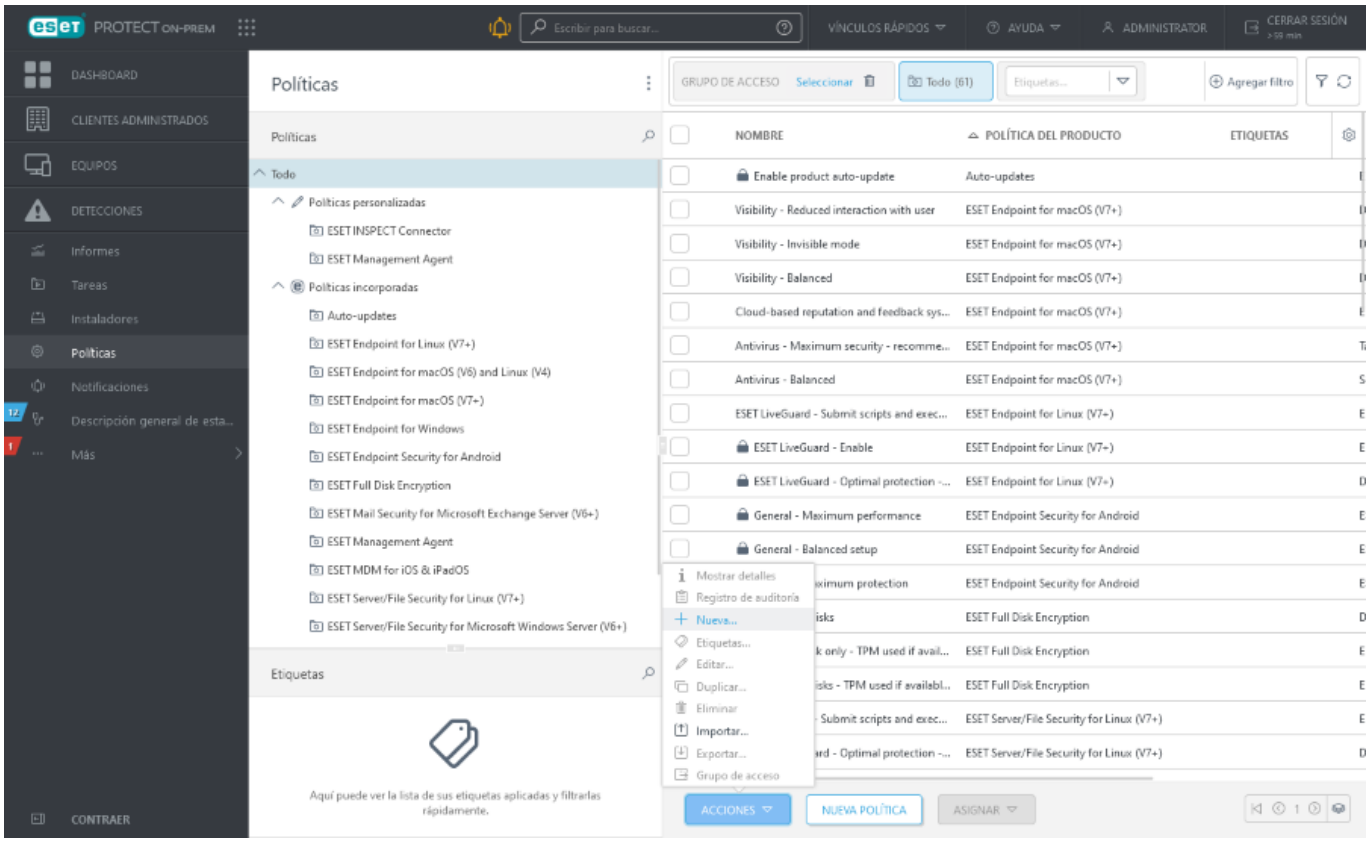
Revise la configuración de esta política y haga clic en **Finalizar**.

Puede solicitar la configuración del agente en un equipo administrado para ver la configuración de políticas del agente aplicada: Haga clic en **Equipos** > haga clic en un equipo > **Detalles** > **Configuración** > Solicitar configuración.

Crear de una política para el intervalo de conexión del agente ESET Management

En este ejemplo, vamos a crear una política nueva para el intervalo de conexión del agente ESET Management. Este valor debe ajustarse en base al tamaño de la infraestructura mediante políticas, luego de instalar ESET PROTECT On-Prem e implementar los Agentes ESET Management y productos de terminales ESET en los equipos cliente.

Cree un Nuevo grupo estático. Agregue una nueva política al hacer clic en **Políticas**. Haga clic en **Acciones** en la parte inferior y seleccione **Nuevo**.

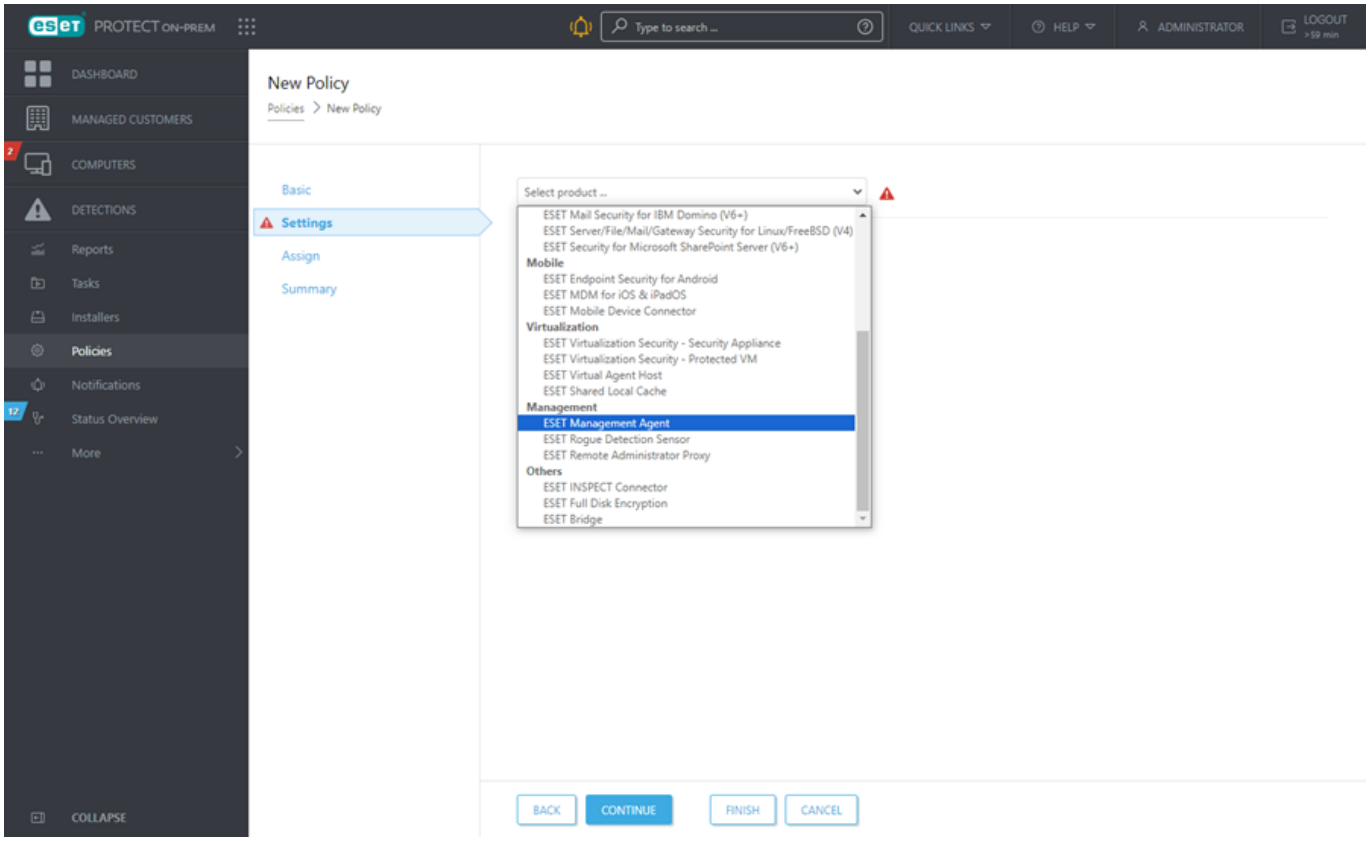


Básica

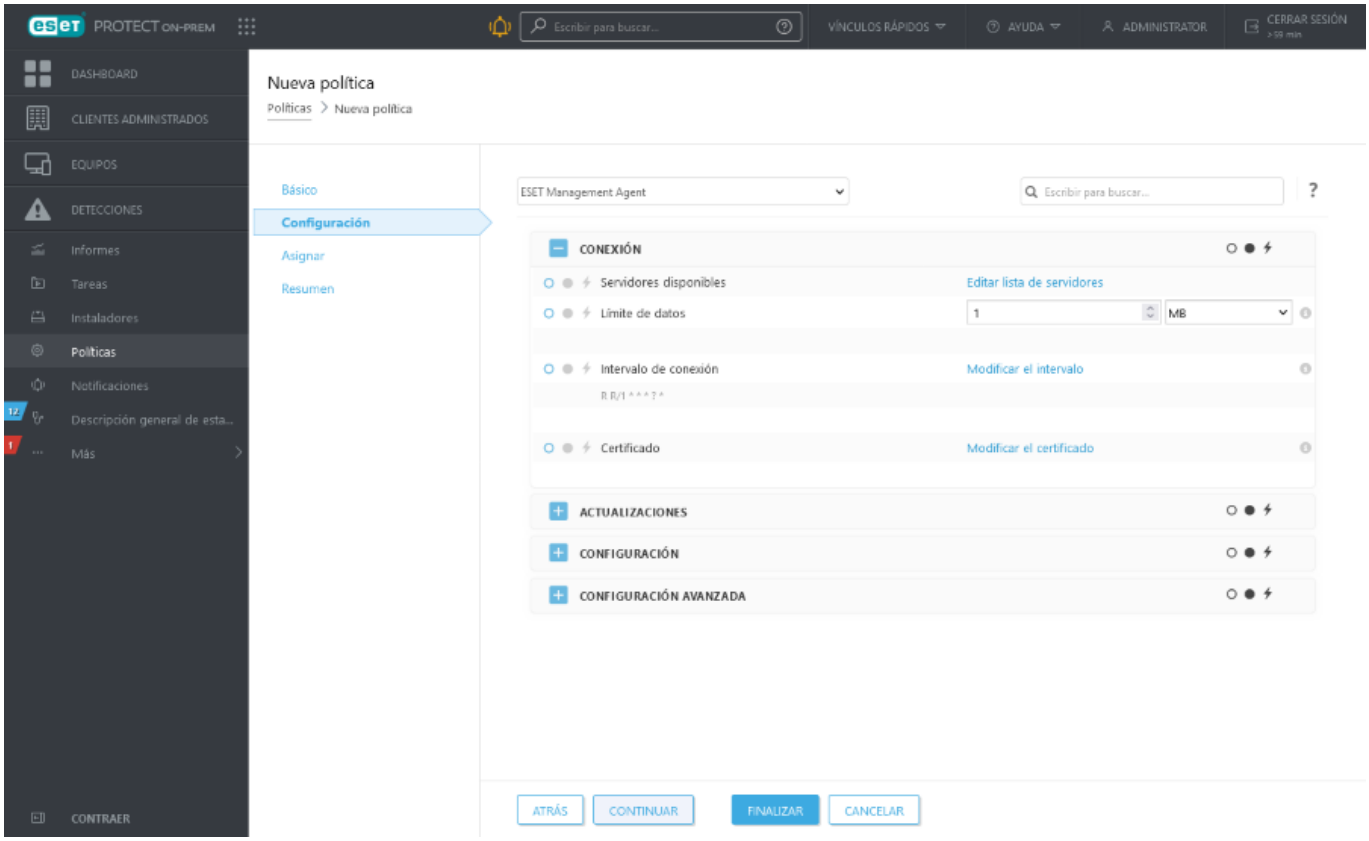
Ingrese un **Nombre** para la directiva nueva (por ejemplo, Intervalo de conexión del agente). El campo **Descripción** es opcional.

Configuración

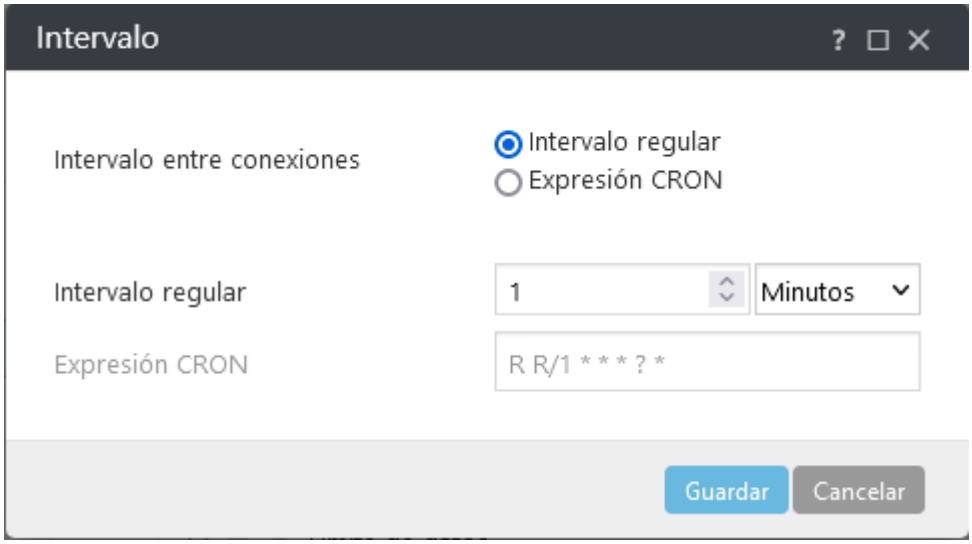
Seleccione el agente **ESET Management** en el menú desplegable **Producto**.



Haga clic en **Intervalo de conexión** > **Cambiar intervalo**.

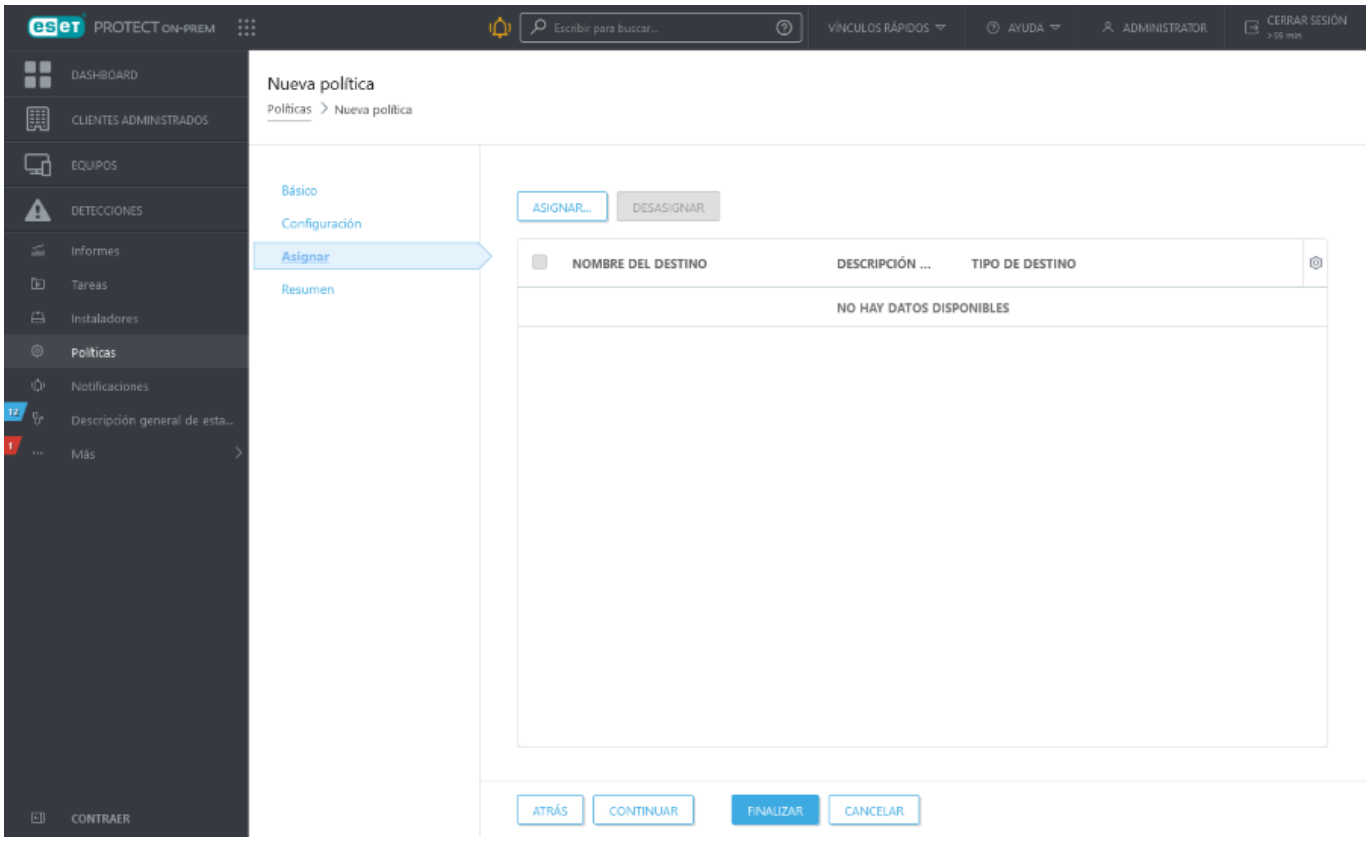


En el campo **Intervalo regular** , cambie el valor por su tiempo de intervalo preferido (60 segundos es el intervalo de replicación predeterminado del agente ESET Management) y haga clic en **Guardar**.



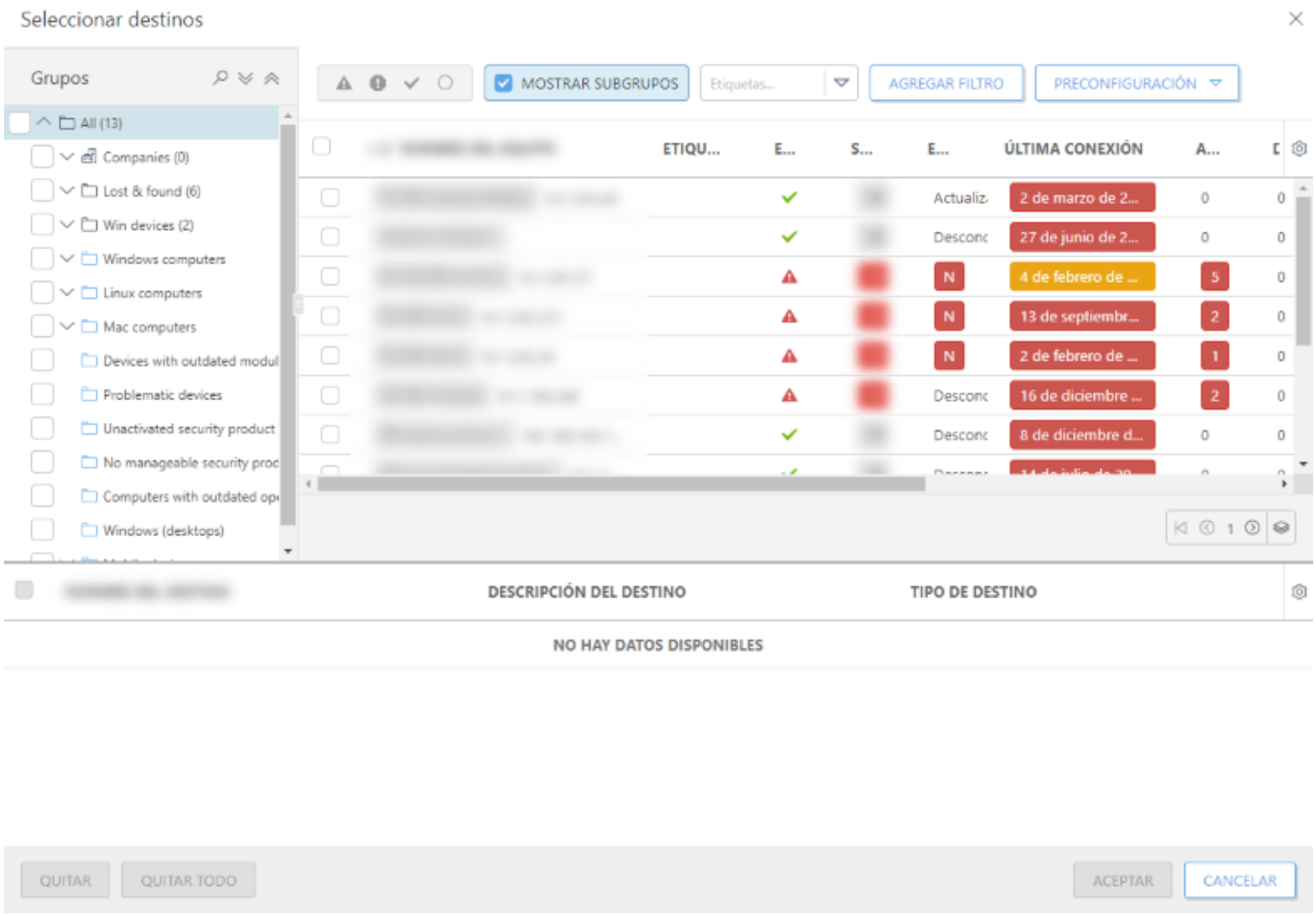
Asignar

Especifique los clientes (equipos/dispositivos móviles individuales o grupos completos) que serán los destinatarios de esta directiva.



Haga clic en **Asignar** para visualizar todos los Grupos estáticos y dinámicos y a sus miembros. Seleccione los equipos o grupos que desee y haga clic en **Aceptar**.

Para asignar todos los equipos de un grupo, asigne el grupo en lugar de los equipos individuales para evitar que la consola web se ralentice.
Si selecciona una gran cantidad de equipos, la consola web muestra una advertencia.



Resumen

Revise la configuración de esta política y haga clic en **Finalizar**. La política se aplica a los destinos después de su próxima conexión con el servidor de ESET PROTECT (en función del intervalo de conexión del agente).

Para aplicar la política inmediatamente, puede ejecutar la acción **Enviar llamada de activación** en los destinos de los **Equipos**.

Crear una política para que un agente ESET Management se conecte al nuevo servidor ESET PROTECT

Esta política le permite cambiar el comportamiento del agente ESET Management al modificar su configuración. Lo siguiente es particularmente útil al migrar equipos clientes a un nuevo servidor ESET PROTECT.

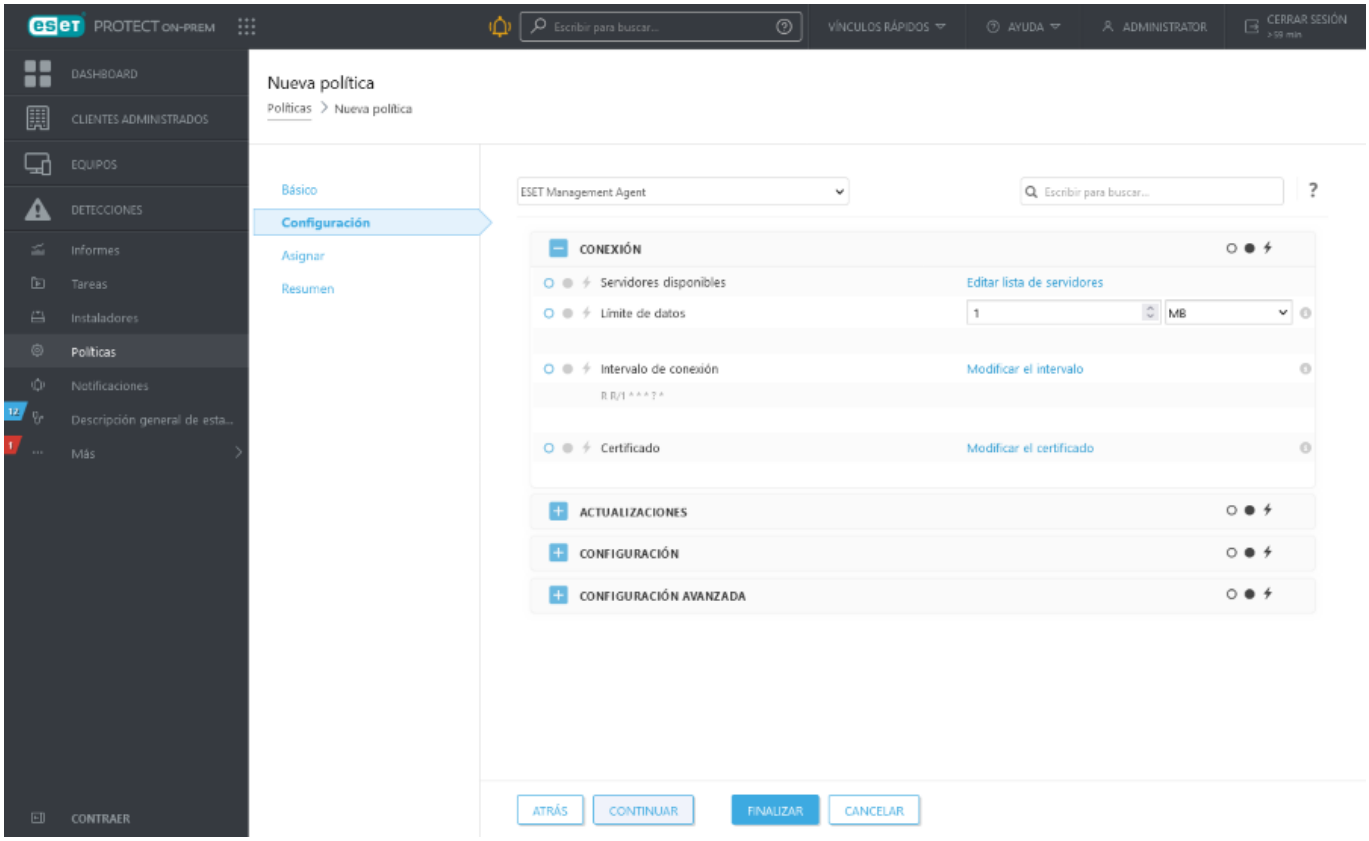
Cree una nueva política para establecer una nueva dirección IP del servidor ESET PROTECT y asigne la política a todos los equipos cliente. Seleccione **Políticas** > crear **Nueva**.

Básica

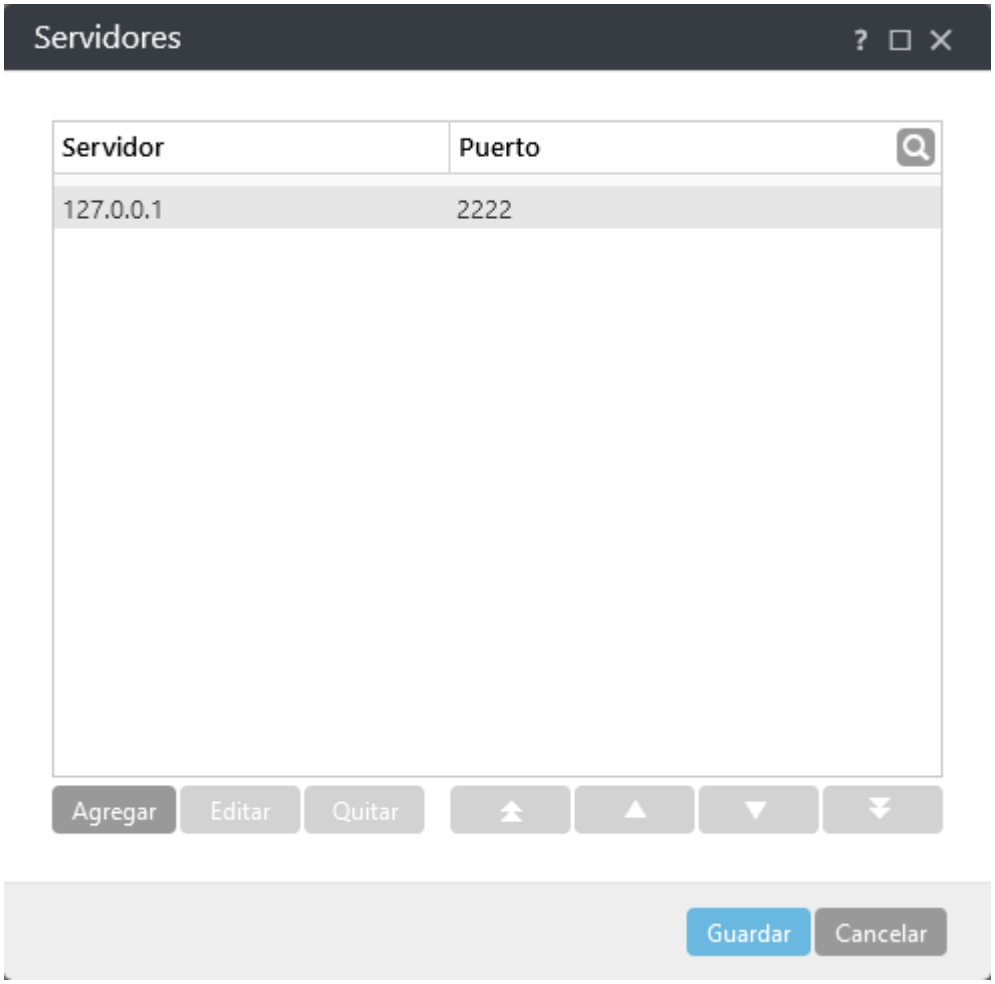
Ingrese un **Nombre** para su política. El campo **Descripción** es opcional.

Configuración

Seleccione **Agente ESET Management** desde el menú desplegable, expanda **Conexión** y haga clic en **Editar lista de servidores** junto a **Servidores a los que conectarse**.



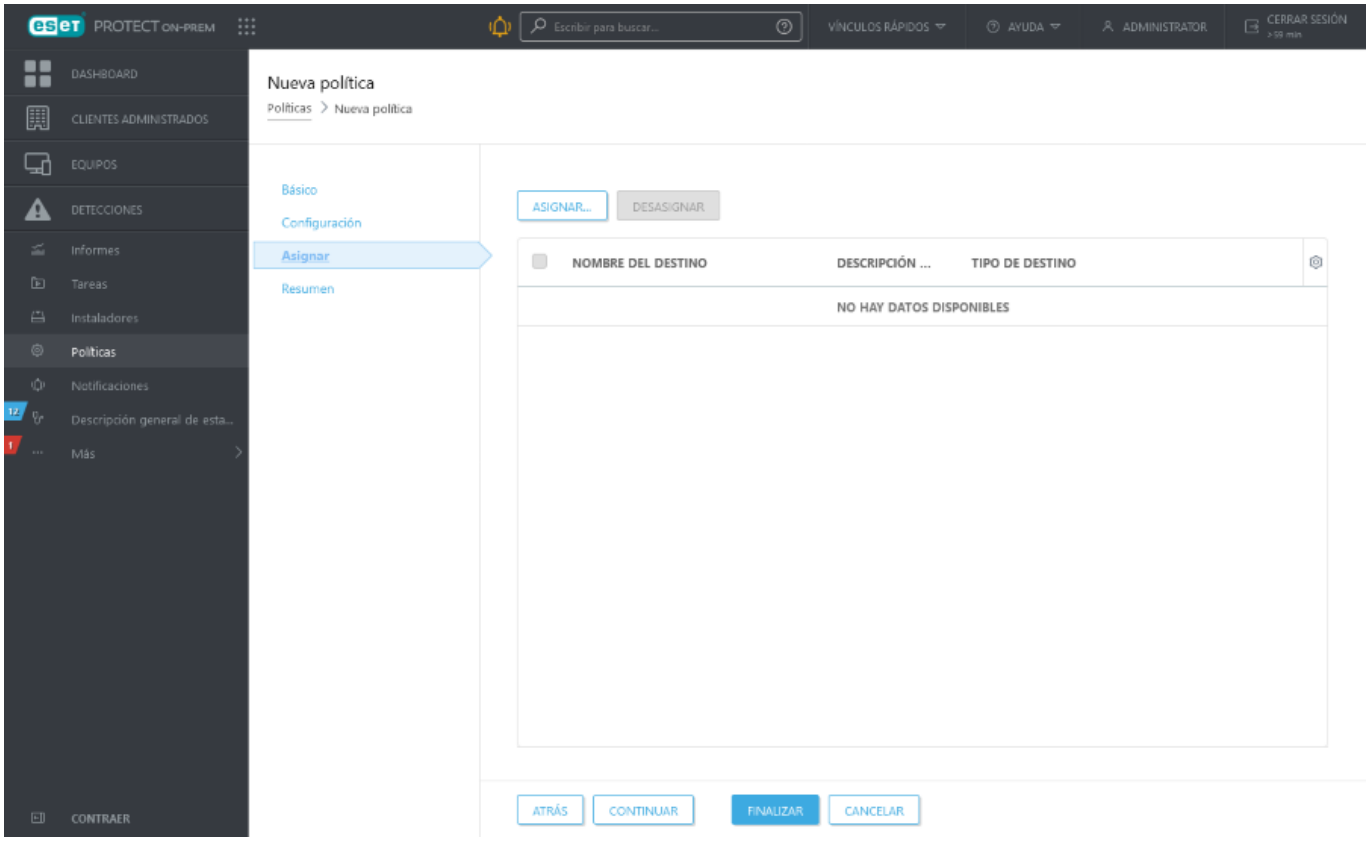
Se abrirá una ventana con una lista de las direcciones de ESET PROTECT Server a las que se puede conectar el agente ESET Management. Haga clic en **Agregar** e ingrese la dirección IP de su nuevo servidor ESET PROTECT en el campo **Host**. Si usa un puerto diferente al puerto 2222 del servidor ESET PROTECT predeterminado, especifique el número de puerto personalizado.



Use los botones de flechas para cambiar la prioridad de los servidores ESET PROTECT en caso que tenga múltiples entradas en la lista. Asegúrese de que su nuevo servidor ESET PROTECT se encuentre en la parte superior; para ello, haga clic en el botón **doble flecha arriba** y, luego, haga clic en **Guardar**.

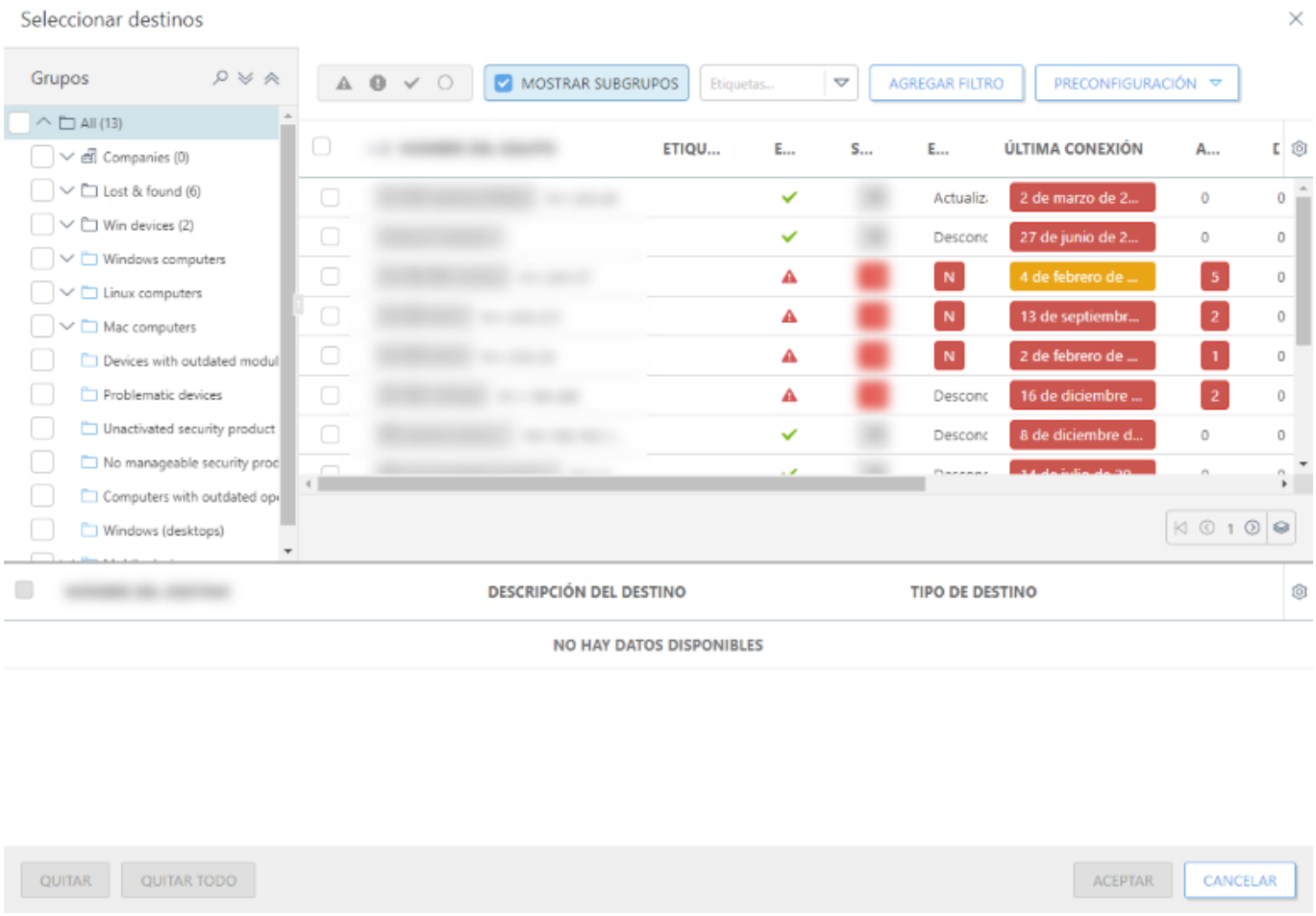
Asignar

Especifique los clientes (equipos/dispositivos móviles individuales o grupos completos) que serán los destinatarios de esta directiva.



Haga clic en **Asignar** para visualizar todos los Grupos estáticos y dinámicos y a sus miembros. Seleccione los equipos o grupos que desee y haga clic en **Aceptar**.

Para asignar todos los equipos de un grupo, asigne el grupo en lugar de los equipos individuales para evitar que la consola web se ralentice.
Si selecciona una gran cantidad de equipos, la consola web muestra una advertencia.



Resumen

Revise la configuración de esta política y haga clic en **Finalizar**. La política se aplica a los destinos después de su próxima conexión con el servidor de ESET PROTECT (en función del intervalo de conexión del agente).

> Para aplicar la política inmediatamente, puede ejecutar la acción **Enviar llamada de activación** en los destinos de los **Equipos**.

Crear una política para permitir la protección por contraseña del agente ESET Management

Siga los siguientes pasos para crear una nueva política que exija una contraseña para proteger al agente ESET Management. Cuando se usa **Configuración protegida por contraseña**, el agente ESET Management no podrá ser desinstalado ni reparado a menos que se proporcione una contraseña. Consulte Protección del agente para más detalles.

Básica

Ingrese un **Nombre** para esta política. El campo **Descripción** es opcional.

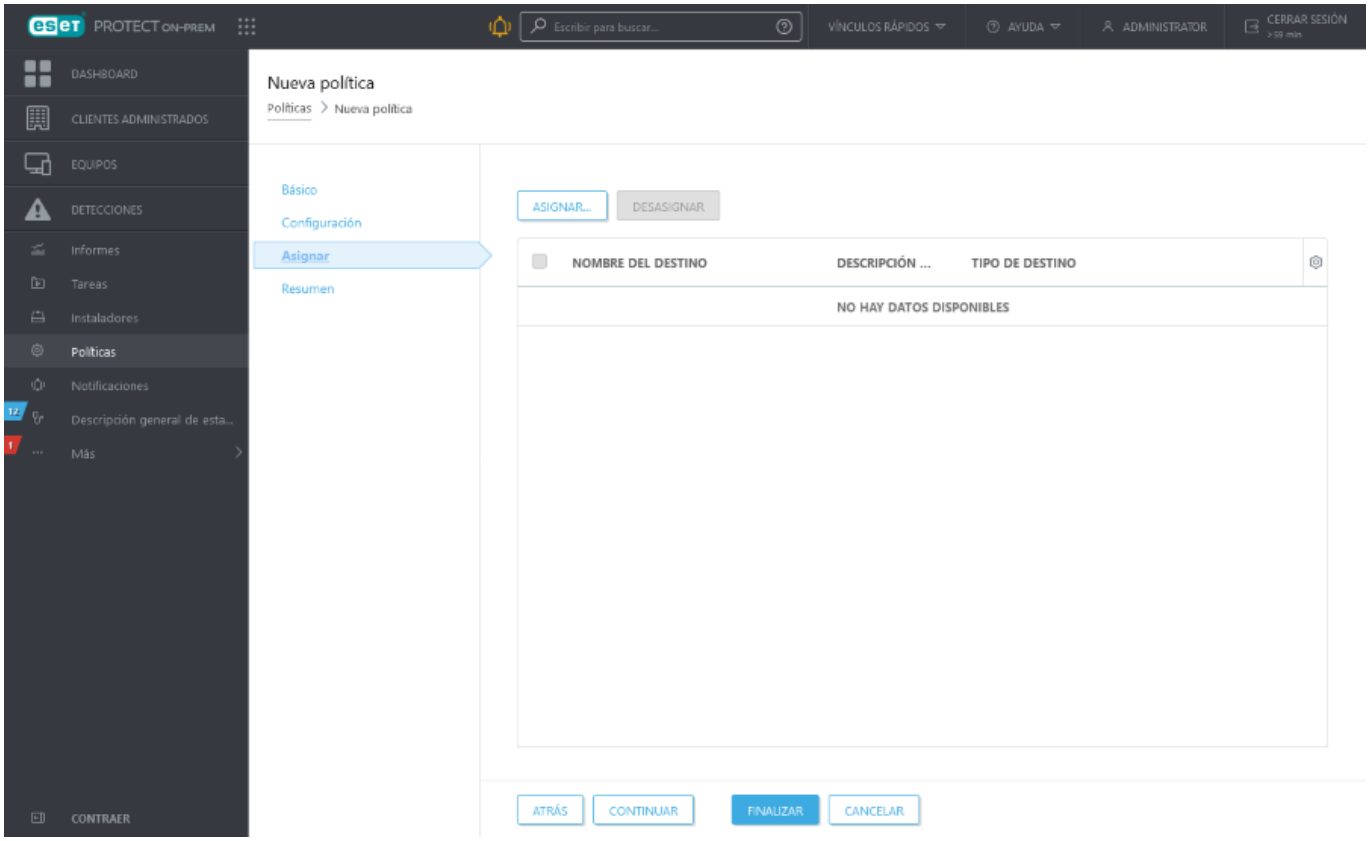
Configuración

Seleccione **Agente ESET Management** en la lista desplegable > expanda **Configuración** > haga clic en **Configurar** junto a **Configuración protegida por contraseña** y escriba la contraseña. Se requerirá esta contraseña si alguien intenta desinstalar o reparar el agente ESET Management en un equipo cliente.

Registre la contraseña en un lugar seguro. Si el agente ESET Management está protegido por contraseña, debe proporcionar la contraseña para desinstalar, reparar o actualizar (con cambios).

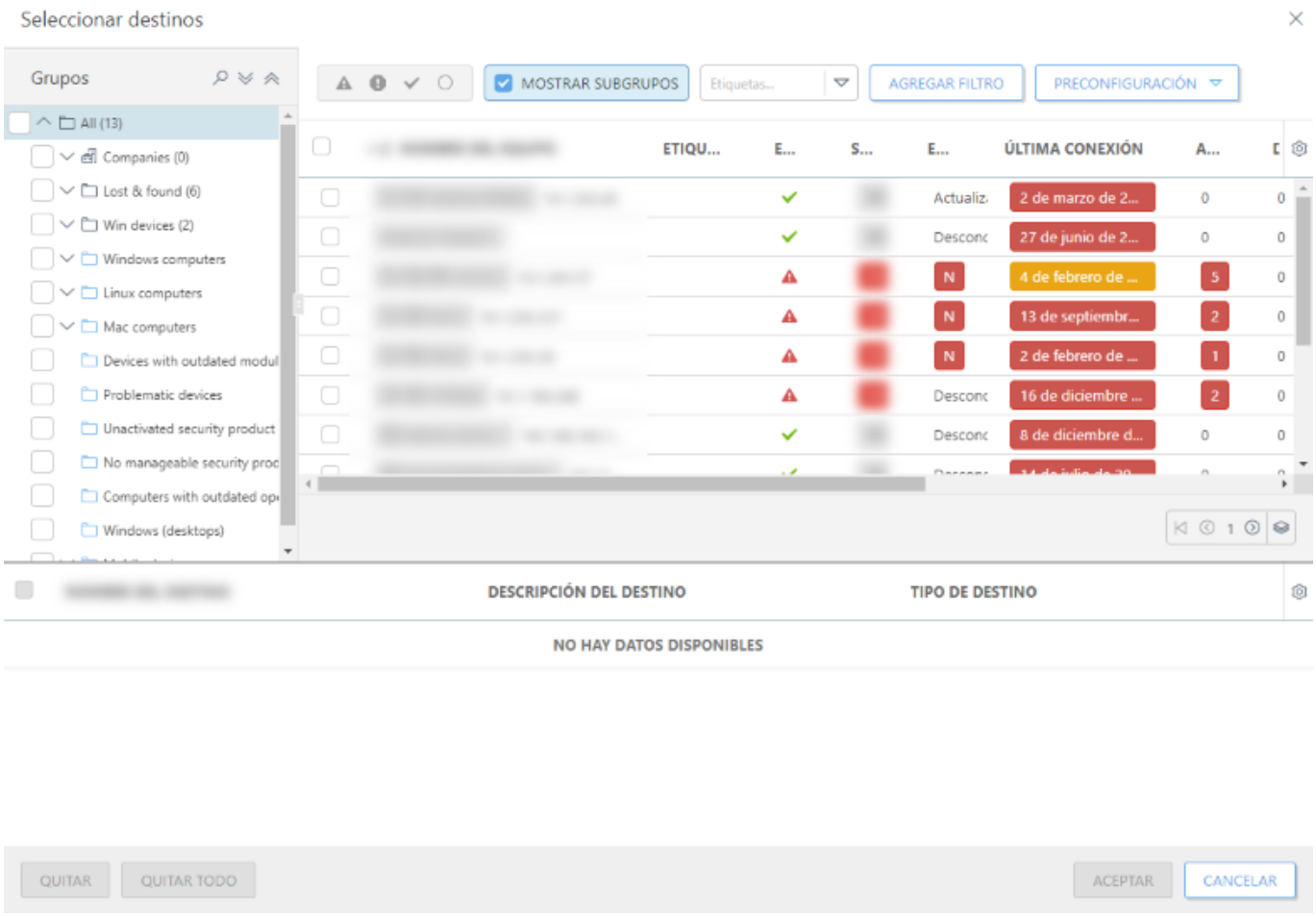
Asignar

Especifique los clientes (equipos/dispositivos móviles individuales o grupos completos) que serán los destinatarios de esta directiva.



Haga clic en **Asignar** para visualizar todos los Grupos estáticos y dinámicos y a sus miembros. Seleccione los equipos o grupos que desee y haga clic en **Aceptar**.

Para asignar todos los equipos de un grupo, asigne el grupo en lugar de los equipos individuales para evitar que la consola web se ralentice.
Si selecciona una gran cantidad de equipos, la consola web muestra una advertencia.



Resumen

Revise la configuración de esta política y haga clic en **Finalizar**. La política se aplica a los destinos después de su próxima conexión con el servidor de ESET PROTECT (en función del intervalo de conexión del agente).

Para aplicar la política inmediatamente, puede ejecutar la acción **Enviar llamada de activación** en los destinos de los **Equipos**.

Resolución de problemas: conexión del Agente

Cuando un equipo cliente no parece conectarse a su servidor ESET PROTECT, le recomendamos realizar una resolución de problemas del agente ESET Management localmente en el equipo cliente.

En forma predeterminada, el agente ESET Management se sincroniza con el servidor ESET PROTECT cada 20 minutos. Puede cambiar esta configuración al crear una nueva política para el intervalo de conexión del agente ESET Management.

Consulte el último archivo de registro del agente ESET Management. Puede encontrarlo aquí:

Windows	*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs*
Linux	*/var/log/eset/RemoteAdministrator/Agent/* */var/log/eset/RemoteAdministrator/EraAgentInstaller.log*
macOS	*/Library/Application Support/com.eset.remoteadministrator.agent/Logs/* */Users/%user%/Library/Logs/EraAgentInstaller.log*

• **last-error.html**: protocolo (tabla) que muestra el último error registrado mientras el agente ESET Management se encuentre en ejecución.

• **software-install.log**: protocolo de texto de la última tarea de instalación remota ejecutada por el agente ESET Management.

• **trace.log**: un informe detallado de toda la actividad del agente ESET Management que incluye cualquier error registrado.

> 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).

• **status.html**: una tabla que muestra el estado actual de las comunicaciones (sincronización) del agente ESET Management con el servidor ESET PROTECT. El registro también incluye la configuración del proxy HTTP, una lista de las políticas aplicadas (incluidas las exclusiones aplicadas) y una lista de grupos dinámicos a los cuales pertenece el dispositivo.

> Le recomendamos que lea nuestro artículo de la base de conocimiento sobre cómo usar el archivo status.html para la resolución de problemas de conexión del agente.

Los problemas más comunes que pueden evitar que el agente ESET Management se conecte al servidor ESET PROTECT son:

• Su red interna no está configurada correctamente. Asegúrese de que el equipo donde se encuentra instalado el servidor ESET PROTECT se pueda comunicar con equipos cliente donde el agente ESET Management se encuentre instalado.

• Su servidor ESET PROTECT no está configurado para escuchar el puerto 2222.

• El DNS no funciona adecuadamente o los puertos están bloqueados por un firewall; consulte nuestra lista de puertos utilizados por ESET PROTECT On-Prem, o consulte nuestro artículo en la Base de conocimientos ¿Qué direcciones en mi firewall de terceros debería abrir para permitir el completo funcionamiento de mi producto ESET?

• Se cuenta con un certificado generado erróneamente que cuenta con funciones falsas o limitadas que no son iguales a la clave pública de la autoridad de certificación del servidor ESET PROTECT; cree un nuevo certificado de agente ESET Management para resolverlo.

• Consulte nuestro artículo de la base de conocimiento para resolver la alerta **El dispositivo usa una conexión de conmutación por error**.

Resolución de problemas: implementación del Agente

Es posible que experimente problemas con la implementación del agente ESET Management. Si la implementación falla, existen diferentes razones que pueden ser la causa. Esta sección le ayudará a:

- Descubrir qué produjo que la implementación del agente ESET Management fallara

- Controlar las causas posibles de acuerdo con la siguiente tabla
- Resolver el problema y realizar una implementación exitosa

Windows

1. Para descubrir por qué falló la implementación del agente, vaya a **Informes** > **Automatización**, seleccione **Información sobre las tareas de implementación del Agente de los últimos 30 días**.
Se mostrará una tabla con información de la implementación. La columna **Progreso** muestra los mensajes de error acerca de por qué falló la implementación del agente.

Si necesita incluso más detalles, puede modificar el nivel de detalle del registro de seguimiento del servidor ESET PROTECT. Navegue hacia **Más** > Configuración > **Configuración avanzada** > **Registro** y seleccione **Error** del menú desplegable. Ejecute la implementación del agente otra vez y, cuando falle, controle las últimas entradas del registro de seguimiento del servidor ESET PROTECT en la parte inferior del archivo. El informe incluirá sugerencias sobre cómo resolver el problema.

El último archivo se puede encontrar aquí:

Registro del servidor ESET PROTECT	*C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs\trace.log*
Registro del agente ESET Management	*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs*

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 reiniciar el servicio del agente de ESET Management).
En caso de problemas de conexión del agente ESET Management, consulte Resolución de problemas: conexión de agente para más información.

2. La siguiente tabla contiene varias razones por las cuales la implementación del agente puede fallar:

Mensaje de error	Causa(s) posible(s)
No se pudo conectar	• No se puede localizar el cliente en la red, el firewall bloquea la comunicación • Los puertos de ingreso 135, 137, 138, 139 y 445 no están abiertos en el firewall del cliente o en Windows Firewall: No se usa la excepción de uso compartido de archivo entrante e impresora • No se pudo resolver el nombre de host del cliente, utilice nombres de equipos FQDN válidos
Acceso denegado	• Cuando realice una instalación desde un servidor unido al dominio, a un cliente unido al dominio, use credenciales de un usuario que sea miembro del grupo Administrador de dominio en formato: **Domain\DomainAdmin** • Cuando realice una implementación desde un servidor unido al dominio a un cliente unido al dominio, puede elevar provisoriamente el servicio del servidor ESET PROTECT desde el servicio de red para ejecutar en la cuenta del administrador de dominio. • Cuando realice la implementación desde un servidor a un cliente que no se encuentra en el mismo dominio, deshabilite el filtrado remoto UAC en el equipo de destino. • Cuando realice una instalación desde un servidor a un cliente en un dominio diferente, use las credenciales de un usuario local que sea miembro del grupo de administradores en el siguiente formato: **Admin**. El nombre del equipo de destino se anexará automáticamente al inicio de sesión. • No se configuró la contraseña para la cuenta del administrador • Permisos de usuarios insuficientes • El recurso compartido de *ADMIN$* no se encuentra disponible • El recurso compartido de *IPC$* no se encuentra disponible • Compartido simple de archivos está habilitada
No se encontró el paquete en el repositorio	• El vínculo al repositorio es incorrecto • El repositorio no está disponible • El repositorio no contiene el paquete requerido
Error 1603	• Compruebe el archivo *ra-agent-install.log*. Se puede localizar en: *C:\Users\%user%\AppData\Local\Temp\ra-agent-install.log* en el equipo destino. • Si el error persiste, siga nuestro artículo de la base de conocimiento.

3. Siga los pasos adecuados para la resolución de problemas de acuerdo con la causa posible:

- **No se puede localizar el cliente en la red**: compruebe la disponibilidad del cliente en el servidor ESET PROTECT. Si obtiene una respuesta, intente iniciar sesión en el equipo cliente de forma remota (por ejemplo, por medio de un escritorio remoto).

- **El firewall bloquea la comunicación**: controle la configuración del firewall en el servidor y en el cliente, así

como también cualquier otro firewall que exista entre estos dos equipos (si corresponde).

- **No se pudo resolver el nombre del host del cliente**: las soluciones posibles para los problemas de DNS pueden incluir, entre otras:

  - Uso del comando `nslookup` de la dirección IP y el nombre de host del servidor o los clientes que tienen problemas con la implementación del Agente. Los resultados deben coincidir con la información del equipo. Por ejemplo, un `nslookup` de un nombre de host debe resolver en la dirección IP el comando `ipconfig` que se muestra en el host en cuestión. Deberá ejecutarse el comando `nslookup` en los clientes y en el servidor.

  - Examinar en forma manual si los registros de DNS tienen duplicados.

- **Los puertos 2222 y 2223 no están abiertos en el firewall:** de la misma forma que en el punto anterior, asegúrese de que estos puertos estén abiertos en todos los firewalls entre los dos equipos (cliente y servidor).

- **No se configuró la contraseña para la cuenta del administrador:** configure una contraseña adecuada para la cuenta del administrador (no use una contraseña en blanco)

- **Derechos de acceso insuficientes:** intente usar las credenciales del Administrador de dominios al crear una Tarea de implementación del agente. Si el equipo cliente se encuentra en un grupo de trabajo, use la cuenta del Administrador local en ese equipo en particular.

> Luego de una implementación exitosa, los puertos 2222 y 2223 no están abiertos en el firewall. Asegúrese de que estos puertos estén abiertos en el firewall entre los dos equipos (cliente y servidor).

- **Para activar** la cuenta del usuario Administrador:

  1. Abra un símbolo del sistema administrativo

  2. Tipo el siguiente comando:

```
net user administrator /active:yes
```

- **El recurso compartido administrativo ADMIN$ no está disponible**: el equipo cliente debe tener el recurso compartido *ADMIN$* activado; asegúrese de que esté presente entre el resto de los recursos compartidos (**Inicio** > **Panel de control** > **Herramientas de administración** > **Administración de quipos** > **Carpetas compartidas** > **Recursos compartidos**).

- **El recurso compartido administrativo IPC$ no está disponible**: verifique que el servidor pueda acceder a *IPC$*, al emitir lo siguiente desde el símbolo del sistema en el servidor:

  `net use \\clientname\IPC$` donde `clientname` es el nombre del equipo de destino.

- **Usar intercambio de archivos simple se encuentra habilitado**: si obtiene el mensaje de error **Acceso denegado** y tiene un entorno mixto (contiene tanto un dominio como un grupo de trabajo), deshabilite **Usar intercambio de archivos simple** o **Usar asistente de intercambio** en todos los equipos que tengan problemas con la implementación del Agente. Por ejemplo, en Windows 11 realice lo siguiente:

  - Haga clic en **Inicio**, escriba `Explorador de archivos` en el cuadro de **búsqueda** y, a continuación, haga clic en **Opciones del Explorador de archivos**. Haga clic en la pestaña **Ver** y, en el cuadro **Configuración avanzada**, desplácese hacia abajo en la lista y quite la selección de la casilla de verificación

que está junto a **Usar el asistente de intercambio**.

- **El vínculo para el repositorio es incorrecto:** en la consola web ESET PROTECT, vaya a **Más** > Configuración, haga clic en **Configuración avanzada** > **Repositorio** y asegúrese de que la URL del repositorio sea correcta.

- **No se encontró el paquete en el repositorio:** este mensaje de error aparece, generalmente, cuando no hay ninguna conexión con el repositorio de ESET PROTECT On-Prem. Controle su conexión a Internet.

Linux y macOS

Si la implementación del agente no funciona en macOS, el problema se relaciona, generalmente, con el SSH. Controle el equipo cliente y asegúrese de que el daemon SSH se esté ejecutando. Una vez solucionado, ejecute la implementación del Agente nuevamente.

Escenarios de ejemplo de implementación del agente ESET Management

Esta sección contiene cuatro escenarios verificados para la implementación de ESET PROTECT On-Prem.

1.Implementación del aparato del servidor ESET PROTECT o el servidor ESET PROTECT para Linux para objetivos de Windows que no participan en un dominio.

2.La implementación del servidor ESET PROTECT para Windows desde la fuente de Windows que no participa en un dominio para objetivos de Windows que no participan en un dominio.

3.Implementación del aparato del servidor ESET PROTECT o el servidor ESET PROTECT para Linux para objetivos de Windows que participan en un dominio.

4.La implementación del servidor ESET PROTECT para Windows desde la fuente de Windows que participa en un dominio para objetivos de Windows que participan en un dominio.

Escenarios de ejemplo del uso del agente ESET Management para objetivos que no participan del dominio

En las siguientes instrucciones se cubren estas situaciones:

- Implementación del aparato del servidor ESET PROTECT o el servidor ESET PROTECT para Linux para objetivos de Windows que **no participan en un dominio**.

- La implementación del servidor ESET PROTECT para Windows desde la fuente de Windows que no participa en un dominio para objetivos de Windows que **no participan en un dominio**.

Condiciones previas:

- Misma red local.
- Nombres de FQDN trabajo, por ejemplo: desktop-win7.test.local mapas para 192.168.1.20 y viceversa.
- Sistema operativo limpio instalado desde MSDN con los valores predeterminados.

Destinos:

Windows 10 Enterprise

1. Creación de un usuario con contraseña que es miembro del grupo de Administradores, por ejemplo: **Admin**.

   a.Abra la **Consola de administración de Microsoft** abriendo la consola **Ejecutar** y escriba "`mmc`" en el campo y haga clic en **OK**.

   b.Agregue el **complemento Usuarios locales y grupos** desde **Archivo** > **Agregar/eliminar complemento**. Agregue un usuario nuevo en la carpeta **Usuarios** y rellene la información necesaria en los campos (no olvide rellenar la contraseña). En la sección **Grupos** abra las **Propiedades** del grupo de **Administradores** y agregue el nuevo usuario creado en el grupo haciendo clic en el botón **Agregar**. Rellene el nombre de inicio de sesión del nuevo usuario creado en **Ingrese los nombres del objeto a seleccionar** y verifíquelo haciendo clic en botón **Comprobar nombres**.

2. En el **Centro de redes y recursos compartidos** cambie la configuración de **Red pública** a **Red privada** haciendo clic en **Red pública** en el lado izquierdo de la **sección Ver la actividad de la red**.

3. Deshabilite el **Firewall de Windows** para la **Red privada** haciendo clic en **Encender o apagar el Firewall de Windows** y seleccione **Apagar el Firewall de Windows** en la configuración de ubicación en la red hogar o **trabajo**.

4. Compruebe que el **Uso compartido de archivos e impresoras** esté habilitado para la **Red privada** haciendo clic en la **Cambiar la configuración avanzada de uso compartido** en el **Centro de redes y recursos compartidos**.

5. Desactivar restricciones remotas de Control de cuentas de usuario (UAC):

   a.Abra el **Editor de registro** y escriba `regedit` en la consola de **Ejecutar** y busque `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`

   b.En el archivo de **Sistema**, cree un nuevo **valor DWORD** con el nombre `LocalAccountTokenFilterPolicy`.

   c.Abra el archivo creado y establezca los **datos de valor** en **1**.

Consola web ESET PROTECT:

En la consola web de ESET PROTECT, cree una nueva tarea del servidor de Instalación del agente:

1. **Destinos:** seleccione los ordenadores Windows de destino.

2. **Nombre de host del servidor (opcional)**: escriba el nombre de FQDN o la dirección IP del servidor de ESET PROTECT. (Puede encontrar el nombre del equipo de FQDN haciendo clic con el botón derecho del ratón en **Ordenador** y seleccionando **Propiedades**. El nombre FQDN aparece junto al **Nombre completo del equipo**).

3. **Nombre de usuario**: escriba **Admin** (sin nombre de dominio ni prefijo del nombre del ordenador) y escriba la **contraseña** de este usuario.

4. **Certificado de ESET PROTECT**: haga clic en **Sin certificado seleccionado** y seleccione **Certificado del agente**.

5. Haga clic en **Finalizar** para ejecutar la tarea.

Escenarios de ejemplo de la implementación del agente ESET Management para objetivos que participan del dominio

En las siguientes instrucciones se cubren estas situaciones:

- Implementación del aparato del servidor ESET PROTECT o el servidor ESET PROTECT para Linux para objetivos de Windows que **participan en un dominio**.

- La implementación del servidor ESET PROTECT para Windows desde la fuente de Windows que participa en un dominio para destinos de Windows que **participan en un dominio**.

Condiciones previas:

- Misma red local.

- Nombres de FQDN trabajo, por ejemplo: desktop-win10.protect.local mapas para 10.0.0.2 y viceversa.

- Sistema operativo limpio instalado desde MSDN con los valores predeterminados.

- Dominio creado `protect.local` con nombre NetBIOS `PROTECT`.

- El usuario `DomainAdmin` creado que es miembro del grupo de seguridad `Domain Admins` en el controlador de dominio.

- Cada máquina se ha unido al dominio `protect.local` con el usuario `DomainAdmin` y este usuario es administrador.

- `DomainAdmin` está habilitado para iniciar sesión en cada máquina y realizar tareas de administración local.

- El servicio del servidor ESET PROTECT para Windows se ejecuta de manera temporal bajo las credenciales "`PROTECT\DomainAdmin`". Tras la instalación, la cuenta de **Servicio de red** es suficiente (no es necesario realizar ningún cambio en el aparato virtual ni en Linux).

Destinos:

Windows 10 Enterprise

1. Abra el **Centro de redes y recursos compartidos**.

2. Compruebe que la red sea la **Red de dominios** en la sección **Ver redes activas**.

3. Deshabilite el **Firewall de Windows** para la **Red de dominio** haciendo clic en **Encender o apagar el firewall de Windows** y seleccione**Apagar el firewall de Windows** en la **configuración de ubicación de red de dominios**.

4. Compruebe que el **Uso compartido de archivos e impresoras** esté habilitado para la **Red de dominio** haciendo clic en la **Cambiar la configuración avanzada de uso compartido** en el **Centro de redes y recursos compartidos**.

Consola web ESET PROTECT:

En la consola web de ESET PROTECT, cree una nueva tarea del servidor de Instalación del agente:

1. **Destinos:** seleccione los ordenadores Windows de destino.

2. **Nombre de host del servidor (opcional)**: escriba el nombre de FQDN o la dirección IP del servidor de ESET PROTECT. (Puede encontrar el nombre del equipo de FQDN haciendo clic con el botón derecho del ratón en **Ordenador** y seleccionando **Propiedades**. El nombre FQDN aparece junto al **Nombre completo del equipo**).

3. **Nombre de usuario**: escriba **PROTECT\DomainAdmin** (es importante incluir todo el dominio) y escriba la **contraseña** de este usuario.

4. **Certificado de ESET PROTECT**: haga clic en **Sin certificado seleccionado** y seleccione **Certificado del agente**.

5. Haga clic en **Finalizar** para ejecutar la tarea.

ESET PROTECT On-Prem Menú principal

Todos los clientes se administran a través de la consola web ESET PROTECT. Puede acceder a la consola web ESET PROTECT desde cualquier dispositivo por medio de un navegador compatible. Se puede acceder al **Menú principal** desde la izquierda en todo momento, excepto mientras se utiliza un asistente. Haga clic en para expandir el menú en el lateral izquierdo de la pantalla. Para colapsarlo, haga clic en **Colapsar**.

El menú principal de la izquierda contiene las secciones principales de ESET PROTECT On-Prem los siguientes elementos:

Dashboard
Clientes administrados
Equipos
Detecciones

Informes
Tareas
Instaladores
Políticas
Notificaciones
Información general de estado
Más

Tablero

El tablero es la página predeterminada que se visualiza luego de que inicie sesión en la consola web ESET PROTECT por primera vez. Muestra los informes predefinidos sobre su red. Puede alternar entre los tableros por medio de las pestañas que se encuentran en la barra superior del menú. Cada tablero consta de varios informes.

Manipulación del tablero

- **Agregar**: haga clic en el símbolo + en la parte superior del encabezado del tablero para agregar un nuevo tablero. Ingrese un nombre para el tablero nuevo y haga clic en **Agregar tablero** para confirmar. Se crea un nuevo tablero en blanco.
- **Mover**: haga clic en el nombre de un tablero y arrástrelo para cambiar su ubicación en relación con otros tableros.
- Puede personalizar sus tableros al agregar, modificar, cambiar el tamaño, mover o reorganizar informes.
- Seleccione el dashboard, haga clic en el ícono de engranaje junto a y seleccione **Establecer como predeterminado** para usarlo como predeterminado para todos los nuevos usuarios de la consola web con acceso a los dashboards.
- **Los usuarios de MSP** pueden hacer clic en **Seleccionar** junto al cliente de MSP para filtrar la vista del dashboard para el cliente seleccionado.

Haga clic en el ícono del engranaje junto al título del tablero seleccionado para obtener las siguientes opciones en el menú desplegable:

Actualizar página	Actualiza las plantillas de informes en este tablero.
Eliminar	Elimina un tablero.
Cambiar nombre	Cambia el nombre del tablero.
Duplicar	Crea una copia del tablero con los mismos parámetros en el grupo hogar del usuario.
Cambiar el diseño	Elige un nuevo diseño para este tablero. El cambio eliminará las plantillas actuales del tablero.

No puede personalizar estos tableros predeterminados: **Descripción general del estado**, **descripción general de la seguridad** y **ESET LiveGuard**.

Los siguientes tableros vienen preconfigurados en ESET PROTECT On-Prem:

Información general de estado

El tablero **Información general de estado** es la pantalla predeterminada que se ve al iniciar sesión en ESET PROTECT On-Prem (excepto que defina otro tablero como predeterminado). Muestra información general sobre su red.

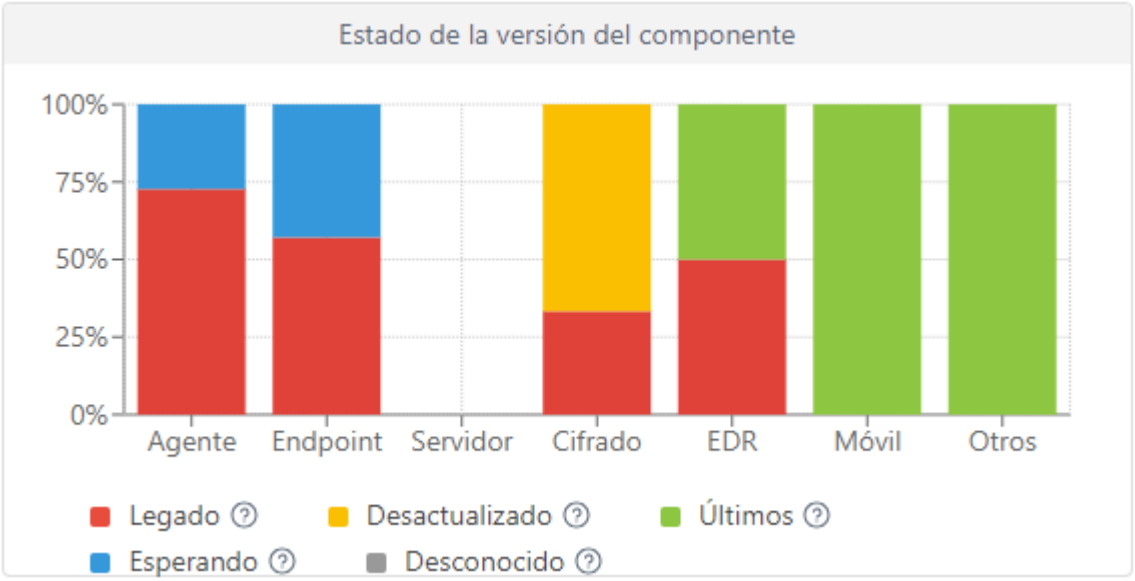
Filtros del dispositivo: muestra la cantidad de dispositivos administrados según el último estado informado. Puede hacer clic en cada uno de los 4 mosaicos para abrir una lista filtrada de dispositivos.

Estado del dispositivo: muestra la cantidad de dispositivos administrados en el producto de seguridad instalado en las pestañas correspondientes. Si no se implementa ningún producto de seguridad de ese grupo, la pestaña mostrará una opción para implementar el paquete de instalación respectivo.

Estado de conexión: muestra la lista de las últimas conexiones de dispositivos administrados.

Estado de la versión del componente

En el gráfico, se muestra la proporción de versiones de componentes de ESET actualizadas y desactualizadas, o de versiones de productos de seguridad de ESET.



Haga clic en el gráfico amarillo o rojo que representa los componentes o aplicaciones desactualizadas y seleccione **Actualizar los componentes de ESET instalados** para iniciar una actualización. Consulte también la Política sobre el fin de ciclo de vida de ESET para productos empresariales.

- **Rojo**(**heredado**): una versión heredada del componente o producto de ESET, o una versión anterior con una vulnerabilidad de seguridad detectada que ya no es compatible y ya no está en ESET Repository.

- **Amarillo** (**desactualizado):** la versión instalada del componente o producto de ESET está desactualizada pero sigue siendo compatible. Por lo general, dos versiones anteriores a la versión más reciente se encuentran en estado amarillo, a menos que contengan una vulnerabilidad de seguridad recientemente detectada.

- **Verde** (**correcto**): está instalada la versión más reciente del componente o producto de ESET o la versión instalada es la última versión del componente o producto de ESET compatible con la consola web ESET

PROTECT utilizada.

> Las versiones anteriores de componentes o productos de ESET informan que son **Correctas** (**verde**) en el gráfico si no hay ninguna versión más reciente del componente o producto compatible en ESET Repository para la versión o la plataforma específicas del sistema operativo (x86, x64, ARM64).

• **Azul** (**en espera**): las actualizaciones automáticas están activadas y la versión más reciente se instalará automáticamente. Obtenga más información sobre las actualizaciones automáticas de lo siguiente:

- ESET Management Agentes
- Productos de seguridad ESET

> Si los componentes de ESET no se actualizan durante mucho tiempo, puede actualizarlos manualmente haciendo clic en el gráfico azul y seleccionando **Actualizar componentes de ESET instalados**. Como alternativa, puede usar la Tarea Cliente de actualización de componentes de ESET PROTECT para actualizar los agentes y la Tarea Cliente de instalación de software para actualizar los productos de seguridad de ESET.

• **Gris** (**desconocido**): no se reconoce la versión del componente o producto de ESET (por ejemplo, poco después de una nueva instalación del producto de ESET).

Estado de administración: muestra la cantidad de dispositivos **Administrados y protegidos** (dispositivos cliente con agente ESET y producto de seguridad instalados), **Administrado** (dispositivos cliente solo con agente ESET), **Sin administrar** (dispositivos cliente en su red conocidos para ESET PROTECT On-Prem pero sin agente) y **Rogue** (dispositivos cliente desconocidos para ESET PROTECT On-Prem pero detectados por Rogue Detection Sensor).

Fuente RSS: muestra una fuente RSS de WeLiveSecurity y Eset Knowledgebase Portal. Cuando hace clic en el ícono del engranaje en **fuente RSS**, puede optar por **Apagar la reproducción automática de la fuente**, o apagar el origen de la fuente individual, o **Apagar la fuente RSS**.

Descripción general de incidentes

El tablero provee una vista general de detecciones sin resolver que se detectaron en los 7 días anteriores, incluyendo seriedad, método de detección, estado de resolución y los 10 equipos/usuarios con más incidentes.

ESET LiveGuard

Si usa ESET LiveGuard Advanced, aquí encontrará una descripción general de los informes ESET LiveGuard Advanced útiles. Haga clic en el ícono del engranaje situado en la parte superior (junto a) y seleccione **Ocultar/Mostrar ESET LiveGuard** para ocultar/mostrar el dashboard.

Equipos

Este tablero le proporciona una visión general de los equipos cliente, que incluye su estado de protección, sistemas operativos y estado de actualización.

Estado del rendimiento del servidor

En este tablero, puede visualizar información acerca del servidor de ESET PROTECT en sí, que incluye carga del servidor, clientes con problemas, carga de la CPU y conexiones de la base de datos.

Detecciones de antivirus

Aquí, puede ver los informes del módulo antivirus de los productos de seguridad del cliente, que incluye detecciones activas, detecciones en los últimos 7/30 días, etc.

Detecciones de firewall

Los eventos de firewall de los clientes conectados según su gravedad, tiempo de generación de informes, etc.

Aplicaciones de ESET

Este dashboard le permite ver información sobre las aplicaciones ESET instaladas.

Protección basada en la nube

Este dashboard le ofrece una visión general de los informes de protección basados en la nube (ESET LiveGrid® y, si tiene la licencia válida, también ESET LiveGuard Advanced).**Acciones en un informe de tablero**

Cambiar de tamaño	Haga clic para ver un informe en modo de pantalla completa.
Actualizar	Actualiza las plantillas de informes.
Descargar	Haga clic en **Descargar** para generar y descargar el informe. Puede seleccionar entre *.pdf* o *.csv*. CSV es apto únicamente para datos de tablas y usa ; (punto y coma) como delimitador Si descarga un informe de CSV y ve los números en una columna en la que esperaba ver texto, le recomendamos descargar un informe de PDF para ver los valores de texto.
Cambiar	Cambia la plantilla de informes por otra de la lista de plantillas.
Editar la plantilla de informes	Edite una plantilla de informe existente. Se aplican las mismas opciones y la misma configuración utilizadas para crear una plantilla de informe nueva.
Configurar intervalo de actualización	Configure intervalos de actualización personalizados para la plantilla.
Programar	Programar informe: puede modificar el desencadenador programado, la limitación y la entrega del informe. Puede encontrar todos los informes programados en la **pestaña Informes programados**.
Eliminar	Elimina la plantilla de informes desde el tablero.
Cambiar nombre	Cambia el nombre de la plantilla de informes.
Esta celda	Elige un nuevo diseño para este tablero. El cambio eliminará las plantillas actuales del tablero.

Permisos para el tablero

Un usuario debe contar con los permisos adecuados para trabajar con los tableros. Solo se pueden utilizar en un tablero las plantillas de informe dentro de un grupo al que el usuario tiene derechos de acceso. Si el usuario no tiene derechos asignados para **Informes y Tablero, el usuario no verá datos en la sección Tablero**. Por defecto, el administrador puede ver todos los datos.

- **Lectura**: el usuario puede enumerar las plantillas de informes y sus categorías, generar informes basados en plantillas de informes y leer su tablero
- **Uso**: el usuario puede modificar su propio tablero con las plantillas de informes disponibles
- **Escritura**: crear/modificar/quitar plantillas y sus categorías

Todas las plantillas predeterminadas se encuentran en el grupo **Todos**.

Exploración en profundidad

Puede usar la función de exploración en profundidad del tablero para examinar datos con mayor detalle. Le permite seleccionar de manera interactiva elementos específicos de un resumen y visualizar sus datos detallados. Enfóquese en los elementos de interés mediante la "exploración en profundidad" de la información del resumen a fin de obtener más información respecto de este elemento en particular. Suelen existir múltiples niveles que puede explorar en profundidad.

Existen varias opciones de exploración en profundidad:

- Mostrar **Información detallada:** nombre y descripción del equipo, nombre del Grupo estático, etc. Muestra los datos originales (no agregados) para la fila marcada.

- Mostrar **Solo** *"valor"*: Solo muestra los datos con el nivel de severidad seleccionado: Información, crítico, riesgo de seguridad, notificación de seguridad, etc.

- **Expandir columna** *"valor"*: esto mostrará información agregada (generalmente para una cuenta o suma). Por ejemplo, si hay solo un número en la columna y hace clic en Expandir columna Equipa, mostrará los detalles de los equipos.

- Mostrar **En la página Equipos (todos):** lo redirige a la página **Equipos** (muestra un resultado de solo 100 elementos).

Acciones de un solo clic.

Los informes con información sobre los problemas descubiertos contienen opciones adicionales de exploración en profundidad cuando hace clic en el elemento en la tabla o gráfico:

- '*tarea para resolver la alerta seleccionada*': puede resolver la alerta al seleccionar la tarea sugerida, que se ejecutará lo antes posible.

  Si la alerta no se puede resolver con una tarea, pero se puede resolver con una configuración de política, aparecerán las siguientes opciones:

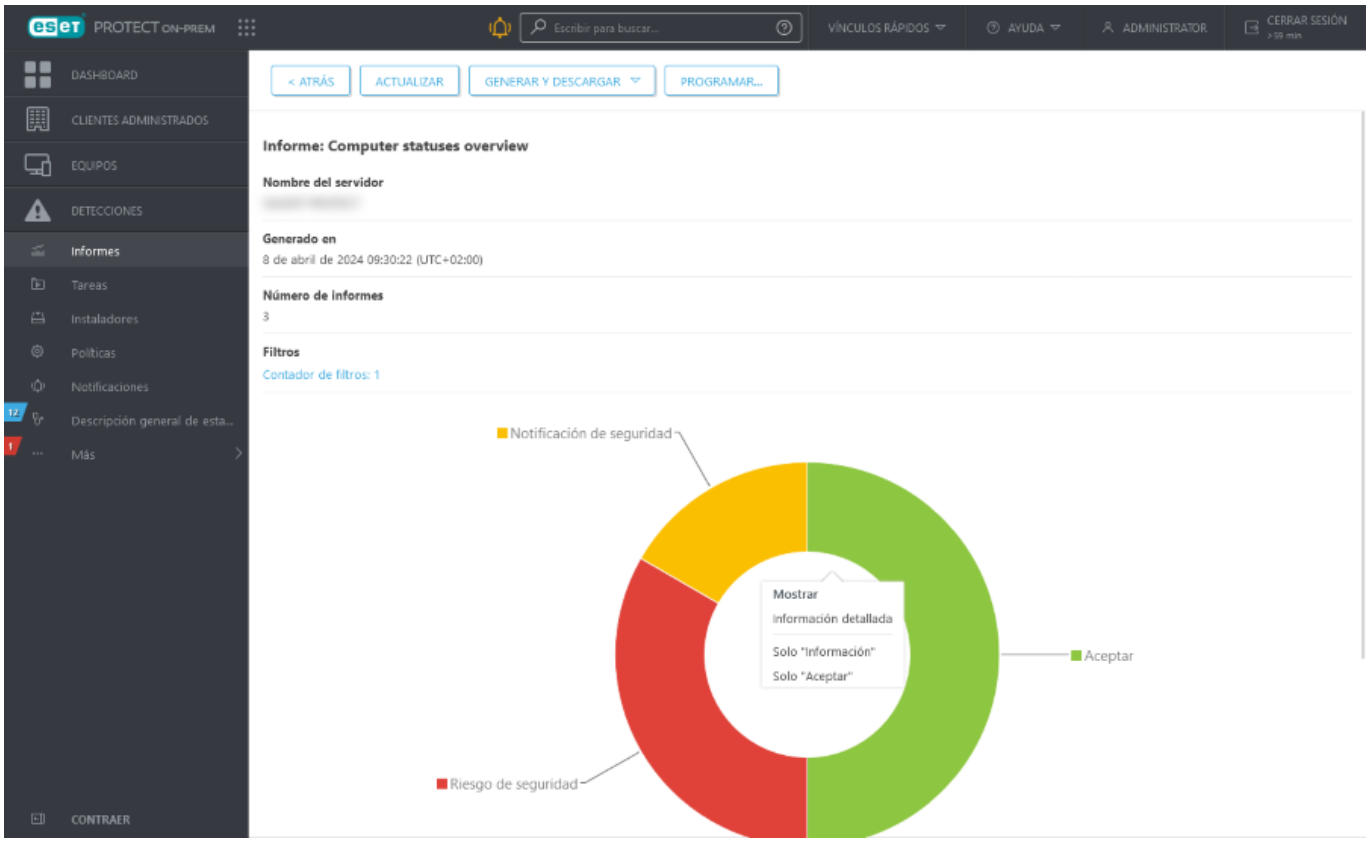
  - Administrar políticas

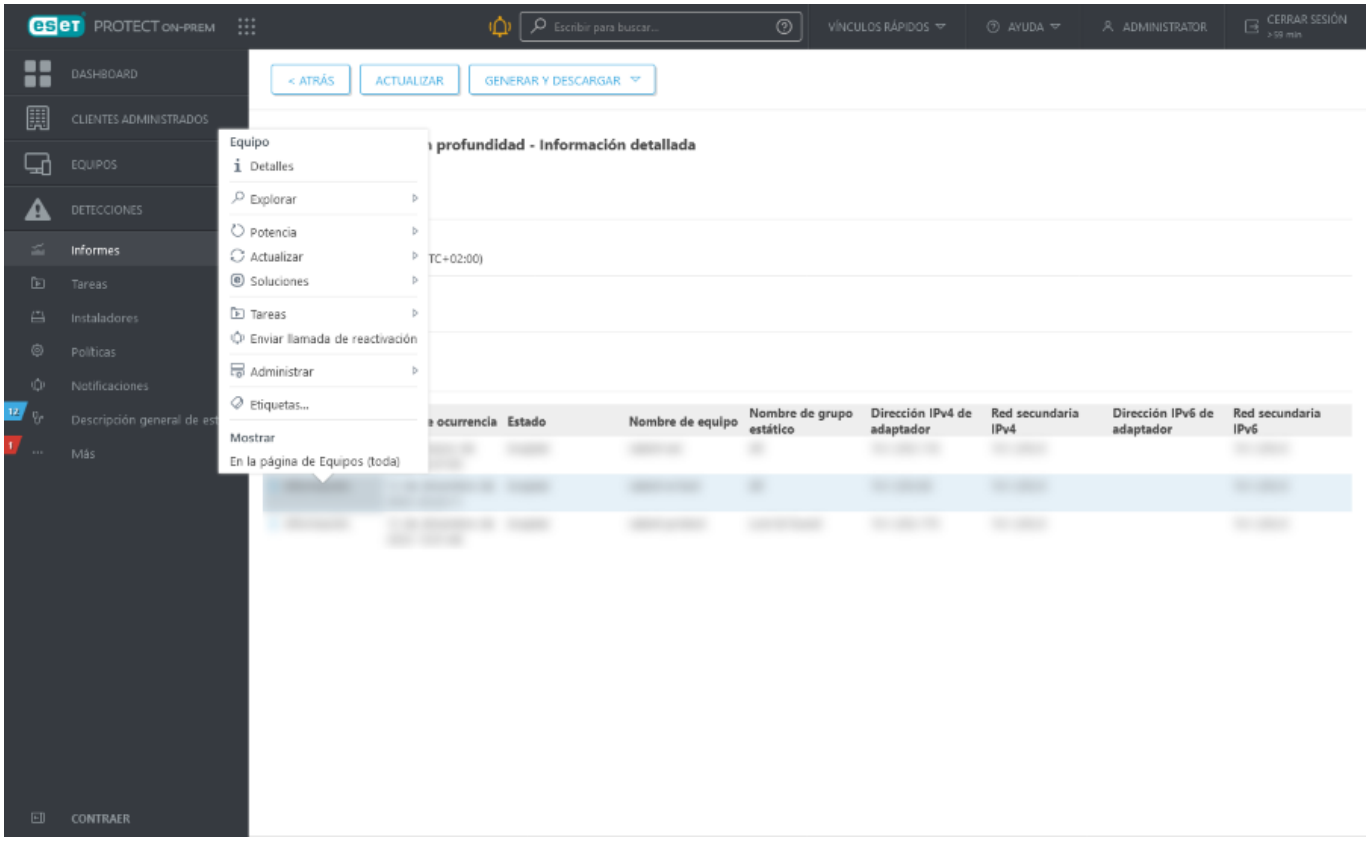
  - **Nueva política**

- **Buscar en la red**: Desencadena una búsqueda en Google para la alerta seleccionada. Puede usar esta opción si no hay una respuesta sugerida (tarea o configuración de política) para resolver la alerta seleccionada.

Los resultados que obtiene con la exploración en profundidad de otros informes mostrará los primeros 1000 elementos solamente.

Haga clic en el botón **Generar y descargar** si desea generar y descargar el informe. Puede seleccionar entre *.pdf* o *.csv*. CSV es apto únicamente para datos de tablas y usa ; (punto y coma) como delimitador Si descarga un informe de CSV y ve los números en una columna en la que esperaba ver texto, le recomendamos descargar un informe de PDF para ver los valores de texto.





Clientes administrados

La sección **Clientes administrados** del menú principal de ESET PROTECT On-Prem solo está disponible para los usuarios del proveedor de servicios administrados (MSP).

En la sección **Clientes administrados**, el usuario MSP puede ver la lista de clientes administrados:

- Haga clic en el nombre del cliente para ver los detalles del cliente: estos son detalles de grupos estáticos porque los grupos estáticos representan a los clientes de ESET PROTECT On-Prem
- Haga clic en un número de la tabla para obtener detalles sobre los dispositivos, las detecciones (sin resolver) y las licencias del cliente

Puede personalizar la tabla principal (ajustar las columnas visibles, agregar o eliminar columnas).

Filtrado de clientes administrados

Puede filtrar los clientes administrados por nombre de cliente:

- En **Clientes administrados**:Para agregar criterios de filtrado, haga clic en **Agregar filtro** y seleccione los elementos de la lista. Escriba las cadenas de búsqueda o seleccione los elementos del menú desplegable en los campos de filtrado y pulse **Intro**. Los filtros activos están resaltados en azul. También puede usar ajustes preestablecidos de filtro
- En otras secciones de la consola web: dashboard, al programar o generar un informe

Equipos

Todos los dispositivos del cliente que se agregaron a ESET PROTECT On-Prem se visualizan aquí y se dividen en grupos. Cada dispositivo está asignado a un único grupo estático. Al hacer clic en un grupo de la lista (a la izquierda) se visualizarán los miembros (clientes) de este grupo en el panel derecho.

Los equipos **no administrados** (clientes de la red que no tienen instalado ESET Management Agent) por lo general aparecen en el grupo de **Perdidos y encontrados**. El estado de un cliente que se muestra en la consola web ESET PROTECT es independiente de la configuración de los productos de seguridad de ESET en el cliente. Es por eso que incluso si un cierto estado no se muestra en el cliente, aún se informa a la consola web ESET PROTECT. Puede arrastrar y soltar los clientes para moverlos entre los grupos.

Haga clic en el botón **Agregar dispositivo** y seleccione lo siguiente:

- **Equipos**: puede agregar equipos al grupo estático seleccionado.
- **Dispositivos móviles**: puede agregar dispositivos móviles al grupo estático seleccionado.
- **Sincronizar a través del servidor de directorio**: puede ejecutar la tarea Sincronización de grupos estáticos.

Haga clic en en un dispositivo para abrir un nuevo menú con acciones disponible para ese dispositivo. También puede seleccionar la casilla de verificación junto a un dispositivo y hacer clic en el botón **Equipo** en la barra

inferior. El menú **Equipo** mostrará diferentes opciones según el tipo de dispositivo. Consulte la Leyenda del icono para obtener información sobre los diferentes tipos y estados de iconos. Haga clic en el número de alertas en la columna **Alertas** para ver la lista de alertas en la sección Detalles del equipo.

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

- Amarillo (error): hace de 2 a 14 días que el equipo no se conecta.
- Rojo (advertencia): hace más de 14 días que no se conecta el equipo.

El ícono **Inspect** abre la sección Equipos de la consola web de ESET Inspect On-Prem. El ESET Inspect On-Prem solo está disponible cuando tiene una licencia de ESET Inspect On-Prem y ESET Inspect On-Prem está conectado a ESET PROTECT On-Prem. Un usuario de la consola web necesita permiso de **Lectura** o superior para **Acceder a ESET Inspect** o permiso de **Lectura** o superior para el usuario **ESET Inspect**.

Filtrar la vista

Hay diferentes formas de filtrar su vista:

- Filtro estándar: Para agregar criterios de filtrado, haga clic en **Agregar filtro** y seleccione los elementos de la lista. Escriba las cadenas de búsqueda o seleccione los elementos del menú desplegable en los campos de filtrado y pulse **Intro**. Los filtros activos están resaltados en azul.

- Puede filtrar por gravedad con los íconos de estado: rojo - **Errores**, amarillo - **Advertencias**, verde - **Aceptado** y gris - Equipos **no administrados**. El ícono de gravedad representa el estado actual del producto de ESET en un equipo cliente en particular. Puede usar una combinación de estos íconos al activarlos o desactivarlos. Por ejemplo, para ver solamente los equipos con advertencias, deje solo el icono amarillo seleccionado (se debe eliminar la selección del resto de los iconos). Para ver tanto las advertencias como los errores, deje solo estos dos iconos activados.

- Haga clic en **Agregar filtro > Categoría de producto** y, con el menú desplegable, puede elegir los tipos de dispositivos a mostrar.

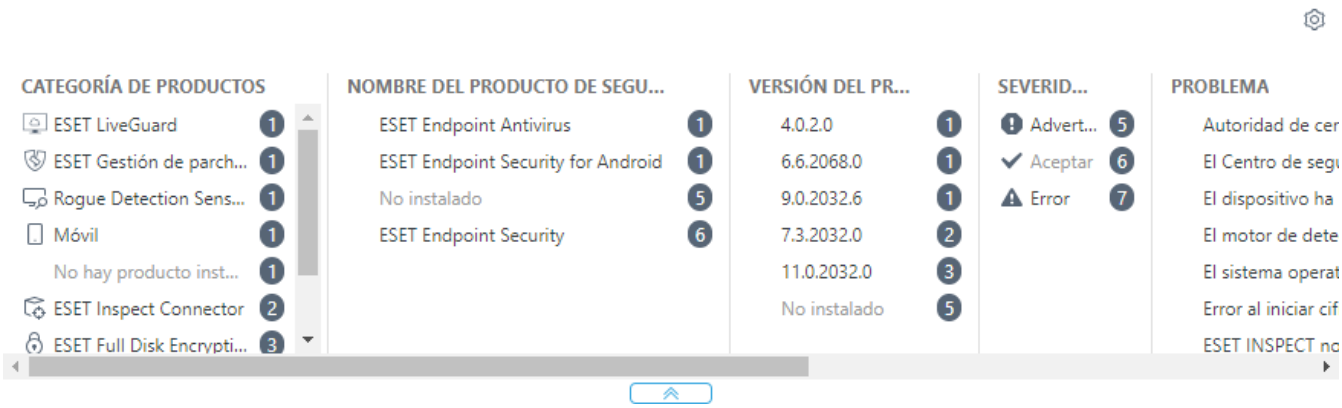
  - **ESET Protected**, protegido por un producto ESET, escritorio, móvil, servidor, servidor de correo, servidor de puerta de enlace, servidor de colaboración, servidor de archivos.

  - **ESET PROTECT On-Prem**, componentes individuales de ESET PROTECT, agente de ESET Management, Rogue Detection Sensor, servidor de ESET PROTECT.

  - **Otro**: ESET LiveGuard, conector de ESET Inspect, servidor de ESET Inspect, ESET Full Disk Encryption, ESET Bridge, dispositivo de seguridad virtual, Shared Local Cache.

- Casilla de verificación de **Mostrar subgrupos**: muestra los subgrupos del grupo actualmente seleccionado.

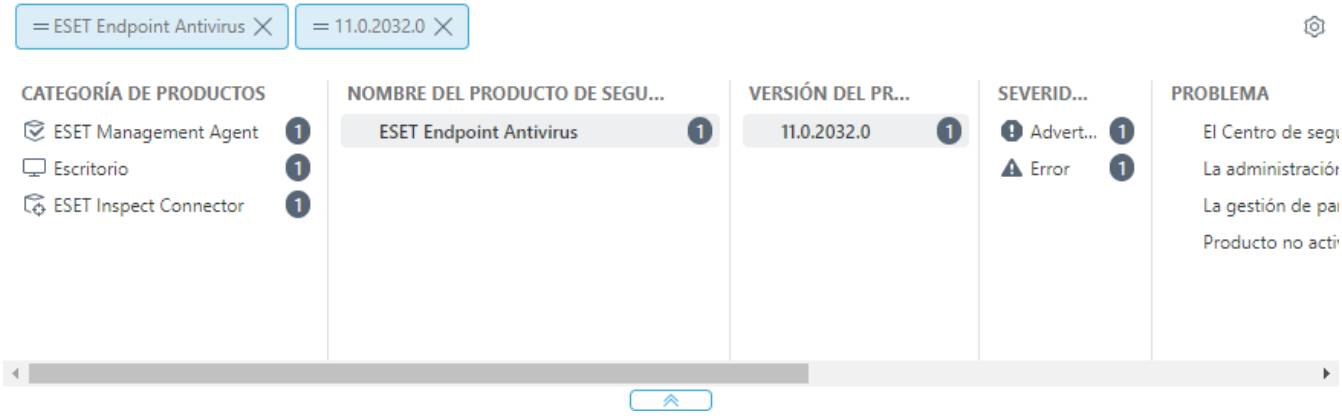
- Puede ver los **Filtros avanzados** como un panel de filtros ampliable en la pantalla **Equipos**.



Los filtros avanzados muestran una vista previa en tiempo real de los valores de varios filtros y el número exacto de resultados de su selección.

Al filtrar grandes conjuntos de equipos, los filtros avanzados muestran qué valores de filtro devolverán un número administrable de resultados, lo que le permitirá encontrar los dispositivos adecuados mucho más rápido.

Haga clic en los elementos de las columnas para aplicar el filtro. Los filtros aplicados aparecen en la parte superior de los filtros avanzados como burbujas azules. Haga clic en el filtro aplicado para cambiar el filtrado por el valor **equivalente** o **no equivalente**.



Haga clic en el ícono del engranaje de una columna para ordenar los valores de la columna o haga clic en el ícono del engranaje situado en la parte superior de los filtros avanzados. Utilice el asistente para ajustar (agregar, quitar, reordenar) las columnas exhibidas. También puede arrastrar y soltar para ajustar las columnas. Haga clic en **Restablecer** para restablecer las columnas de la tabla a su estado predeterminado (las columnas disponibles predeterminadas en el orden predeterminado).

> Solo puede utilizar filtros avanzados con grupos estáticos. Los grupos dinámicos no son compatibles con filtros avanzados.

- Use Grupos dinámicos o Informes para obtener un filtrado más avanzado.

- Para encontrar los equipos marcados como Maestro para clonación, haga clic en **Agregar filtro** > seleccione **Maestro para clonación** > seleccione la casilla de verificación ubicada junto al filtro **Maestro para clonación**.

Personalización del diseño y de los filtros

Puede personalizar la vista de la pantalla de la consola web actual:

- Administre el panel lateral y la tabla principal.
- Agregar filtro y filtros preestablecidos. Puede usar etiquetas para filtrar los elementos mostrados.

> Si no puede encontrar un equipo en particular en la lista y sabe que está en su infraestructura de ESET PROTECT, asegúrese de que todos los filtros se encuentren desactivados.

Detalles del equipo

Para más información sobre un equipo, seleccione un equipo cliente en un grupo estático o dinámico y haga clic en **Detalles**, o bien, en el nombre del equipo para mostrar el panel lateral Vista previa del equipo a la derecha.

El ícono **Inspect** abre la sección Equipos de la consola web de ESET Inspect On-Prem. El ESET Inspect On-Prem solo está disponible cuando tiene una licencia de ESET Inspect On-Prem y ESET Inspect On-Prem está conectado a ESET PROTECT On-Prem. Un usuario de la consola web necesita permiso de **Lectura** o superior para **Acceder a ESET Inspect** o permiso de **Lectura** o superior para el usuario **ESET Inspect**.

La ventana de información consta de las siguientes partes:

Vista general:

Equipo

- Haga clic en el ícono de edición para cambiar el nombre o la descripción del equipo. Puede seleccionar **Permitir nombre duplicado** si ya existe otro equipo administrado con el mismo nombre.
- Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
- **FQDN**: nombre de dominio completamente calificado del equipo

> Si tiene sus equipos cliente y el servidor de ESET PROTECT ejecutándose bajo Active Directory, puede llenar automáticamente los campos **Nombre** y **Descripción** usando la tarea Sincronización del Grupo Estático.

- **Grupo principal**: puede cambiar el grupo principal estático del equipo.
- **IP**: la dirección IP de la máquina.
- **Recuento de políticas aplicadas**: Haga clic en el número para ver la lista de políticas aplicadas.
- **Miembro de Grupos Dinámicos**: La lista de grupos dinámicos en la que el equipo cliente estaba presente durante la última replicación.

Hardware

Este mosaico contiene una lista de los parámetros de hardware clave, información sobre el sistema operativo y los identificadores únicos. Haga clic en la vista de mosaico para ver la pestaña de **Detalles - Hardware**. Consulte también el inventario de hardware.

Alertas

- **Alertas**: enlace a la lista de problemas con el equipo actual.

- **Recuentos de detecciones sin resolver**: recuento de detecciones no resueltas. Haga clic en el recuento para ver la lista de detecciones sin resolver.

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

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

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

- **Última hora de inicio**: fecha y hora del último inicio del dispositivo administrado. El equipo administrado debe ejecutar el agente ESET Management 10.0 y posterior para ver la **Última hora de arranque**. Una versión de agente anterior informa **n/a**.

- **Última hora de la exploración**: información sobre la hora de la última exploración.

- **Motor de detección**: Versión del motor de detección en el dispositivo de destino.

- **Actualizado**: El estado de la actualización.

Productos y Licencias

Lista de componentes de ESET instalados en el equipo. Haga clic en la vista de mosaico para ver la pestaña de **Detalles - Producto y Licencias**.

Cifrado

La ventana de cifrado solo es visible en estaciones de trabajo compatibles con ESET Full Disk Encryption.

- Haga clic en **Cifrar equipo** para iniciar el asistente para Habilitar cifrado.

- Cuando el cifrado está activo, haga clic en **Administrar** para administrar las opciones de cifrado.

- Si el usuario no puede iniciar sesión con su contraseña o no se puede acceder a los datos cifrados de la estación de trabajo debido a un problema técnico, el administrador puede iniciar el proceso de recuperación de cifrado.

ESET LiveGuard Advanced

En el mosaico se proporciona información básica sobre el servicio. Puede tener dos estados de mosaico:

- Blanco: estado predeterminado. Una vez que ESET LiveGuard Advanced se activa y queda funcionando, el mosaico se mantiene en estado blanco.

- Amarillo: si hay un problema con el servicio de ESET LiveGuard Advanced, la ventana se vuelve amarilla y muestra información sobre el problema.

Necesita la licencia ESET LiveGuard Advanced para activar ESET LiveGuard Advanced.

Acciones disponibles:

- **Habilitar**: haga clic en **Habiltar** para configurar la tarea de activación y la política para el producto de ESET LiveGuard Advanced en la máquina actual. Como alternativa, haga clic en un equipo o en el ícono del engranaje junto a un grupo estático y seleccione **Soluciones** > **Habilitar ESET LiveGuard.** En la ventana de configuración, seleccione el nivel de protección y haga clic en **Habilitar ESET LiveGuard**:
  - **Protección óptima (recomendado):** los archivos en riesgo, incluidos los tipos de documentos que admiten macros, se enviarán a un servidor seguro ESET para la exploración automatizada y el análisis del comportamiento. El acceso a los archivos está limitado hasta que estos hayan sido evaluados como seguros.
  - **Protección básica**: ESET LiveGuard Advanced explorará un conjunto limitado de archivos.
- Archivos enviados: lista de todos los archivos enviados a los servidores de ESET.

Después de habilitar ESET LiveGuard Advanced:

- El dashboard ESET LiveGuard mostrará los informes mejorados de su red administrada ESET LiveGuard Advanced.
- Cada dispositivo tendrá habilitado el Sistema de reputación ESET LiveGuard Advanced de ESET LiveGrid® y el Sistema de comentarios de ESET LiveGrid®. Consulte las políticas de su dispositivo.

Usuarios

- **Usuarios registrados** (únicamente equipos): dominio y nombre de usuario de los usuarios registrados en el dispositivo.
- **Usuarios asignados**
  - Haga clic en **Agregar usuario** para asignar un usuario desde Usuarios del equipo a este dispositivo.

    Un equipo solo puede asignarse a 200 usuarios como máximo en una operación.
  - Haga clic en el ícono de la papelera para desasignar un usuario actual.
  - Haga clic en el nombre del usuario asignado para mostrar los detalles de su cuenta.

Ubicación

La ventana está disponible solo para dispositivos móviles. Solo puede localizar dispositivos en la Apple Business Manager (ABM) de iOS cuando está activado el Modo extraviado.

Virtualización

El mosaico aparece después de marcar el equipo como Maestro para clonación y muestra la configuración de IEV. Haga clic en el ícono de engranaje para cambiar la configuración de IEV.

En la parte inferior, están disponibles los siguientes botones:

- Haga clic en el botón **Aislamiento de red** para ejecutar tareas de cliente de aislamiento de red en el equipo:
  - o Aislar de la red
  - o Finalizar aislamiento de la red
- El botón de **Virtualización** se usa para configurar el equipo para clonación. Es necesario cuando los equipos son clonados o se cambia el hardware.
  - oMarcar como maestro para clonar
  - o**Deshabilitar detección de hardware**: Si se deshabilita la detección de hardware, el cambio es permanente. ¡Esta acción es irreversible!
  - o**Desmarcar como Maestro para clonación**: Quita la marca de maestro. Después de aplicar esto, cada nueva clonación de la máquina da lugar a una pregunta.

> La detección de huella digital de equipos no es compatible con:
> - Linux, macOS, Android, iOS
> - equipo sin ESET Management Agente

Configuración:

Pestaña **Configuración**: contiene una lista de las configuraciones instaladas de los productos ESET (Agente de ESET Management, endpoint de ESET, etc.). Las opciones disponibles son:

- Hacer clic en el botón **Solicitar configuración** para crear una tarea para que el Agente de ESET Management recopile todas las configuraciones de productos administrados. Después de entregar la tarea al Agente de ESET Management, se ejecuta inmediatamente y los resultados se entregan al Servidor de ESET PROTECT en la siguiente conexión. Esto le permite ver la lista de todas las configuraciones de los productos administrados.
- Abra una configuración desde el menú contextual y conviértala en una política. Haga clic en una configuración para verla en el visor.
- Una vez abierta la configuración, puede convertirla en una política. Haga clic en **Convertir a política**, la configuración actual se transferirá al asistente de políticas y puede modificar y guardar la configuración como una nueva política.
- Descargue la configuración para fines de diagnóstico y soporte. Haga clic en la configuración seleccionada y luego en **Descargar para diagnóstico** en el menú desplegable.

Pestaña de **Políticas aplicadas**: Lista de políticas aplicadas al dispositivo. Si ha aplicado una política para un producto de ESET o una característica de un producto de ESET que no están instalados en el equipo, la política se muestra atenuada en la lista.

Puede ver las políticas asignadas al dispositivo seleccionado, así como las políticas aplicadas a los grupos que contienen el dispositivo.
Hay un icono de bloqueo junto a políticas bloqueadas (no editables): políticas integradas específicas (por ejemplo, la política de actualización automática o las políticas de ESET LiveGuard) o políticas en las que el usuario tiene el permiso de **Lectura**, pero no de **Escritura**.

Haga clic en **Administrar directivas** para administrar, editar, asignar o eliminar una política. Las políticas se aplican en función del orden (columna **Orden de las políticas**). Para cambiar la prioridad de la aplicación de políticas, seleccione la casilla de verificación junto a una política y haga clic en el botón **Aplicar antes** o **Aplicar más tarde**.

Ficha **Exclusiones aplicadas**: lista de exclusiones aplicadas al dispositivo.

Registros (solo equipos)

- **SysInspector**: Haga clic en **Solicitar registro (solo en Windows)** para ejecutar la tarea de solicitud de registro SysInspector para los clientes seleccionados. Una vez completada la tarea, se muestra una nueva entrada en la lista de registros de ESET SysInspector. Haga clic en un registro de la lista para explorarlo.

- **Recopilador de registros**: Haga clic en **Ejecutar recopilador de registros** para ejecutar la Tarea de recopilador de registros. Después de completar la tarea, se añade una nueva entrada en la lista de registros. Haga clic en un registro de la lista para descargarlo.
- **Registros de diagnóstico**: - Haga clic en **Diagnósticos** > **Encender** para iniciar el modo Diagnósticos en la máquina actual. El modo de diagnóstico obligará al cliente a enviar todos los registros al servidor de ESET PROTECT. Puede examinar todos los registros en 24 horas. Los registros se clasifican en cinco categorías: **Registro de spam**, **Registro de firewall**, **Registro de HIPS**, **Registro de de dispositivo de control** y **Registro de control Web**. Haga clic en **Diagnóstico** > **Reenviar todos los registros** para reenviar todos los registros del agente en la siguiente replicación. Haga clic en **Diagnóstico** > **Apagar** para detener el modo Diagnóstico.

El límite de tamaño de archivo para la entrega de registros por dispositivo es de 200 MB. Puede acceder a los registros desde la consola web en la sección **Detalles** > **Registros**. Si los registros recopilados por la tarea son mayores que 200 MB, se producirá un error en la tarea. Si la tarea falla, usted puede:
- Recopilar los registros localmente en el dispositivo.
- Cambiar el nivel de detalle de los registros y repetir la tarea:
  - En el caso de los objetivos de Windows, use el parámetro `/Targets:EraAgLogs` para recopilar solo los registros del agente ESET Management.
  - En el caso de los objetivos de Linux/macOS, use el parámetro `--no-productlogs` para excluir registros del producto de seguridad ESET instalado.

Ejecuciones de la tarea

Una lista de tareas ejecutadas. Puede filtrar la vista para limitar los resultados, ver los detalles de las tareas, editar, duplicar, quitar, ejecutar o volver a ejecutar la tarea.

Aplicaciones instaladas:

Muestra una lista de los programas instalados en un cliente con detalles como versión, tamaño, estado de seguridad, etc. Puede activar los informes de aplicaciones de terceros (que no son de ESET) a través de la configuración de la política del agente.

Si administra dispositivos Android y ha aplicado una política para permitir las excepciones de la aplicación (**Control de aplicaciones** > **Habilitar control de aplicaciones** > **Habilitar bloqueo** > **Excepciones**):

- Administración de dispositivos móviles local (ESET PROTECT On-Prem): las aplicaciones de la lista están resaltadas y tienen el estado de seguridad **Permitido por excepción**.

- Administración de dispositivos móviles en la nube (ESET PROTECT): las aplicaciones de la lista no están resaltadas y no tienen ningún estado de seguridad.

Seleccione una aplicación y haga clic en **Desinstalar** para quitarla.

- Se le solicitará que ingrese los **Parámetros de desinstalación**. Son parámetros de línea de comando opciones para el instalador (paquete de instalación). Los parámetros de desinstalación son únicos para cada instalador de software. Puede encontrar más información en la documentación para el producto específico.

- Marque la casilla al lado de **Reiniciar automáticamente cuando sea necesario** si desea que el equipo cliente se reinicie automáticamente luego de la instalación. De manera alternativa, puede dejar esta opción sin seleccionar y el equipo cliente se puede reiniciar manualmente. Puede configurar el comportamiento de reinicio o apagado de los equipos administrados. El equipo debe ejecutar el Agente de ESET Management 9.1 y versiones posteriores, además de un producto de seguridad de ESET compatible con esta configuración.

Cuando desinstala el agente ESET Management del equipo del cliente, el dispositivo ya no es administrado por ESET PROTECT On-Prem:
- El producto de seguridad de ESET puede conservar algunas configuraciones después de desinstalar el agente ESET Management.
- Si el agente ESET Management está protegido por contraseña, debe proporcionar la contraseña para desinstalar, reparar o actualizar (con cambios). 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.

Si hay una actualización del producto ESET disponible, puede actualizar el producto ESET haciendo clic en el botón **Actualización de productos ESET**.

- ESET PROTECT On-Prem admite la actualización automática de agentes ESET Management en equipos administrados.
- Los dispositivos iOS informan la lista de software instalado en ESET PROTECT On-Prem una vez por día. El usuario no puede forzar la actualización de la lista.

Alertas

Muestra una lista de alertas y los detalles: Problema, Estado, Producto, Ocurrencia, Gravedad, etc. Es posible acceder a esta lista directamente desde la sección **Equipos**, haciendo clic en el recuento de la columna **Alertas**. Puede administrar las alertas a través de acciones de un clic.

Preguntas (solo equipos)

La lista de preguntas relacionadas con la clonación está en la pestaña **Preguntas**. Lea más sobre la resolución de problemas para equipos cambiados o clonados.

Detecciones y cuarentena

- **Detecciones**: se muestran todos los tipos de detección, pero puede filtrarlas por: **Categoría de detección**: **antivirus**, archivos bloqueados, ESET Inspect, **firewall**, **HIPS** y **protección web**.
- **Cuarentena**: puede ver una lista de las detecciones en cuarentena con detalles tales como Nombre de la detección, Tipo de detección, Nombre del objeto, Tamaño, Primera ocurrencia, Recuento, Motivo del usuario, etc.
- **Archivos enviados**: una lista de todos los archivos enviados a los servidores de ESET.

Detalles

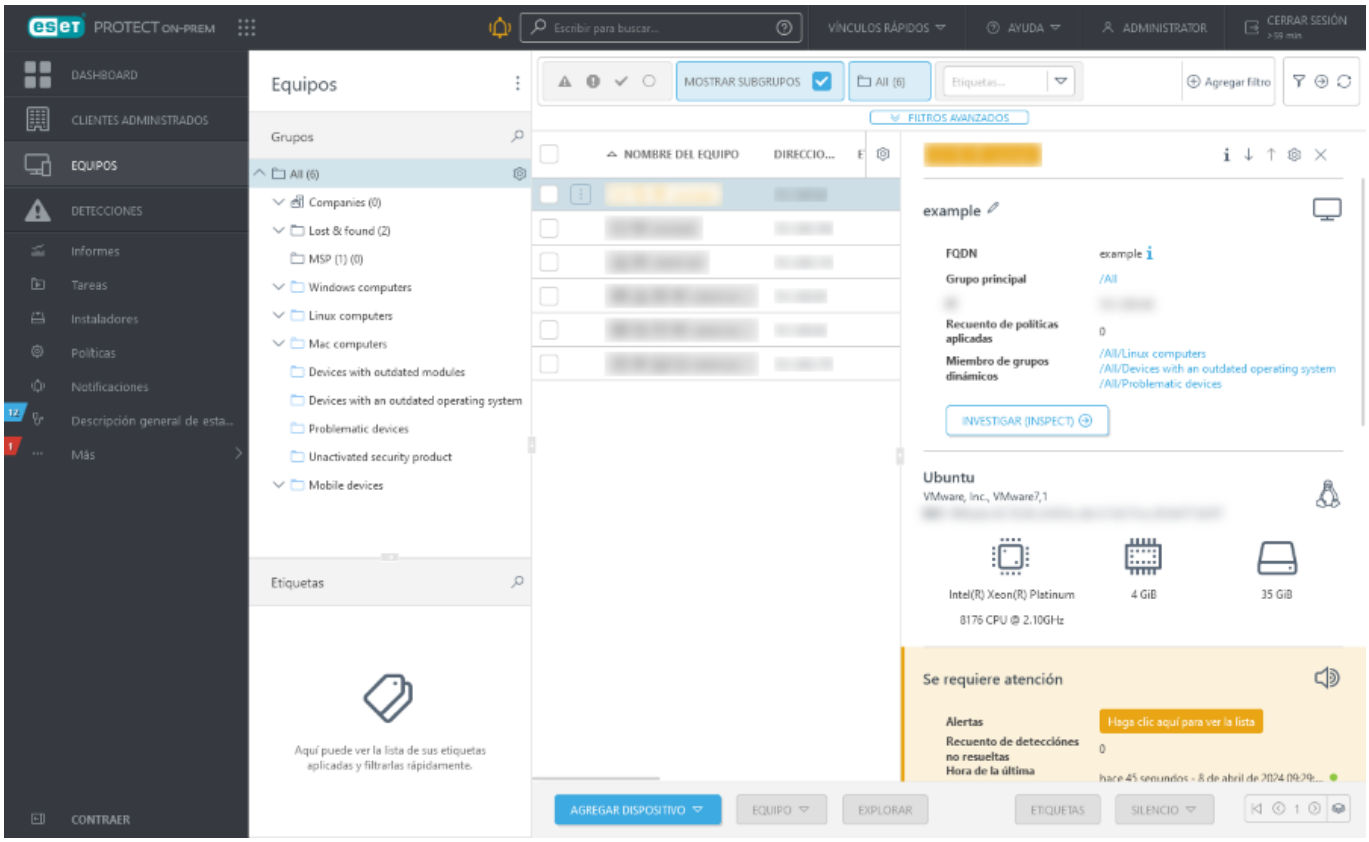
- **Básico**: información acerca del dispositivo: Nombre del sistema operativo, Tipo, Versión, Número de serie, Nombre FQDN, etc. En esta sección, también se incluye información sobre si el dispositivo está silenciado, cómo se administra, cuándo se actualizó por última vez y la cantidad de políticas aplicadas.
- **Hardware**: información acerca del hardware, el fabricante y el modelo del equipo, la CPU, la memoria RAM, el almacenamiento (incluida la capacidad y el espacio libre), los periféricos e información de la red (IPv4, IPV6, subred, adaptador de red...). Consulte también el inventario de hardware.
- **Producto y Licencias**: Versión del motor de detección actual, versiones de los Productos de Seguridad de ESET instalados, licencias en uso.
- **Cifrado:** si utiliza ESET Full Disk Encryption, consulte la descripción general del estado del cifrado del disco.

Vista previa del equipo

En **Equipos**, haga clic en el nombre de un equipo para ver el panel lateral de vista previa del equipo a la derecha. El panel lateral de vista previa del equipo contiene la información más importante sobre el equipo seleccionado.

Manipulación de la vista previa del equipo:

- **Mostrar detalles:** abre el menú Detalles del equipo
- **Siguiente**: muestra el siguiente dispositivo en el panel lateral de vista previa del equipo.
- **Anterior**: muestra el dispositivo anterior en el panel lateral de vista previa del equipo.
- **Administrar el contenido de los detalles del equipo**: puede gestionar qué secciones del panel lateral de vista previa del equipose muestran y en qué orden.
- **Cerrar**: cierra el panel lateral de vista previa del equipo.



Eliminar equipo de administración

Para quitar un dispositivo de la administración, haga clic en **Equipos**, seleccione un dispositivo > y haga clic en **Administrar** > **Quitar**. Un cuadro de diálogo mostrará los pasos necesarios para eliminar el equipo seleccionado de la administración.

Cuando pase al siguiente paso, asegúrese de haber completado el paso anterior con éxito. Esto es esencial para que el dispositivo se elimine de manera correcta.

1. **Restablecer configuración de punto final**: haga clic en **Administrar políticas** y elimine todas las políticas aplicadas para permitir la administración del dispositivo local. Consulte las **Reglas de eliminación de políticas** en la sección **Políticas**. Si se configura una contraseña para acceder a la configuración del producto de punto de conexión, cree una nueva política para eliminar la contraseña (seleccione configurar una contraseña, pero no ingrese ninguna). Para equipos cifrados con ESET Full Disk Encryption, siga los pasos de descifrado.

2. **Detener administración del equipo**: ejecute una tarea Detener administración o desinstale el agente ESET Management o el producto de seguridad de ESET localmente en un equipo. Esto suspende la conexión entre el equipo y ESET PROTECT On-Prem.

3. **Eliminar equipo de la base de datos**: luego de asegurarse de que el equipo ya no esté conectado a ESET PROTECT On-Prem, puede eliminarlo de la lista de equipos administrados.

Seleccione la casilla de verificación **Quiero desactivar los productos ESET instalados** para quitar la licencia de todos los productos ESET instalados en el equipo seleccionado. Consulte también Desactivación de los productos comerciales ESET.

Grupos

Se puede pensar en los grupos como carpetas donde los equipos y otros objetos se categorizan.

Para equipos y dispositivos, puede usar los grupos predefinidos y las plantillas de grupos, o crear nuevos. Los equipos del cliente se pueden agregar a grupos. Esto le ayuda a mantener los equipos estructurados y ordenados a su gusto. Puede agregar un equipo a un grupo estático.

Los grupos estáticos se administran de forma manual, mientras que los grupos dinámicos se ordenan de forma automática en función de los criterios específicos que se encuentran en una plantilla. Una vez que los equipos están agrupados, puede asignar políticas, tareas o configuraciones a estos grupos. La política, tarea o configuración se aplica a todos los miembros del grupo. Hay dos tipos de grupos cliente:

Grupos estáticos

Los Grupos estáticos son grupos de equipos de clientes seleccionados y otros objetos. Los miembros del grupo son estáticos y solo pueden agregarse o eliminarse de forma manual, no en función de criterios dinámicos. Un objeto puede pertenecer a un solo Grupo estático. Un grupo estático solo se puede eliminar si no contiene objetos.

Grupos dinámicos

Los Grupos dinámicos son grupos de dispositivos (no de otros objetos, como tareas o políticas) que han pasado a ser miembros del grupo por cumplir con determinados criterios. Si un dispositivo cliente no cumple estos criterios, será eliminado del grupo. Los equipos que cumplen con los criterios se agregarán al grupo de forma automática (de ahí el nombre “dinámico”).

Haga clic en el ícono del engranaje  , ubicado junto al nombre del grupo, para ver las acciones de grupo y los detalles del grupo disponibles.

Los equipos que son miembros del grupo se mencionan en el panel de la derecha.

Acciones de grupo

Vaya a **Equipos** y seleccione el grupo que desea administrar. Haga clic en el ícono  junto al nombre del grupo y seleccione Mover. Se mostrará un menú con las siguientes opciones:

Acción de grupo	Descripción de acciones de grupo	Grupos estáticos	Grupos dinámicos
Mostrar detalles	Proporciona un resumen general del grupo seleccionado.	✔	✔
Registro de auditoría	Ver el registro de auditoría del elemento seleccionado.	✔	✔
Nuevo grupo estático	El grupo seleccionado será el grupo principal predeterminado, pero puede cambiarlo más adelante cuando cree un grupo estático nuevo.	✔	X
Nuevo grupo dinámico	El grupo seleccionado será el grupo principal predeterminado, pero puede cambiarlo más adelante cuando cree un grupo dinámico nuevo.	✔	✔
Notificación nueva	Crea una nuevo certificado.	X	✔
Agregar nuevo	Agrega un nuevo dispositivo.	✔	X

Acción de grupo	Descripción de acciones de grupo	Grupos estáticos	Grupos dinámicos
Tareas	Seleccione tareas de cliente que se deben ejecutar en los dispositivos de este grupo: **Explorar**: ejecuta la tarea Exploración a pedido en todos los clientes del grupo seleccionado. **Actualización**: • **Actualizar módulos**: ejecuta la tarea Actualización de módulos (se desencadena la actualización en forma manual). • **Actualizar productos ESET**: ejecuta la tarea Instalación del software en equipos con productos de seguridad ESET obsoletos. • **Actualizar sistema operativo**: ejecuta la tarea Actualización del sistema operativo en equipos del grupo seleccionado. **Móvil**: consulte la sección Acciones Anti-Theft para obtener más información. • **Volver a inscribirse**: vuelva a inscribir un dispositivo móvil. • **Buscar**: solicita las coordenadas GPS de su dispositivo móvil. • **Bloquear**: el dispositivo se bloqueará o se marcará como perdido cuando se detecte actividad sospechosa. • **Desbloquear**: el dispositivo se desbloqueará. • **Borrar código de acceso**: quita el código de acceso de un dispositivo iOS/iPadOS. • **Sirena/modo extraviado**: desencadena una sirena muy fuerte en forma remota; la sirena se iniciará incluso si su dispositivo está silenciado. • **Restablecimiento de fábrica**: todos los datos almacenados en su dispositivo se borrarán de forma permanente. **Ejecutar tarea**: seleccione una o más tareas de cliente y ejecútelas en el dispositivo seleccionado. **Nueva tarea**: cree una nueva tarea de cliente. Seleccione una tarea y configure el límite (opcional) para esta tarea. La tarea se pondrá en cola de acuerdo con la configuración de tareas. Esta opción desencadena de inmediato una tarea existente, que se selecciona de una lista de tareas disponibles. El desencadenador no está disponible para esta tarea, ya que la misma se ejecutará de inmediato. **Tareas recientes**: lista de las Tareas de clientes recientes de todos los grupos y equipos.	✔	✔
Soluciones	**Habilitar ESET Inspect On-Prem**: haga clic en junto a un grupo estático y seleccione **Soluciones** > **Habilitar ESET Inspect On-Prem** para activar y habilitar ESET Inspect On-Prem en el ordenador. **Habilitar ESET LiveGuard** –Haga clic en un equipo ícono del engranaje junto a un grupo estático y seleccione **Soluciones** > **Habilitar ESET LiveGuard** para activar y habilitar el ESET LiveGuard Advanced. **Habilitar la Gestión de parches y vulnerabilidades**: haga clic en junto a un grupo estático y seleccione **Soluciones** > **Habilitar Gestión de parches y vulnerabilidades** para habilitar la Gestión de parches y vulnerabilidades en el equipo.	✔	x
Informes	Seleccione y ejecute un informe a partir del grupo seleccionado.	✔	x
Administrar políticas	Administrar políticas asignadas al grupo seleccionado.	✔	✔
Editar	Le permite editar el grupo seleccionado. Se aplica la misma configuración que cuando crea un grupo nuevo (estático o dinámico).	✔	✔
Mover:	Selecciona un grupo y lo mueve como un subgrupo de otro grupo.	✔	✔
Eliminar	Quita el grupo seleccionado.	✔	✔
Aplicar antes **Aplicar más tarde**	Cambia el nivel de prioridad de un grupo dinámico.	x	✔
Importar	Importa una lista (por lo general, un archivo de texto) de equipos, como miembros del grupo seleccionado. Si los equipos ya existen como miembros de este grupo, el conflicto se resolverá en función de la acción seleccionada:	✔	x
Exportar	Exporta los miembros del grupo (y subgrupos, si se seleccionan) en una lista (archivo *.txt*). Esta lista puede usarse para revisión o podrá importarse más adelante.	✔	x

Detalles del grupo

Cuando elije la acción de grupo **Mostrar detalles**, puede ver la información general del grupo seleccionado:

Vista general:

En **Información general**, puede editar la configuración del grupo al hacer clic en o **Agregar descripción**. Puede ver la información sobre la ubicación del grupo y su **Grupo principal** y los **Grupos secundarios**. Si el grupo seleccionado es un Grupo dinámico, también puede ver la operación y las reglas en función de las cuales se evalúan y asignan los equipos al grupo.

Tareas

Puede ver y editar las tareas de clientes asignadas al grupo.

Políticas

Puede asignar una política existente al grupo o crear una política nueva. Puede ver y editar las políticas asignadas al grupo.

> Puede ver solamente las políticas asignadas al grupo seleccionado. No puede ver las políticas aplicadas a equipos individuales en el grupo.

Las políticas se aplican en función del orden (columna **Orden de las políticas**). Para cambiar la prioridad de la aplicación de políticas, seleccione la casilla de verificación junto a una política y haga clic en el botón **Aplicar antes** o **Aplicar más tarde**.

Alertas

El listado de alertas de equipos en el grupo. Puede administrar las alertas a través de acciones de un clic.

Exclusión

Lista de exclusiones aplicadas al grupo.

Grupos estáticos

Los grupos estáticos se utilizan para:

- Organizar dispositivos y crear jerarquías de grupos y subgrupos
- Organizar objetos
- Ser grupos hogar para los usuarios

Grupo de pertenencia: el grupo de pertenencia se detecta automáticamente según el conjunto de permisos asignado del usuario activo en ese momento.

> Situación de ejemplo:
> La cuenta de usuario activa actualmente tiene el derecho de acceso de **Escritura** para la **tarea del cliente Instalación del software** y el **grupo de pertenencia** de la cuenta de usuario es "Department_1". Cuando el usuario cree una nueva **tarea del cliente Instalación del software**, se seleccionará automáticamente "Department_1" como **grupo de pertenencia** de la tarea del cliente.

Si el grupo de pertenencia seleccionado previamente no cumple con sus expectativas, podrá seleccionar el grupo de pertenencia de forma manual.

Los Grupos estáticos solo pueden crearse de forma manual. Los dispositivos se pueden mover manualmente a los grupos. Cada equipo o dispositivo móvil puede pertenecer a un Grupo estático únicamente. La administración de grupos estáticos está disponible mediante las acciones de grupos.

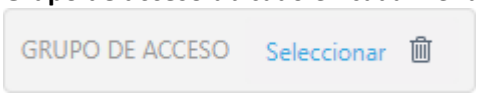
Hay dos Grupos estáticos predeterminados:

- **Todos**: este es un grupo principal para todos los dispositivos de la red del servidor de ESET PROTECT. Todos los objetos creados por el administrador (por defecto) están dentro de este grupo. Siempre se muestra y no se le puede cambiar el nombre. El acceso a este grupo le da acceso a los usuarios a todos los subgrupos; por lo que debe distribuirse con cuidado.
- **Perdidos y encontrados**: un grupo secundario del grupo **Todos**. Cada nuevo equipo que se conecta al servidor ESET PROTECT por primera vez se muestra, automáticamente, en este grupo. El grupo se puede volver a nombrar o copiar, pero no se puede eliminar o mover.

Para mover un equipo a otro grupo estático, haga clic en el equipo > seleccione **Administrar** > **Mover a grupo** > seleccione el grupo estático de destino y haga clic en **Aceptar**.

Se puede eliminar un grupo dinámico solo si:
- El usuario tiene permisos de escritura sobre el grupo
- El grupo está vacío

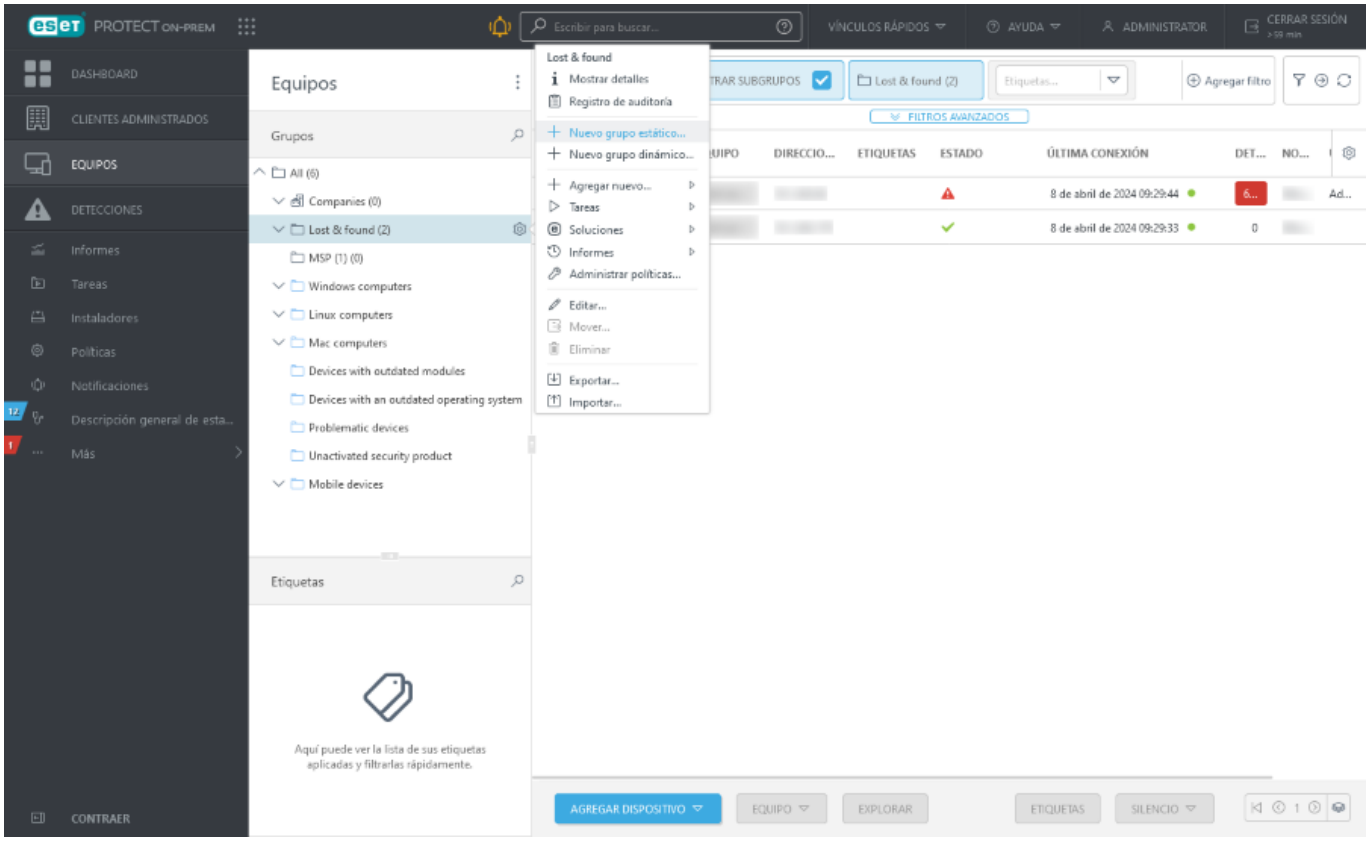
Si todavía hay objetos en el grupo estático, la operación de eliminación fallará. Hay un botón de filtro de **Grupo de acceso** ubicado en cada menú (por ejemplo, **Instaladores**) con objetos.



Haga clic en **Seleccionar** para elegir un grupo estático; se mostrarán solo los objetos dentro de este grupo. Con esta vista filtrada, el usuario puede manipular fácilmente los objetos de un grupo.

Cree un Nuevo grupo estático

Para crear un nuevo grupo estático, haga clic en **Equipos**, seleccione el ícono de engranaje junto a un grupo estático y seleccione **Grupo estático nuevo**.



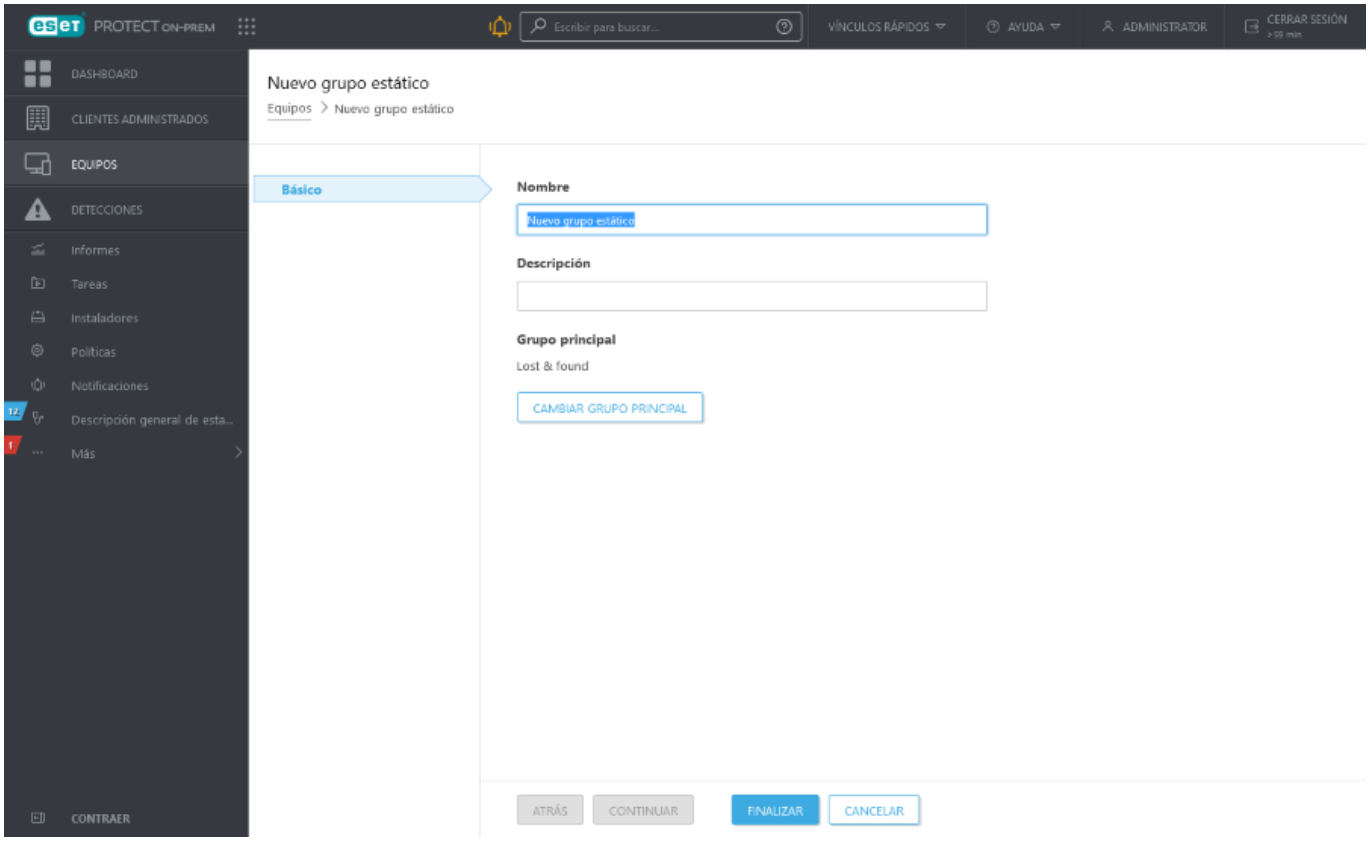
Básica

Ingrese un **Nombre** y una **Descripción** para el grupo nuevo.

- De manera opcional, puede cambiar el **Grupo principal**. En forma predeterminada, el grupo principal es el grupo que seleccionó cuando comenzó a crear el grupo estático nuevo. Si desea cambiar el grupo principal, haga clic en **Cambiar grupo principal** y seleccione un grupo principal del árbol.

- El grupo principal del nuevo grupo estático debe ser un grupo estático. No es posible que se incluya un grupo estático en un grupo estático.

Haga clic en **Finalizar** para crear el Grupo estático nuevo.



Importar clientes desde Active Directory

Para importar clientes de AD, cree una nueva tarea del servidor: Sincronización de grupos estáticos.

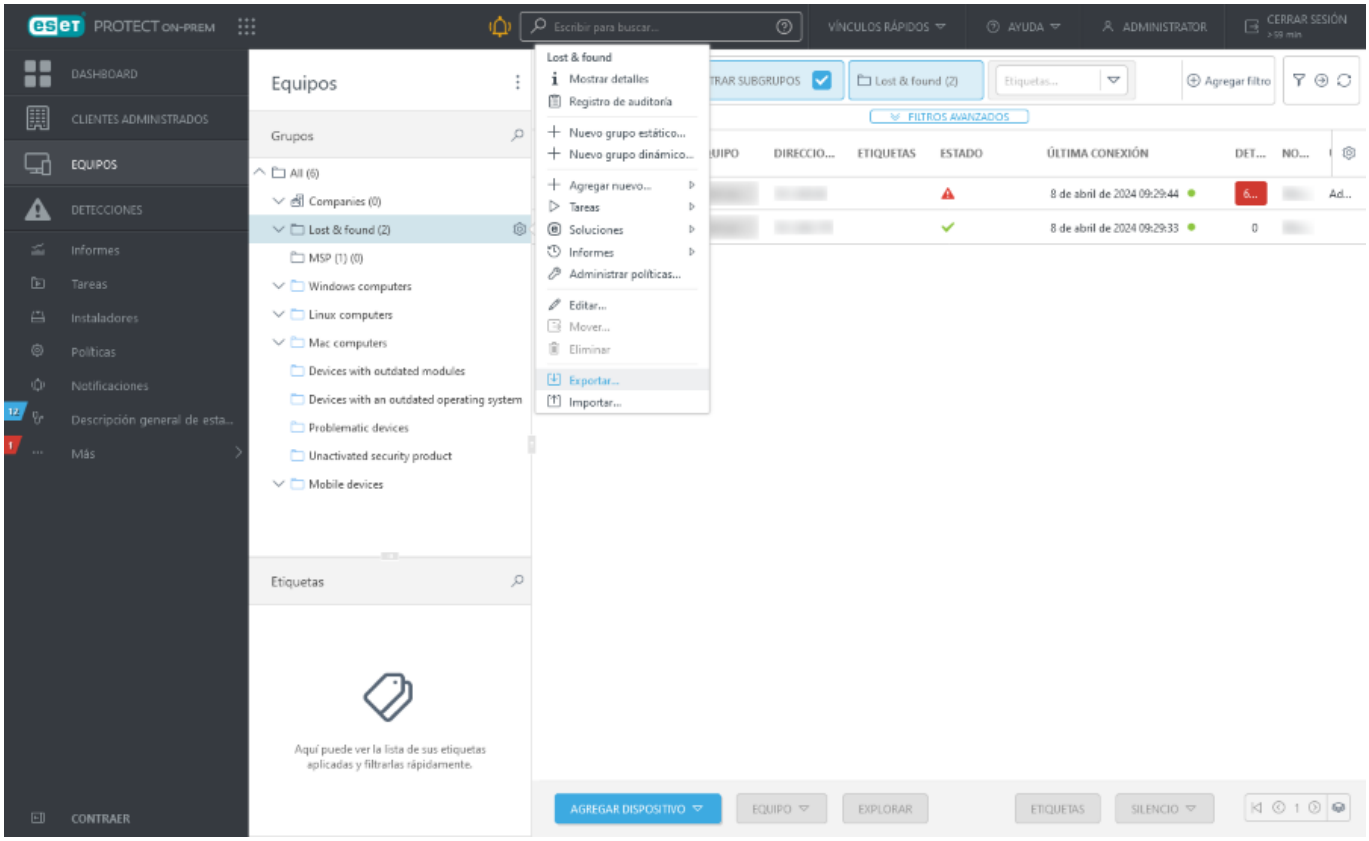
Seleccione un grupo al que desea agregar los nuevos equipos de la AD. Además, seleccione los objetos en el AD desde donde desea realizar la sincronización y qué hacer con los duplicados. Ingrese la configuración de su conexión al servidor AD y establezca el Modo de sincronización para el **Active Directory/Open Directory/LDAP**.

Exportar grupos estáticos

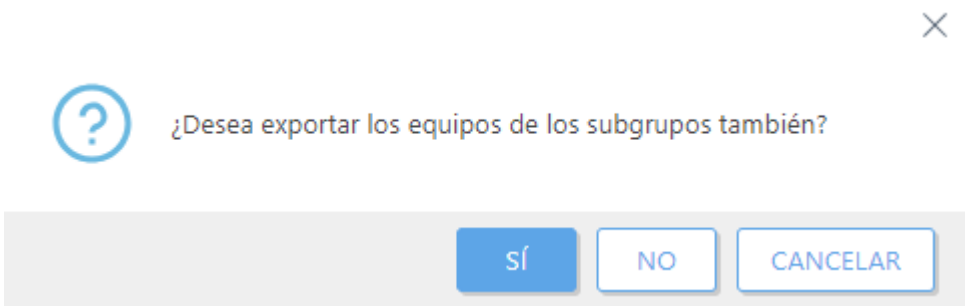
Exportar una lista de equipos que se encuentran en la estructura de ESET PROTECT On-Prem es simple. Puede exportar la lista y almacenarla como una copia de seguridad para que pueda importarla nuevamente en el futuro, por ejemplo, si desea restaurar la estructura del grupo.

Los grupos estáticos necesitan contener al menos un equipo. No es posible exportar grupos vacíos.

1. Vaya a **Equipos** y seleccione el grupo estático que quiera exportar.
2. Haga clic en el ícono del engranaje y seleccione **Exportar**.



3. Si el grupo estático seleccionado contiene subgrupos con equipos, puede seleccionar exportar equipos de los subgrupos, también.

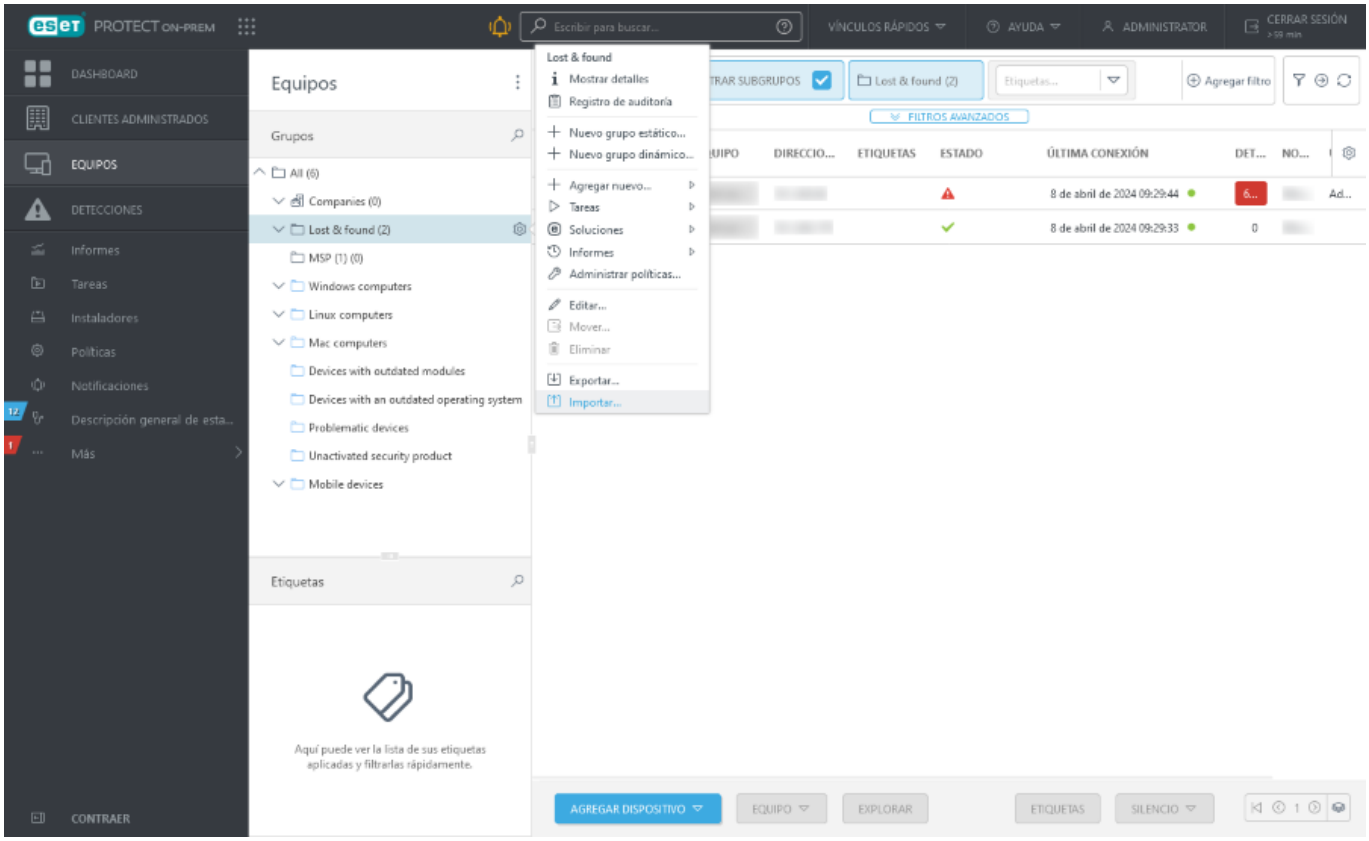


4. El archivo se guardará en formato *.txt*.

> Los Grupos dinámicos no se pueden exportar porque estos son solo vínculos a los equipos según los criterios definidos en las Plantillas de los grupos dinámicos.

Importar Grupos estáticos

Los archivos exportados desde los grupos estáticos se pueden importar nuevamente a la consola web ESET PROTECT y se pueden incluir en la estructura del grupo existente.



1. Haga clic en **Equipos** y seleccione cualquier grupo estático.

2. Haga clic en el ícono del engranaje y seleccione **Importar**.

3. Haga clic en **Examinar** y desplácese hasta el archivo *.txt*. Cada línea del archivo debe contener una ruta completa al nombre del equipo/dirección IP (con una barra diagonal inversa como separador). Por ejemplo:

```
All\Lost & found\Computer_Name
All\Lost & found\10.20.30.40
```

4. Seleccione el archivo del grupo y haga clic en **Abrir**. El nombre del archivo se muestra en el cuadro de texto.

5. Seleccione una de las siguientes opciones para resolver conflictos:

- **No cree ni mueva dispositivos si se han encontrado las mismas entradas en otro lugar**: si existen grupos estáticos y los equipos del archivo *.txt* ya pertenecen a este grupo, esos equipos se omiten y no se importan. Se visualiza información al respecto.

- **Mover los dispositivos existentes si aún no existen en las rutas importadas. Siempre que sea posible, mantenga los dispositivos administrados en la misma ruta de acceso**: si existen grupos estáticos y los equipos del archivo *.txt* ya pertenecen a este grupo, es necesario mover los equipos a otros grupos estáticos antes de la importación; luego de la importación, estos equipos se moverán nuevamente a los grupos originales de donde se habían movido.

- **Duplique los dispositivos existentes si aún no existen en las rutas importadas**: si los grupos estáticos existen y los equipos del archivo *.txt* ya existen en este grupo, los duplicados de estos equipos se crean en el mismo grupo estático. El equipo original se visualiza con toda la información y el duplicado se visualiza únicamente con el nombre de su equipo.

6. Haga clic en **Importar** para importar el grupo estático y los equipos.

Árbol del grupo estático para ESET Business Account o ESET MSP Administrator

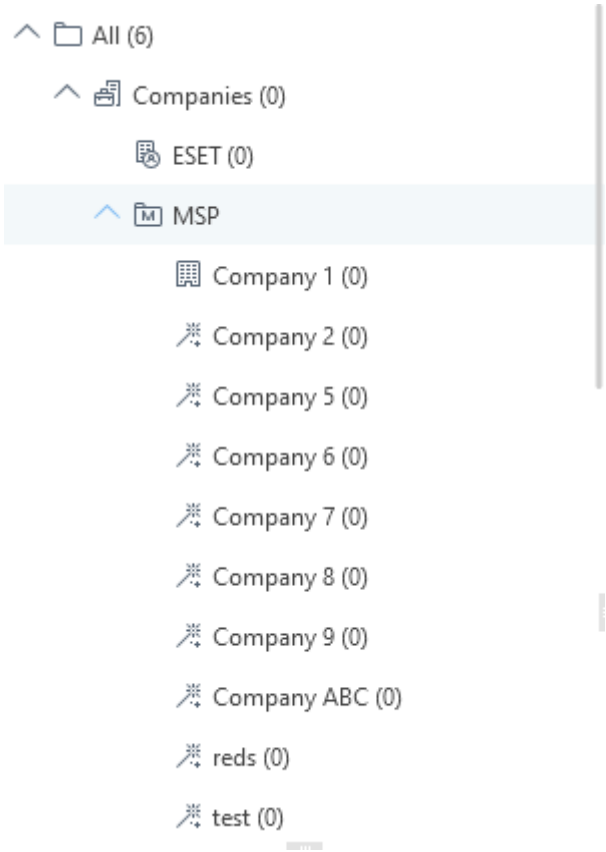
Si importa licencias desde ESET Business Account, la estructura de la empresa ESET Business Account (incluidos los sitios) aparece en el árbol de grupo estático (una nueva característica de la versión de ESET PROTECT On-Prem 9.1).

Si importa licencias desde ESET MSP Administrator, la estructura de ESET MSP Administrator aparece en el árbol de grupo estático. Obtenga más información sobre ESET PROTECT On-Prem para proveedores de servicios administrados.

Estructura de árbol de grupos estáticos para ESET Business Account o ESET MSP Administrator

Puede ver la estructura de árbol del grupo estático para ESET Business Account o ESET MSP Administrator en **Equipos** en el árbol del grupo estático, en **Todas** > **Empresas**.

> Le recomendamos que utilice una cuenta en línea (ESET Business Account o ESET MSP Administrator. Consulte también Introducción a ESET Business Account) y sincronícela con ESET PROTECT On-Prem para aprovechar al máximo ESET PROTECT On-Prem.
> Si activó ESET PROTECT On-Prem con una clave de licencia o una licencia sin conexión, y no sincronizó licencias desde ESET Business Account o ESET MSP Administrator, no verá ESET Business Account o ESET MSP Administrator en la estructura de árbol del grupo estático.



En **Empresas**, puede ver uno o más árboles de ESET Business Account o ESET MSP Administrator según las cuentas sincronizadas en la opción Administración de licencias.

Si tiene una cuenta de ESET MSP Administrator, consulte los detalles sobre la estructura de las entidades en el MSP.

Sincronización del sitio ESET Business Account

Si tiene sitios de ESET Business Account, ESET PROTECT On-Prem los sincroniza automáticamente con el árbol del grupo estático y asigna licencias de cada sitio al grupo estático correspondiente (marcado con el ícono) debajo de la empresa ESET Business Account.

- Se recomienda utilizar el sitio de grupos estáticos creados automáticamente para administrar sus sitios (en lugar de crear grupos estáticos manualmente).
- Debe crear administradores de sitios y asignar sus permisos de forma manual. Seleccione el grupo estático del sitio correspondiente como el grupo de pertenencia de cada administrador del sitio y asigne al administrador un conjunto de permisos con el mismo grupo de pertenencia.

Por ejemplo, tiene dos sitios (**site1** y **site2**):
1.Cree un usuario para cada sitio (**site1_admin** y **site2_admin**).
2.Opcional: Asigne el grupo de pertenencia (sitio) correspondiente a cada usuario (**site1** a **site1_admin** y **site2** a **site2_admin**).
3.Cree un conjunto de permisos para cada usuario (**site1_permissions** para **site1_admin** y **site2_permissions** para **site2_admin**).
4.Asigne el grupo estático correspondiente a cada conjunto de permisos (**site1** a **site1_permissions** y **site2** a **site2_permissions**).
5.Asigne las funcionalidades y el nivel de acceso necesarios de cada conjunto de permisos (**Lectura**, **Uso**, **Escritura**).
6.Asigne cada conjunto de permisos al usuario correspondiente (**site1_permissions** a **site1_admin** y **site2_permissions** a **site2_admin**).
7.Ahora, cada administrador del sitio solo puede ver su sitio y sus objetos (por ejemplo, licencias).

Si sincroniza un sitio en la estructura de árbol del grupo estático y cambia el nombre del sitio en ESET Business Account, también cambiará su nombre en ESET PROTECT On-Prem.

Si sincroniza un sitio en la estructura de árbol del grupo estático y quita el sitio en ESET Business Account, su ícono en ESET PROTECT On-Prem cambiará a .

Objetos compartidos

La estructura de árbol de grupos estáticos ESET Business Account o ESET MSP Administrator contiene grupos estáticos dedicados adicionales llamados **Objetos compartidos**.

Puede utilizar los **Objetos compartidos** para compartir objetos de la consola web (políticas, plantillas de grupos dinámicos, etc.) a más usuarios con acceso limitado (acceso a grupos estáticos al mismo nivel que los **Objetos compartidos** o debajo de ellos en la estructura de árbol):

1. Seleccione **Objetos compartidos** como grupo de acceso para el objeto de la consola web. El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario.

2. Asigne el permiso **Uso** a **Objetos compartidos**.

- Asegúrese de que no se asigne el permiso de **Escritura** en **Objetos compartidos** a usuarios limitados para evitar que los editen. El permiso **Uso** es suficiente.
- No puede almacenar equipos en **Objetos compartidos**. Los **Objetos compartidos** no están visibles en **Grupos** en **Equipos**.

Grupos dinámicos

Los Grupos dinámicos pueden ser vistos con los filtros con base en el estado del equipo. Un equipo puede coincidir con más de un filtro y, por lo tanto, puede estar asignado a más de un Grupo dinámico. Esto hace que los Grupos dinámicos sean diferentes de los Grupos estáticos, porque un solo cliente no puede pertenecer a más de un grupo estático.

Los Grupos dinámicos son grupos de clientes seleccionados en función de condiciones específicas. Para que un equipo se convierta en un miembro de un Grupo dinámico específico, debe cumplir con ciertas condiciones definidas en la plantilla de grupo dinámico. Cada plantilla consiste en una o varias Reglas. Puede especificar estas reglas al crear una nueva Plantilla. Si el equipo de un cliente no cumple con los criterios, se eliminará del grupo. Si

cumple con las condiciones definidas, se agregará al grupo.

Los dispositivos se evalúan para la inclusión en los grupos dinámicos cada vez que ingresan en ESET PROTECT On-Prem. Cuando un dispositivo cumple con los valores especificados en una plantilla de grupo dinámico, se asigna automáticamente a este grupo. Los equipos se filtran del lado del Agente, por lo que no es necesario transferir información adicional al servidor. El Agente decide, por cuenta propia, a qué Grupos dinámicos pertenece un cliente y solo notifica al servidor acerca de esta decisión.

> Si el dispositivo cliente no está conectado (por ejemplo, se encuentra apagado), su membresía en los grupos dinámicos no se actualiza. Luego de volver a conectar el dispositivo, su membresía en los grupos dinámicos se actualizará.

Después de instalar ESET PROTECT On-Prem, hay disponibles algunos grupos dinámicos predefinidos. También puede crear grupos dinámicos personalizados. Existen dos formas para hacerlo:

- Primero, cree una plantilla y, luego, cree un grupo dinámico.
- Cree una plantilla nueva cuando cree un nuevo grupo dinámico.

Puede usar grupos dinámicos en otras partes de ESET PROTECT On-Prem. Puede asignarles políticas (ver cómo se aplican las políticas) o preparar una tarea para todos los equipos del grupo.

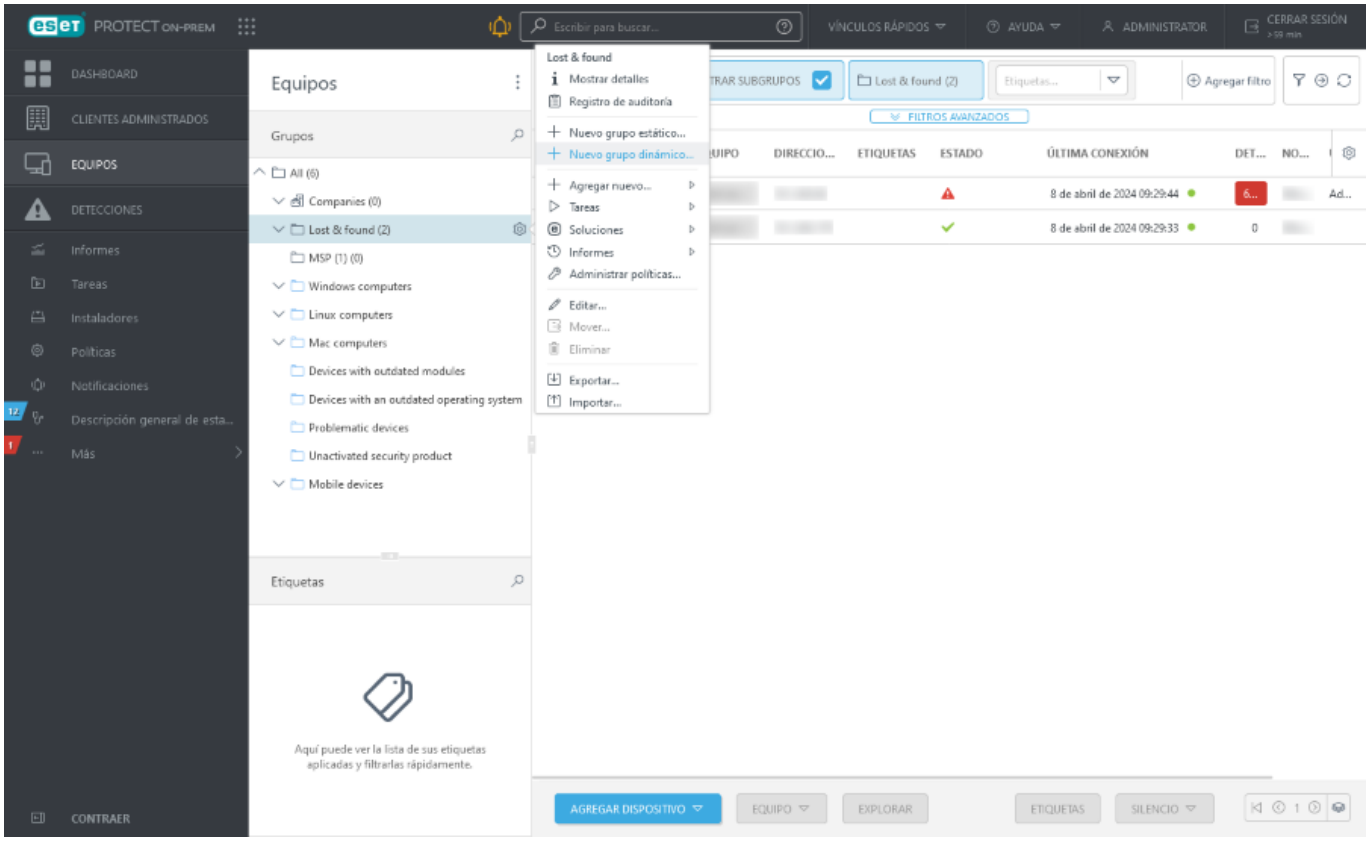
Un grupo dinámico puede pertenecer a un grupo estático o grupos dinámicos. Sin embargo, un grupo estático no puede estar dentro de un grupo dinámico. Todos los grupos dinámicos que pertenecen a un grupo estático solo filtran dispositivos dentro de ese grupo estático. Si un grupo dinámico se encuentra dentro de otro grupo dinámico, filtra los resultados del grupo dinámico superior. Una vez creado el grupo, puede moverse libremente por el árbol.

La administración de grupos dinámicos está disponible mediante las acciones de grupos.

Crear un nuevo grupo dinámico

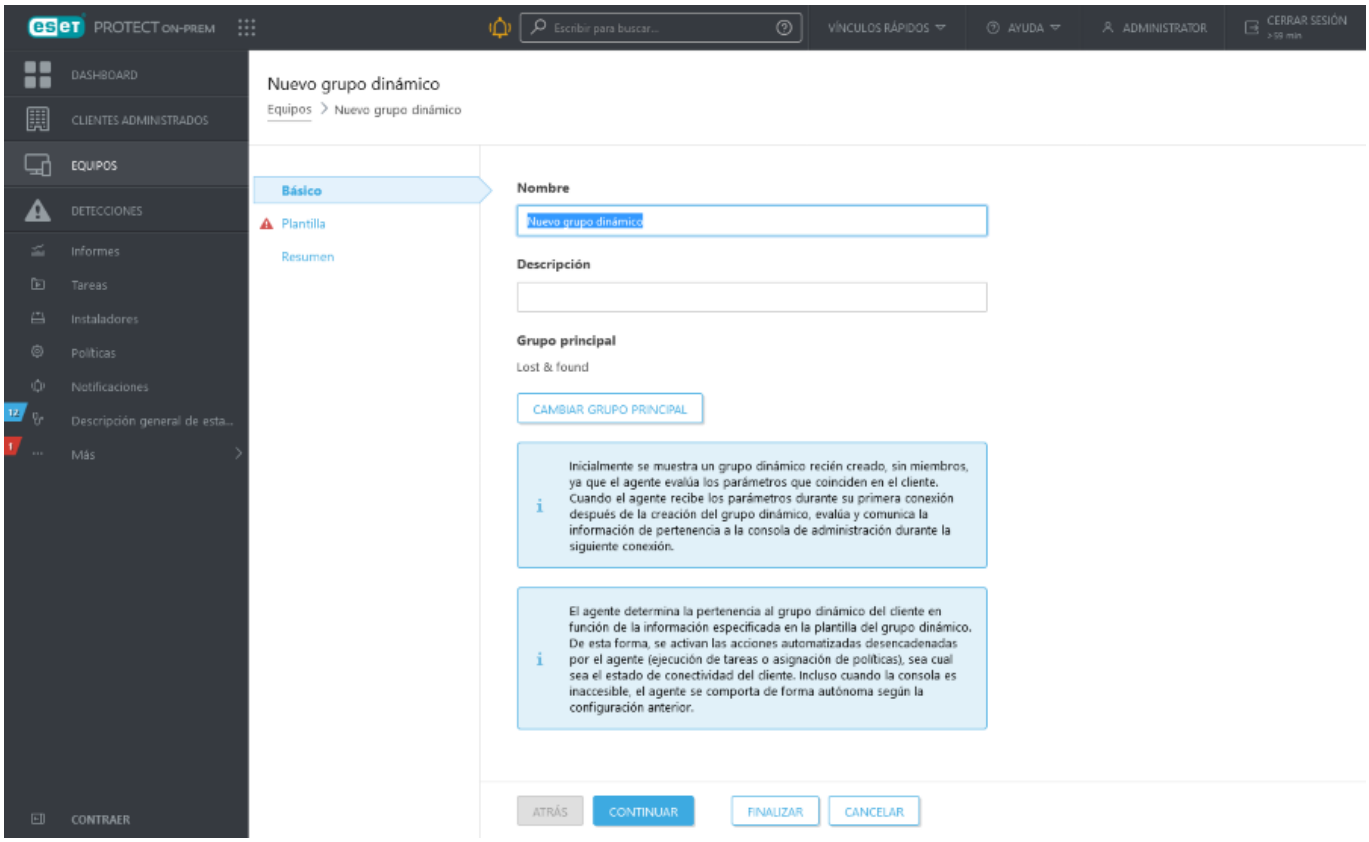
Siga estos pasos para crear un nuevo grupo dinámico.

1. Haga clic en **Equipos**, seleccione el ícono de engranaje junto a cualquier grupo y seleccione **Grupo estático nuevo**. Aparecerá un Asistente de grupo dinámico nuevo.



2. Ingrese un nombre y una descripción para la plantilla nueva.

3. También puede cambiar el grupo principal al hacer clic en **Cambiar grupo principal**.



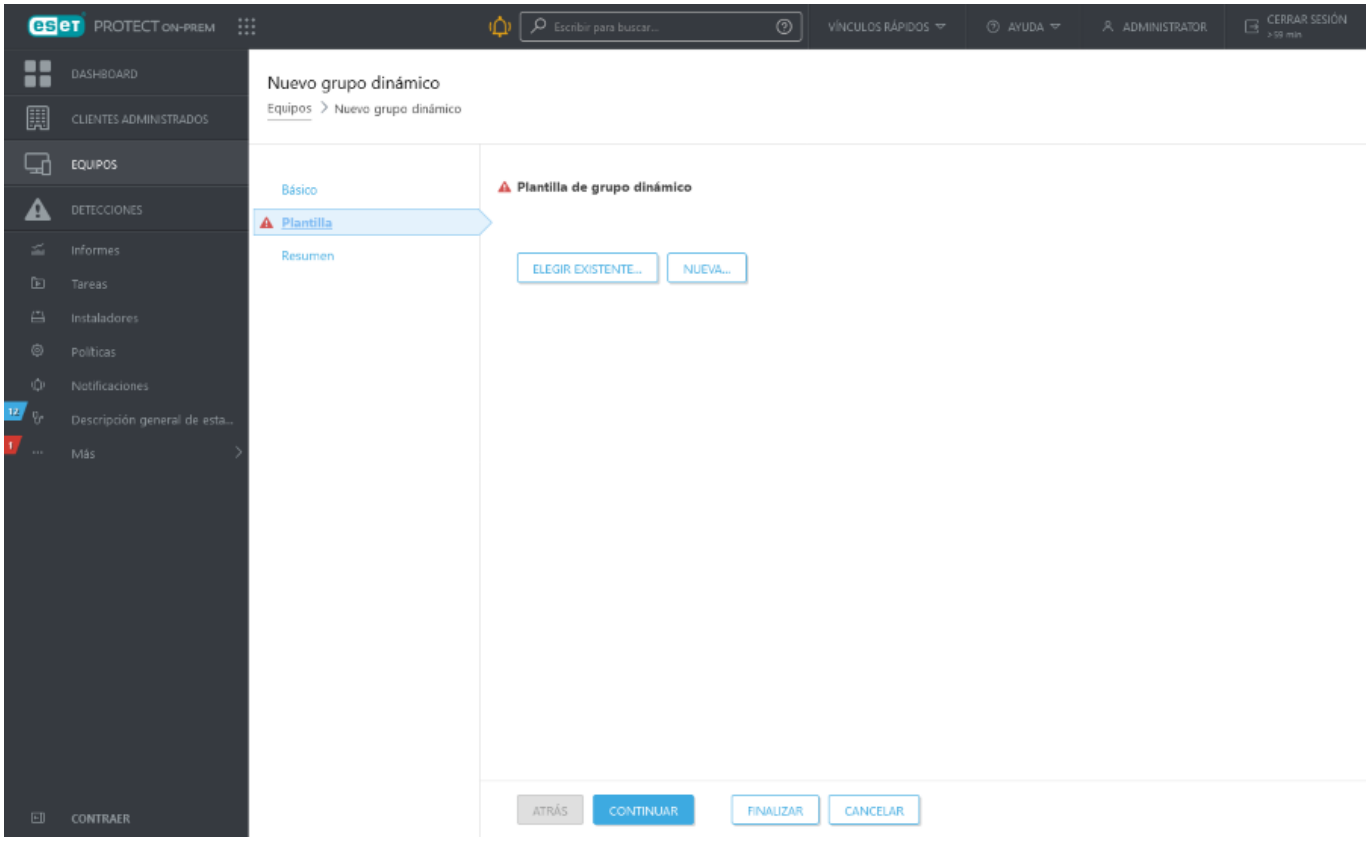
4. Haga clic en **Plantilla**. Cada Grupo dinámico se crea desde una plantilla que defina cómo el grupo filtra equipos cliente. Se pueden crear ilimitados grupos dinámicos con una plantilla.

Una plantilla es un objeto estático en un grupo estático. Los usuarios deben contar con los permisos adecuados para acceder a las plantillas. Un usuario necesita de permisos de acceso para poder trabajar con plantillas de grupo dinámico. Todas las plantillas predefinidas se encuentran en el grupo estático **Todos** y, por defecto, se encuentran disponibles solo para el administrador. Los otros usuarios necesitan permisos adicionales asignados. Como resultado, es posible que los usuarios no puedan ver ni usar plantillas predeterminadas. Las plantillas se pueden mover a un grupo donde los usuarios tengan permisos.
Para duplicar una plantilla, el usuario debe contar con permisos de **Uso** (para plantillas de grupo dinámico) para el grupo donde se encuentra la plantilla fuente y de **Escribir** para el grupo hogar del usuario (donde se almacenará el duplicado). Consulte el ejemplo de duplicación de objetos.

- Si desea crear un grupo desde una plantilla predefinida o desde una plantilla que ya ha creado, haga clic en **Seleccionar existente** y seleccione la plantilla adecuada en la lista.

- En caso de que todavía no haya creado ninguna plantilla, y ninguna de las plantillas predefinidas de la lista le parezca adecuada, haga clic en **Nuevo** y siga los pasos para crear una plantilla nueva.

Para más casos de uso sobre cómo crear un nuevo grupo dinámico con base en una plantilla de grupo dinámico consulto los ejemplos.



5. Haga clic en **Resumen**. El grupo nuevo aparecerá debajo del grupo principal.

Mover grupo estático o dinámico

Un Grupo dinámico puede pertenecer a cualquier otro grupo, incluidos los Grupos estáticos. No puede moverse un grupo estático a un grupo dinámico. Además, no se puede mover grupos estáticos predefinidos (por ejemplo, **Perdidos y encontrados**) a ningún otro grupo. El resto de los grupos pueden moverse libremente.

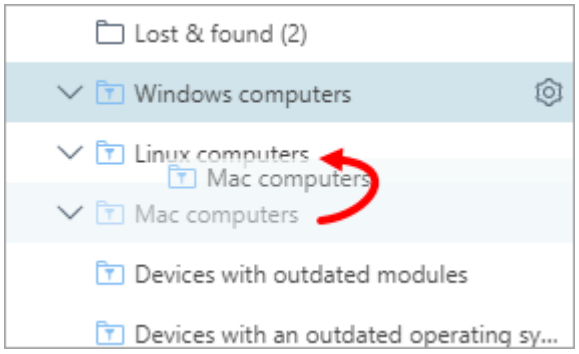
Haga clic en el ícono junto al nombre del grupo y seleccione **Mover**. Aparecerá una ventana con la estructura

de árbol del grupo. Seleccione los grupos de destino (estáticos o dinámicos) a los que desea mover el grupo seleccionado. El grupo de destino se convertirá en un grupo principal. Además, puede mover los grupos al arrastrarlos y soltarlos en el grupo de destino que desee.

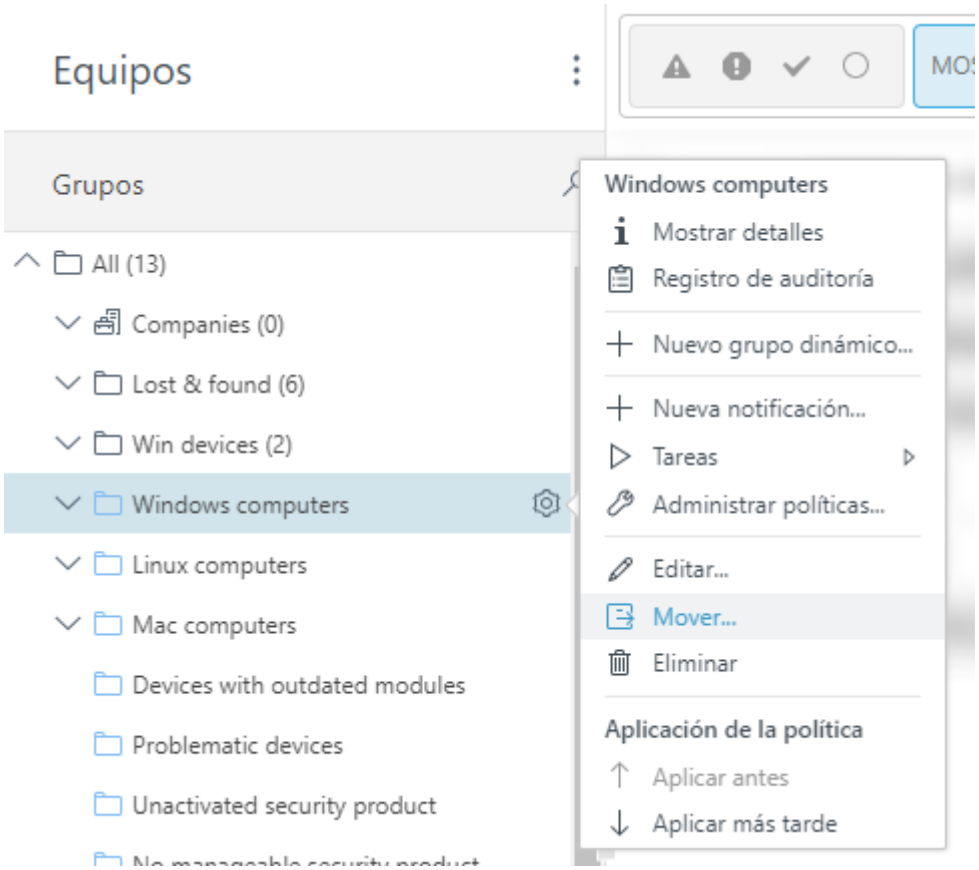
> El Grupo dinámico en una posición nueva comienza a filtrar equipos (con base en la Plantilla) sin relación alguna con su ubicación anterior.

Hay 3 métodos para mover un grupo:

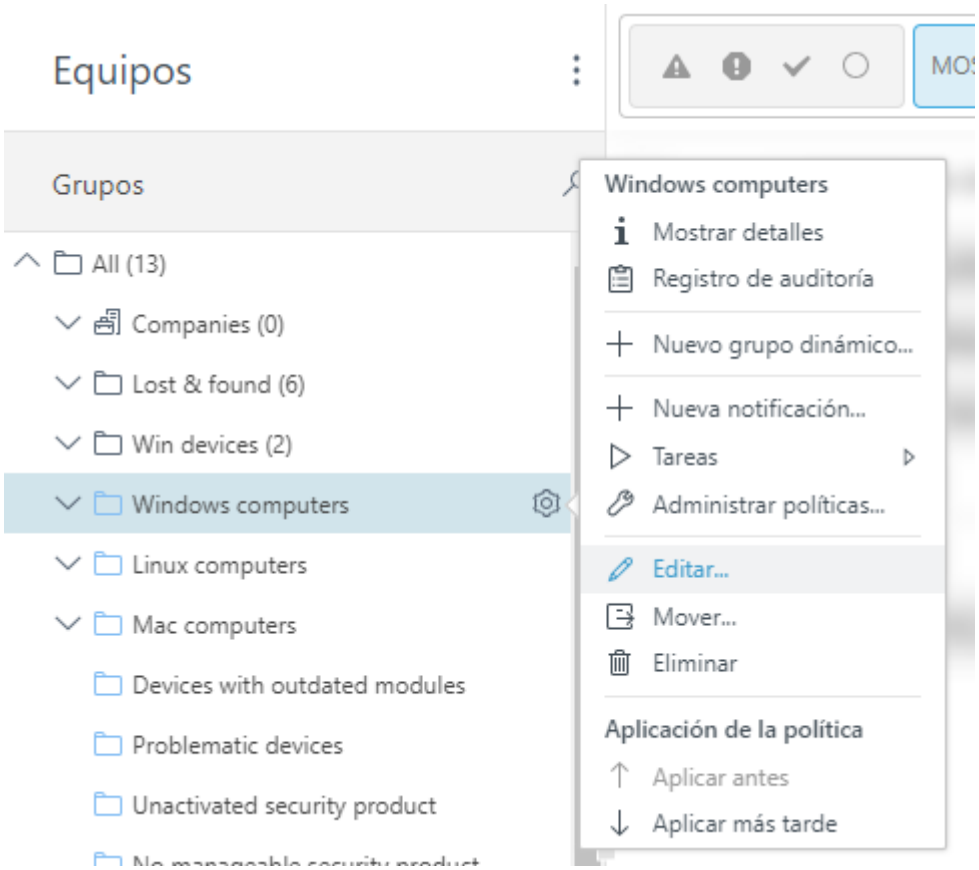
- **Arrastrar y soltar**: haga clic y mantenga el grupo que desea mover, luego suéltelo sobre el nuevo grupo principal.



- Haga clic en el icono ⚙ > **Mover** >, seleccione un nuevo grupo principal de la lista y haga clic en **Aceptar**.

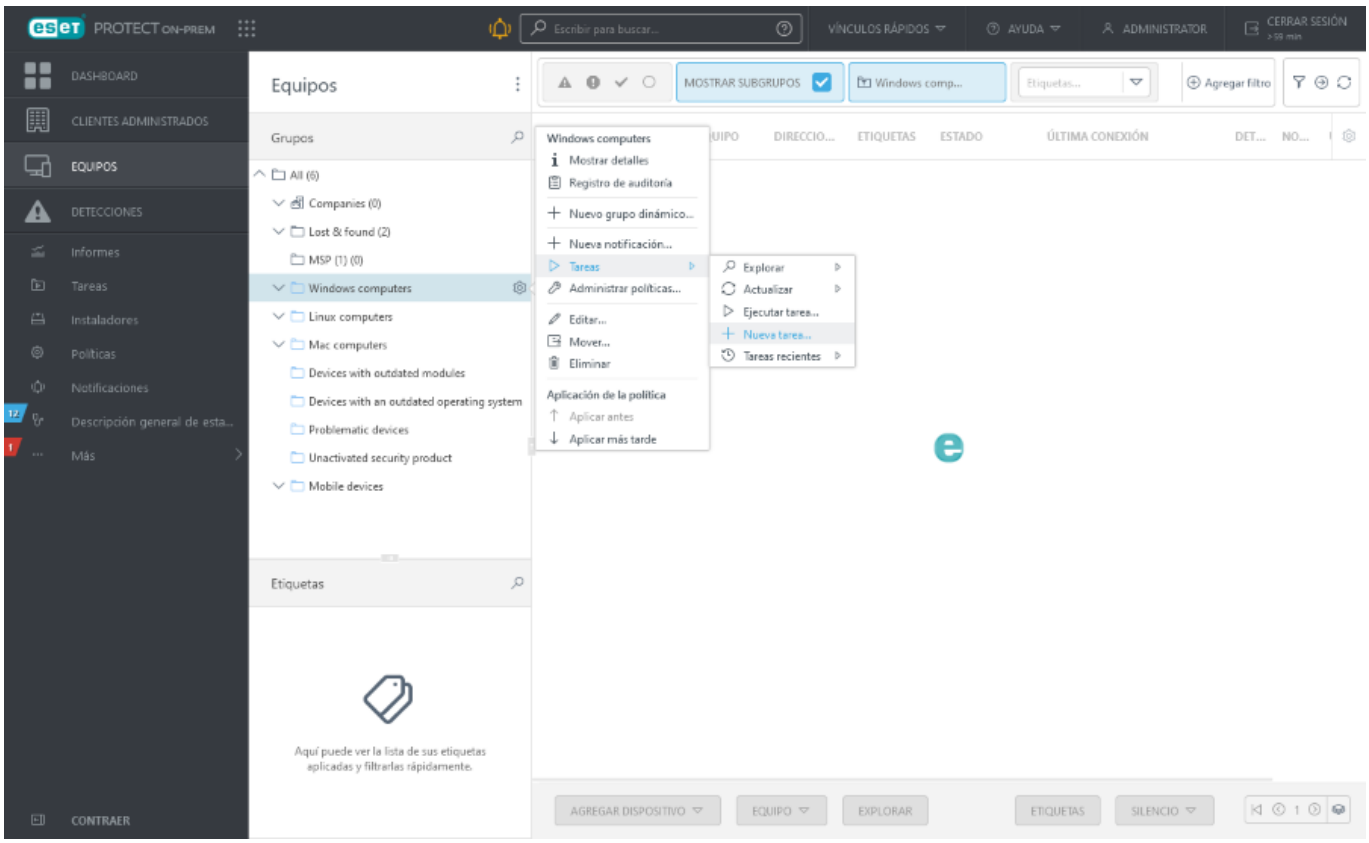


- Haga clic en el ícono ⚙ > **Editar >** y seleccione **Cambiar grupo principal**. Seleccione un nuevo grupo principal de la lista y haga clic en **Aceptar**.



Asignar una tarea de cliente a un grupo

Haga clic en **Equipos**, seleccione **Grupo estático** o **Grupo dinámico** y haga clic en el ícono del engranaje > **Tareas** > **Nueva tarea**. Se abrirá una nueva ventana del Asistente de nuevas tareas de clientes.

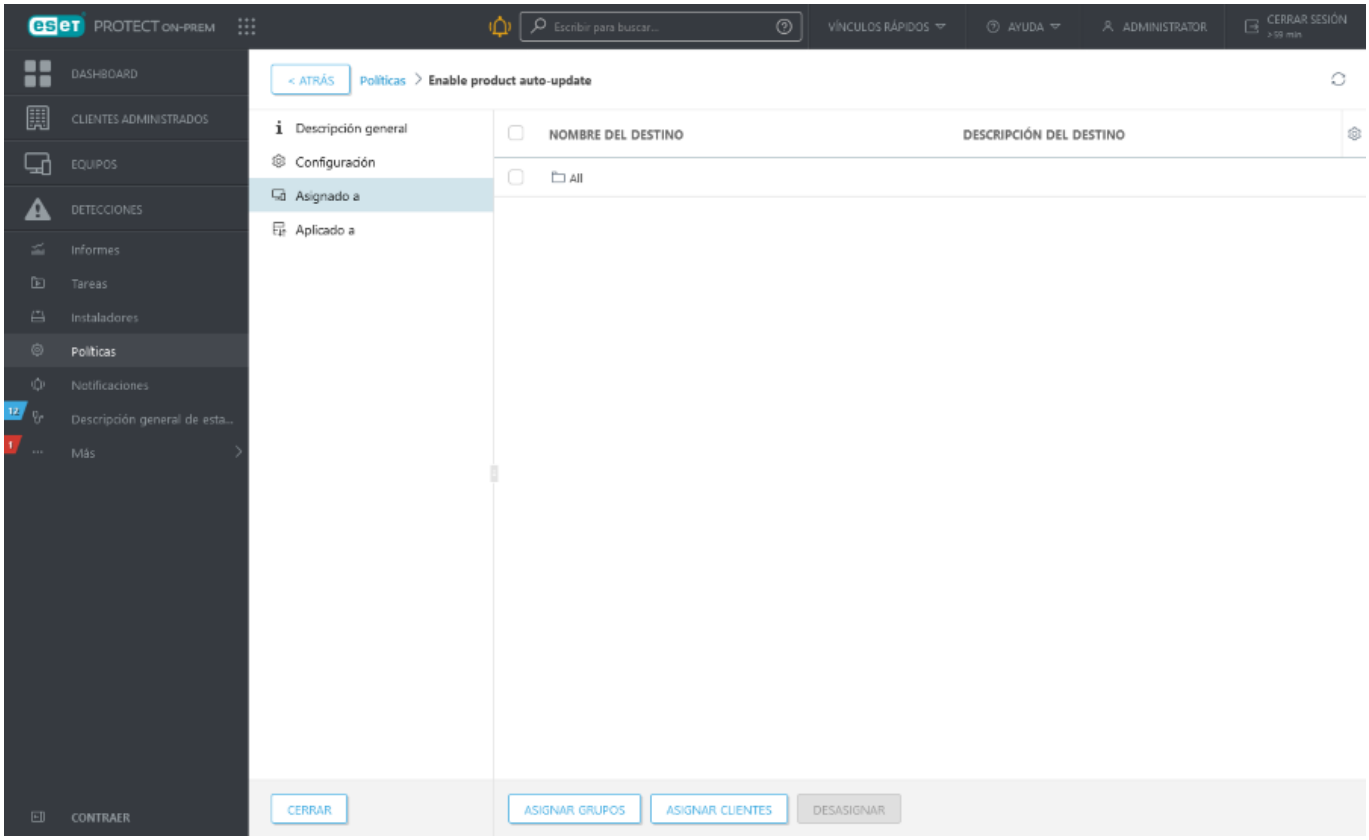


Asignar una política a un grupo

Después de crear una política, puede asignarla a un **Grupo estático** o **dinámico**. Hay dos formas de asignar una política:

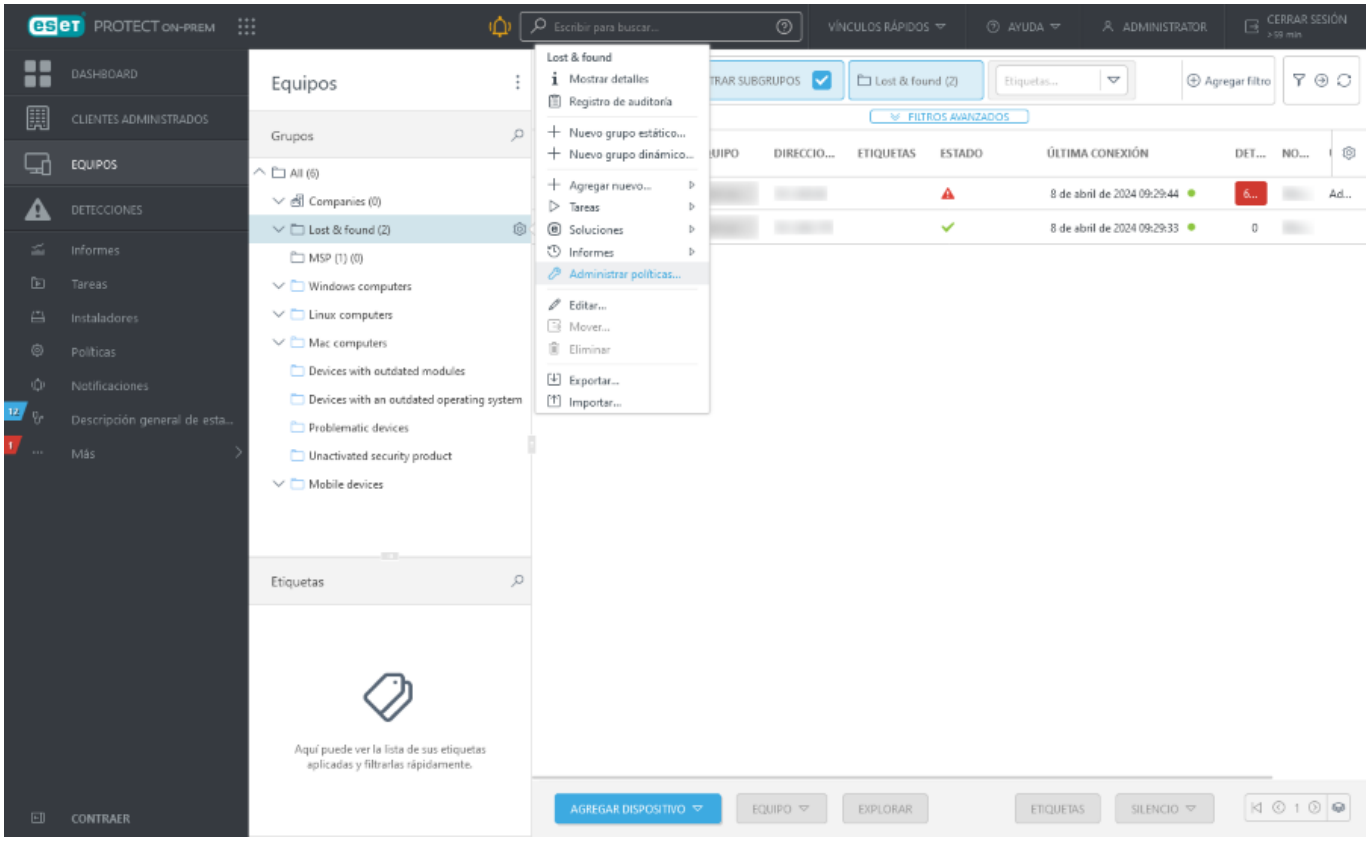
Método I.

En **Políticas**, seleccione una política y haga clic en **Acciones** > **Mostrar detalles** > **Asignado a** > **Asignar grupo(s)**. Seleccione un grupo estático o dinámico de la lista (puede seleccionar más grupos) y haga clic en **Aceptar**.



Método II.

1. Haga clic en **Equipos** y luego en el ícono del engranaje junto al nombre del grupo y seleccione **Administrar políticas**.



2. En la ventana de **Orden de aplicación de políticas** haga clic en **Agregar política**.

3. Seleccione la casilla de verificación junto a la política que desea asignar a este grupo y haga clic en **Aceptar**.

4. Haga clic en **Cerrar**.

Para ver qué políticas se asignaron a un grupo en particular, seleccione ese grupo y haga clic en la pestaña de **Políticas** para visualizar una lista de políticas asignadas al grupo.

Para ver cuáles grupos están asignados a una política en particular, seleccione la política y haga clic en **Mostrar detalles** > **Aplicado a**.

Para obtener más información acerca de las políticas, consulte el capítulo Políticas.

Detecciones

La sección **Detecciones** le brinda una vista general de todas las detecciones encontradas en los dispositivos administrados.

A la izquierda, se visualiza la estructura del Grupo. Puede explorar los grupos y ver las detecciones encontradas en los miembros de un grupo determinado. Para ver todas las detecciones encontradas en los clientes asignados a los grupos de su cuenta, seleccione el grupo **Todos** y quite todos los filtros aplicados.

Consulte el glosario de ESET para obtener más información acerca de las tecnologías de ESET y los tipos de detecciones o ataques contra los que protegen.

Estado de la detección

Hay dos tipos de detecciones en función del estado:

- **Detecciones activas**: las detecciones activas son aquellas que aún no fueron desinfectadas. Para limpiar la detección, ejecute una **exploración exhaustiva** con la limpieza habilitada en la carpeta que contenga la detección. La tarea de exploración debe finalizar correctamente para limpiar la detección y no tener más detecciones. Si un usuario no resuelve una detección activa en un plazo de 24 horas después de su descubrimiento, pierde el estado **Activo**, pero queda sin resolver.

- **Detecciones resueltas**: estas son detecciones que han sido marcadas por un usuario como resueltas, sin embargo aún no han sido analizadas con la **Exploración exhaustiva**. Los dispositivos con detecciones marcadas como resueltas seguirán apareciendo en la lista de resultados filtrados hasta que se realice la exploración.

El estado de **Detección controlada** indica si un producto de seguridad de ESET realizó una acción contra una detección (en función del tipo de detección y la configuración del nivel de limpieza):

- **Sí:** el producto de seguridad de ESET realizó una acción contra la detección (quitar, limpiar o poner en cuarentena).

- **No:** el producto de seguridad de ESET no realizó ninguna acción contra la detección.

Puede usar la **Detección controlada** como filtro en Informes, Notificaciones y Plantillas de grupos dinámicos.

No todas las detecciones encontradas en los dispositivos de los clientes se ponen en cuarentena. Las detecciones que no se ponen en cuarentena incluyen:
- Detecciones que no pueden eliminarse
- Detecciones que son sospechosas por su comportamiento, pero no se detectan como malware, por ejemplo, las PUA.

Durante la limpieza de la base de datos, también se quitan los elementos en Detecciones que corresponden a registros de incidentes desinfectados (independientemente del estado de la detección). De forma predeterminada, el período de limpieza para los registros de incidentes (y Detecciones) se establece en 6 meses. Puede cambiar el intervalo en **Más** > Configuración.

Agregación de detecciones

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

Detecciones en archivos

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

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

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

Filtrar detecciones

De forma predeterminada, se muestran todos los tipos de detecciones de los últimos siete días, incluidas las detecciones que han sido desinfectadas exitosamente. Puede filtrar las detecciones según varios criterios: **Equipo sin sonido y Ocurrió** están habilitados de forma predeterminada.

Algunos filtros están activos de forma predeterminada. Si las detecciones se indican en el botón **Detecciones** del menú principal, pero no las puede ver en la lista de detecciones, compruebe qué filtros están habilitados.

Agrupación de detecciones

Para agrupar las detecciones, seleccione en el menú desplegable:

- **Sin agrupar**: vista predeterminada
- **Agrupadas por el equipo**: detecciones agrupadas por un nombre de equipo
- **Agrupadas por categoría**: detecciones agrupadas por una categoría de detección
- **Agrupadas por tipo**: detecciones agrupadas por una categoría de detección y su tipo de detección
- **Agrupadas por hash**: detecciones agrupadas por un hash
- **Agrupadas por causa**: detecciones agrupadas por una causa
- **Agrupadas por usuario**: detecciones agrupadas por un usuario

Para ver todas las detecciones agrupadas en una fila concreta, haga clic en cualquier fila y en **Abrir detección de listas**. A continuación, la información sobre el grupo de detección se muestra en la parte superior de la página. Haga clic en el ícono de la **flecha hacia abajo** para desplazarse entre las detecciones agrupadas. Haga clic en el ícono de la **flecha hacia atrás** para volver a los grupos de detección.

Para una vista más específica, puede agregar otros filtros, como:

- **Categoría de detección**: **antivirus**, archivos bloqueados, ESET Inspect, **firewall**, **HIPS** y **protección web**.
- **Tipo de detección**
- **Dirección IP** del cliente que informó la detección
- **Explorador**: seleccione el tipo de análisis que informó la detección. Por ejemplo, el **Explorador antiransomware** muestra las detecciones informadas por la protección contra ransomware.

• **Acción**: seleccione la acción que se ha llevado a cabo en la detección. Los productos de seguridad ESET informan las siguientes acciones a ESET PROTECT On-Prem:

o**limpio**: se limpió la detección.

o**quitado/borrado mediante una acción de quitar**: se eliminó la detección.

o**era parte de un objeto**: se quitó un archivo que contenía la detección.

o**bloqueo/conexión finalizada**: se bloqueó el acceso al objeto detectado.

o**conservado**: no se realizó ninguna acción debido a varias razones, por ejemplo:

➢ En la alerta interactiva, el usuario seleccionó manualmente no realizar ninguna acción.

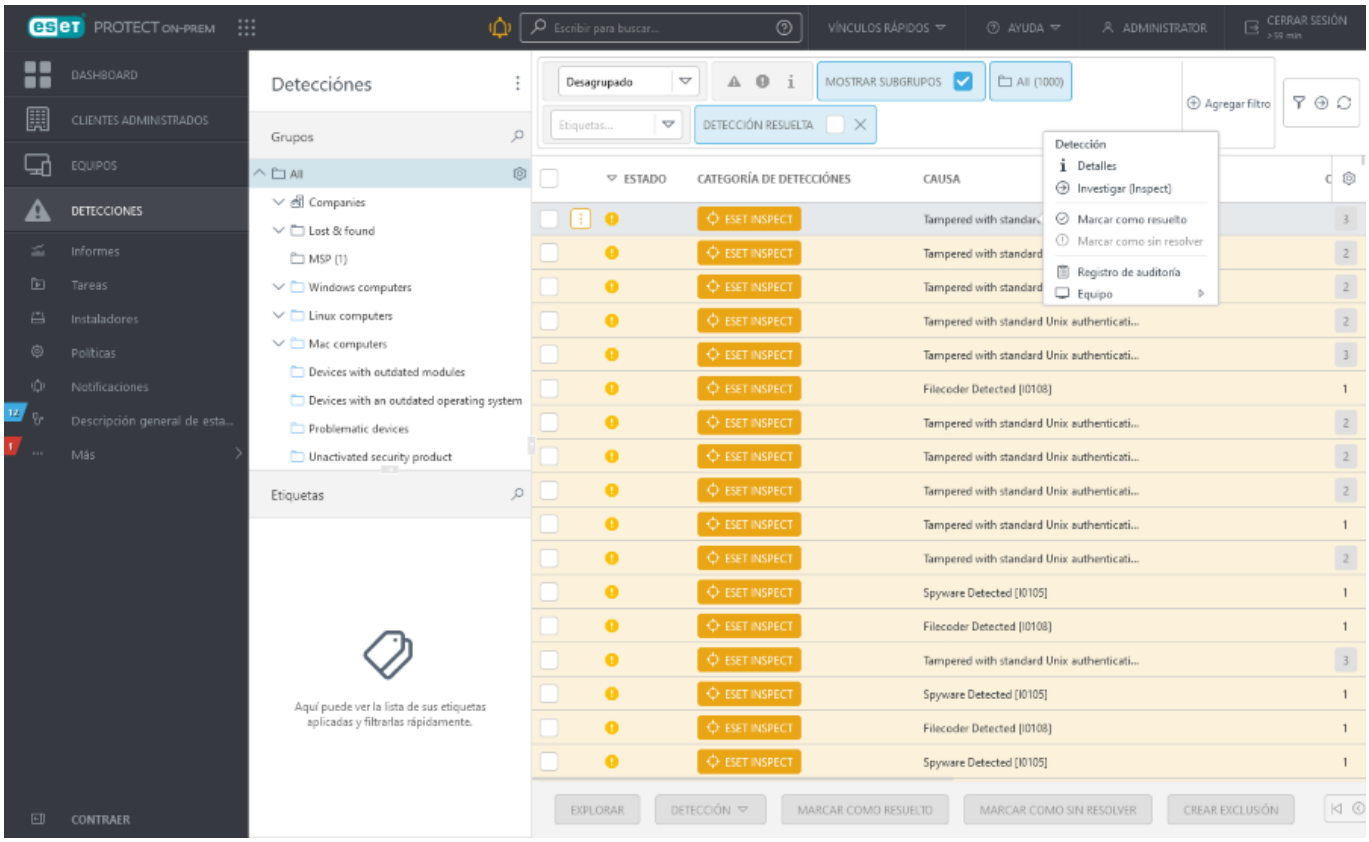
➢ En la configuración del motor de detección del producto de seguridad ESET, el nivel de **Protección** para la categoría de detección se define más bajo que el nivel de **Informe**.

Personalización del diseño y de los filtros

Puede personalizar la vista de la pantalla de la consola web actual:

- Administre el panel lateral y la tabla principal.
- Agregar filtro y filtros preestablecidos. Puede usar etiquetas para filtrar los elementos mostrados.

Administrar detecciones



Haga clic en el nombre de una detección para ver el panel lateral de vista previa de la detección a la derecha.

Para administrar detecciones, haga clic en el elemento y seleccione una de las acciones disponibles, o bien, seleccione la casilla de verificación ubicada junto a uno o más elementos, y use los botones de la parte inferior de la pantalla Detecciones:

- **Exploración**: ejecuta la Tarea de exploración bajo demanda en el dispositivo que informó la detección seleccionada.
- **Detalles**: consulte la sección Detalles de la detección.
- **Equipo**: lista de acciones que puede realizar en el equipo en el que se encontró la detección. Esta lista es la misma que la que aparece en la sección Equipos.
- **Registro de auditoría** - Ver el registro de auditoría del elemento seleccionado.
- **Marcar como resuelto** o **Marcar como no resuelto**: puede marcar las detecciones como resueltas/no resueltas aquí o en la opción Detalles del equipo.
- **Ruta de exploración**: (disponible únicamente para detecciones de **antivirus**; archivos con rutas conocidas): crea la Tarea de exploración bajo demanda con rutas y objetivos predefinidos.
- **Crear exclusión**: (disponible únicamente para detecciones de **antivirus** y reglas IDS del **firewall**): crea exclusiones de detecciones.
- **Investigar (Inspect)** le permite abrir los detalles del elemento directamente en la consola web de ESET Inspect On-Prem. El ícono **Inspect** en la esquina superior derecha abre la sección Detecciones de la consola web de ESET Inspect On-Prem. El ESET Inspect On-Prem solo está disponible cuando tiene una licencia de ESET Inspect On-Prem y ESET Inspect On-Prem está conectado a ESET PROTECT On-Prem. Un usuario de la consola web necesita permiso de **Lectura** o superior para **Acceder a ESET Inspect** o permiso de **Lectura** o superior para el usuario **ESET Inspect**.
- La función **Enviar el archivo a ESET LiveGuard** se encuentra disponible solo para **archivos bloqueados**. El usuario puede enviar un archivo a análisis de malware (ESET LiveGuard Advanced) desde la ESET PROTECT Consola Web. Puede ver los detalles del análisis de archivos en Archivos enviados. Puede enviar manualmente archivos ejecutables para su análisis desde el producto de punto de conexión ESET ESET LiveGuard Advanced (necesita tener la licencia ESET LiveGuard Advanced).

Vista previa de la detección

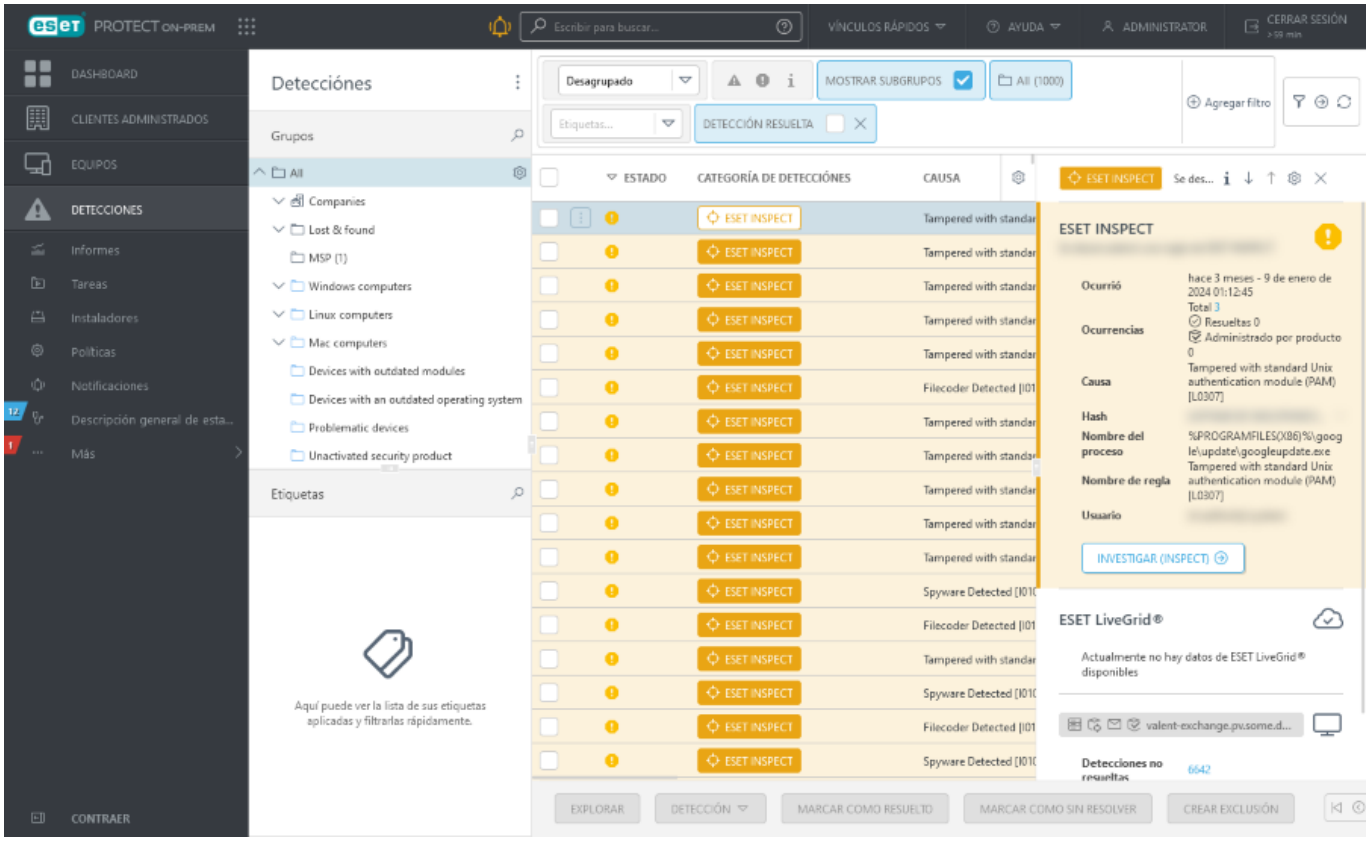
En **Detecciones**, haga clic en el nombre de una detección para ver el panel lateral de vista previa de la detección a la derecha. El panel lateral de vista previa de la detección contiene la información más importante sobre la detección seleccionada.

Manipulación de la vista previa de la detección:

- **Mostrar detalles:** abre Detalles de la detección.
- **Siguiente**: muestra el siguiente dispositivo en el panel lateral de vista previa de la detección.
- **Anterior**: muestra el dispositivo anterior en el panel lateral de vista previa de la detección.

• **Administrar el contenido de los detalles de la detección**: puede gestionar qué secciones del panel lateral de vista previa del equipo se muestran y en qué orden.

• **Cerrar**: cierra el panel lateral de vista previa de la detección.



Detalles de la detección

Hay dos secciones en Detalles de la detección:

• **Información general**: la sección **Información general** contiene información básica sobre la detección. Desde esta sección, puede administrar la detección con diversas acciones (las acciones disponibles dependen de la categoría de detección) o ir a Detalles del equipo para acceder a información detallada sobre el equipo en el que ocurrió la detección.

• **Ocurrencias**: la sección **Ocurrencias** se encuentra activa únicamente cuando la detección es acumulada y aporta la lista de ocurrencias individuales de la detección. Puede marcar todas las ocurrencias de la misma detección como resueltas/sin resolver.

Crear exclusión

Puede excluir el(los) elemento(s) seleccionado(s) para evitar que se los **detecte** en el futuro. Haga clic en una detección y seleccione **Crear exclusión**. Puede excluir únicamente las detecciones del **Antivirus** y del **Firewall** - Reglas IDS. Puede crear una exclusión y aplicarla a más equipos/grupos. La sección **Más** > **Exclusiones** contiene todas las exclusiones creadas, incrementa la visibilidad y simplifica la administración.

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

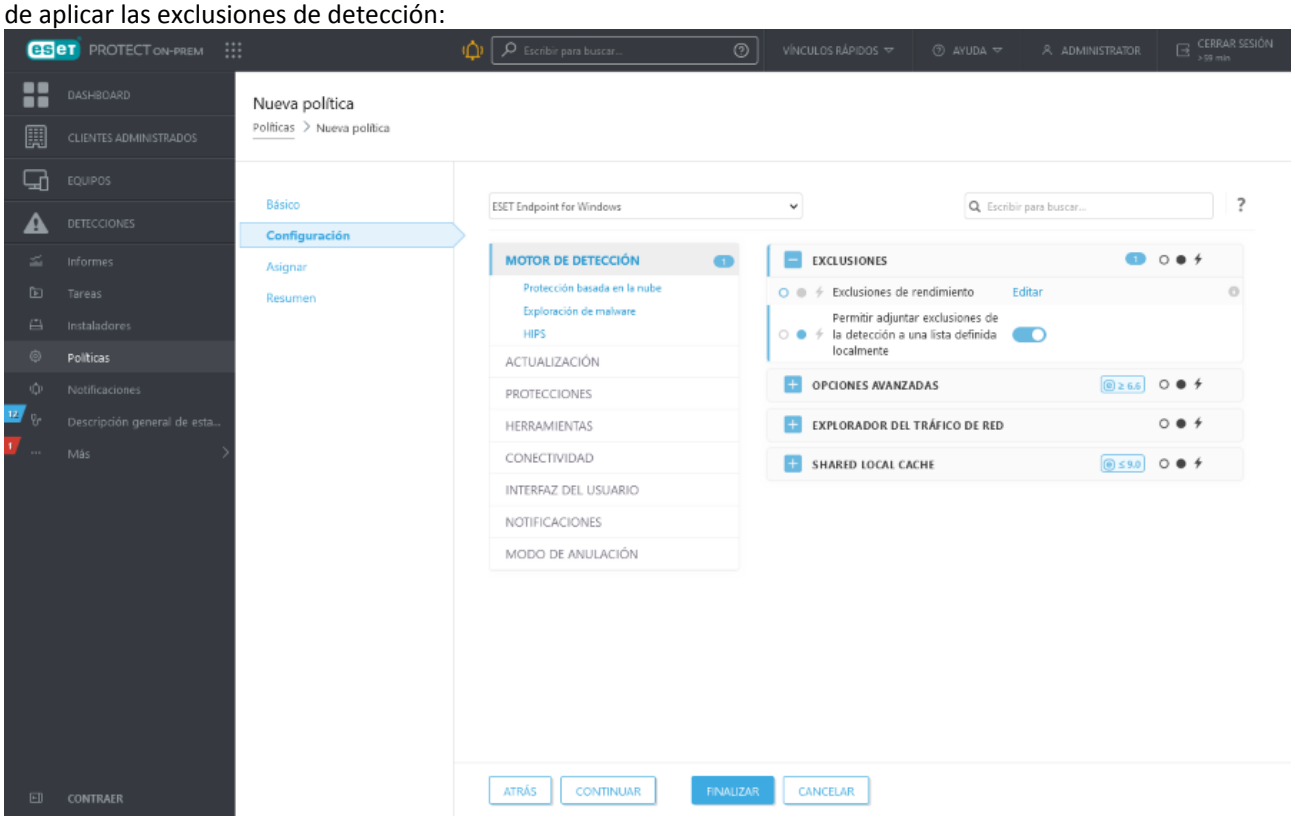
En ESET PROTECT On-Prem, hay dos categorías de exclusión de **antivirus**:

- **Exclusiones de rendimiento**: exclusiones de archivos y carpetas definidas por una ruta. Puede crearlas por medio de una política. Consulte también formatos y ejemplos de exclusiones del rendimiento.

- **Exclusiones de detección**: exclusiones de los archivos que se definen mediante el nombre de la detección, el nombre de la detección y su ruta, o el hash del objeto. Consulte también ejemplos de exclusiones de detección por nombre de detección.

Limitaciones de las exclusiones de detección

- En ESET PROTECT On-Prem, no puede crear exclusiones de detección a través de una política.
- En caso de que sus políticas incluyan exclusiones de detección previas, puede migrar las exclusiones de una política a la lista Exclusiones .
- De manera predeterminada, las exclusiones de detección reemplazan a la lista de exclusiones existentes locales en los equipos administrados. Para conservar la lista de exclusiones locales existentes, deberá aplicar la configuración de la política **Permitir adjuntar exclusiones de la detección a una lista definida localmente** antes de aplicar las exclusiones de detección:



Configuración

Puede excluir una o más detecciones en función de los **criterios de exclusión** seleccionados.

Detecciones de antivirus

- **Ruta y Detección**: excluir cada archivo por su ruta y nombre de detección, incluido el nombre de archivo (por ejemplo, *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

- **Archivos exactos**: excluir cada archivo por su hash.

- **Detección**: excluir cada archivo por nombre de la detección.

Detecciones en archivos

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

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

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

Detecciones de firewall - Reglas IDS

- **Detección y contexto** (recomendado): excluye la detección del firewall mediante el uso de una combinación de los siguientes criterios: por detección, aplicación y dirección IP.
- **Dirección IP**: excluye las detecciones del firewall por una dirección de IP remota. Utilice esta opción si la comunicación de la red con un equipo en particular provoca falsos positivos.
- **Detección**: excluye la detección e ignora los falsos positivos desencadenados a partir de equipos remotos múltiples.
- **Aplicación**: excluye la aplicación de las detecciones de la red. Permite la comunicación de la red para una aplicación que provoca falsos positivos de IDS.

La opción recomendada se selecciona previamente en función del tipo de detección.

Seleccione la casilla de verificación **Resolver alertas coincidentes** para resolver de manera automática las alertas cubiertas por la exclusión.

Opcionalmente, puede agregar un **Comentario**.

Destino

> ⚠ Puede asignar exclusiones (para detecciones de **Antivirus** y reglas IDS del **Firewall**) únicamente a equipos con productos de seguridad ESET compatibles instalados. No se aplicarán las exclusiones a productos de seguridad ESET no compatibles y se procederá a ignorarlas.

La exclusión se aplica de manera predeterminada al grupo hogar de un usuario.

Para cambiar las asignaciones, haga clic en **Agregar destinos** y seleccione el(los) destino(s) en el(los) que se aplicará la exclusión, o seleccione la(s) asignación(es) existente(s) y haga clic en **Quitar destinos**.

Vista previa

Le permite obtener la información general sobre las exclusiones creadas. Asegúrese de que la configuración de las exclusiones sea correcta según sus preferencias.

> ⚠ Luego de crear la exclusión, no puede editarla. Solo puede cambiar la asignación o quitar la exclusión.

Haga clic en **Finalizar** para crear la exclusión.

Puede ver y administrar todas las exclusiones creadas en **Más** > **Exclusiones**. Para comprobar si un equipo o un grupo tienen exclusiones aplicadas, vaya a Detalles del equipo > **Configuración** > **Exclusiones aplicadas** o Detalles del grupo > **Exclusiones**.

Productos de seguridad ESET compatibles con exclusiones

⚠ No se aplicarán las exclusiones a productos de seguridad ESET no compatibles y se procederá a ignorarlas.

Exclusiones de la detección antivirus

Todos los productos de seguridad administrables de ESET son compatibles con las exclusiones de detección **Antivirus**, excepto por el siguiente:

- ESET Endpoint Security para Android
- ESET LiveGuard Advanced
- ESET Inspect On-Prem

Exclusiones IDS del firewall

Los siguientes productos de seguridad de ESET son compatibles con las exclusiones IDS del **firewall**:

- ESET Endpoint Antivirus para Windows versión 8.0 y posteriores
- ESET Endpoint Security para Windows versión 8.0 y posteriores

Protección Anti-Ransomware

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

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

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

web ESET PROTECT.

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

ESET Inspect On-Prem

ESET Inspect On-Prem é un sistema integral de detección y respuesta de punto final que incluye características como: detección de incidentes, administración y respuesta ante incidentes, recolección de datos, indicadores de detección de riesgos potenciales, detección de anomalías, detección de comportamiento e incumplimientos de políticas. Para más información acerca de ESET Inspect On-Prem, su instalación y funciones, consulte la ayuda de ESET Inspect On-Prem.

Se ha cambiado el nombre de las siguientes soluciones de seguridad empresarial de ESET:

Nombre anterior:	Nombre nuevo:	Se ha cambiado el nombre en la versión:
ESET PROTECT	ESET PROTECT On-Prem	11.0
ESET PROTECT Cloud	ESET PROTECT	5.0
ESET Inspect	ESET Inspect On-Prem	2.0
ESET Inspect Cloud	ESET Inspect	

Configuración de ESET Inspect On-Prem

ESET Inspect On-Prem requiere que ESET PROTECT On-Prem haga lo siguiente:

- Crear un usuario de ESET Inspect On-Prem con los permisos adecuados. ESET PROTECT On-Prem contiene los conjuntos de permisos predefinidos para los usuarios de ESET Inspect On-Prem. Un usuario de la consola web necesita permiso de **Lectura** o superior para **Acceder a ESET Inspect** o permiso de **Lectura** o superior para el usuario **ESET Inspect**.

- Cree certificados utilizados durante la Instalación del servidor ESET Inspect.

- ActivarESET Inspect On-Prem en un dispositivo conectado a ESET PROTECT On-Prem. Necesita una licencia ESET Inspect On-Prem para activar ESET Inspect On-Prem.

Si ha actualizado el ESET PROTECT servidor, reinicie el servicio Server ESET Inspect para garantizar que todos los futuros cambios en ESET PROTECT On-Prem (por ejemplo, actualizaciones de permisos) se reflejen en ESET Inspect On-Prem.

Implementar el conector ESET Inspect en equipos administrados

Haga clic en **Equipos** > haga clic en un equipo o seleccione más equipos, y haga clic en **Equipo** > **Soluciones** > **Habilitar ESET Inspect On-Prem** para implementar el conector ESET Inspect en los equipos

Windows/Linux/macOS administrados.

Generar informes de detecciones de ESET Inspect On-Prem en ESET PROTECT On-Prem.

Si usted agrega un dispositivo que ejecuta el ESET Inspect Connector (debidamente configurado y conectado a ESET Inspect Servidor) a ESET PROTECT On-Prem, ESET Inspect On-Prem informa las detecciones detectadas en la sección ESET PROTECT On-Prem Detecciones. Puede filtrar estas detecciones seleccionando la categoría de detección de **ESET Inspect**.

Otro tipo de detecciones notificadas por ESET Inspect On-Prem son **Archivos bloqueados**: los intentos bloqueados de lanzar ejecutables bloqueados en ESET Inspect On-Prem (hashes bloqueados).

Administrar ESET Inspect detecciones en ESET PROTECT On-Prem

Haga clic en la detección y seleccione **Investigar (Inspect)** para ver los detalles de la detección en la consola web de ESET Inspect On-Prem.

Asegúrese de usar los navegadores web y los productos de ESET compatibles para permitir la administración de detecciones ESET Inspect en la consola web de ESET PROTECT.

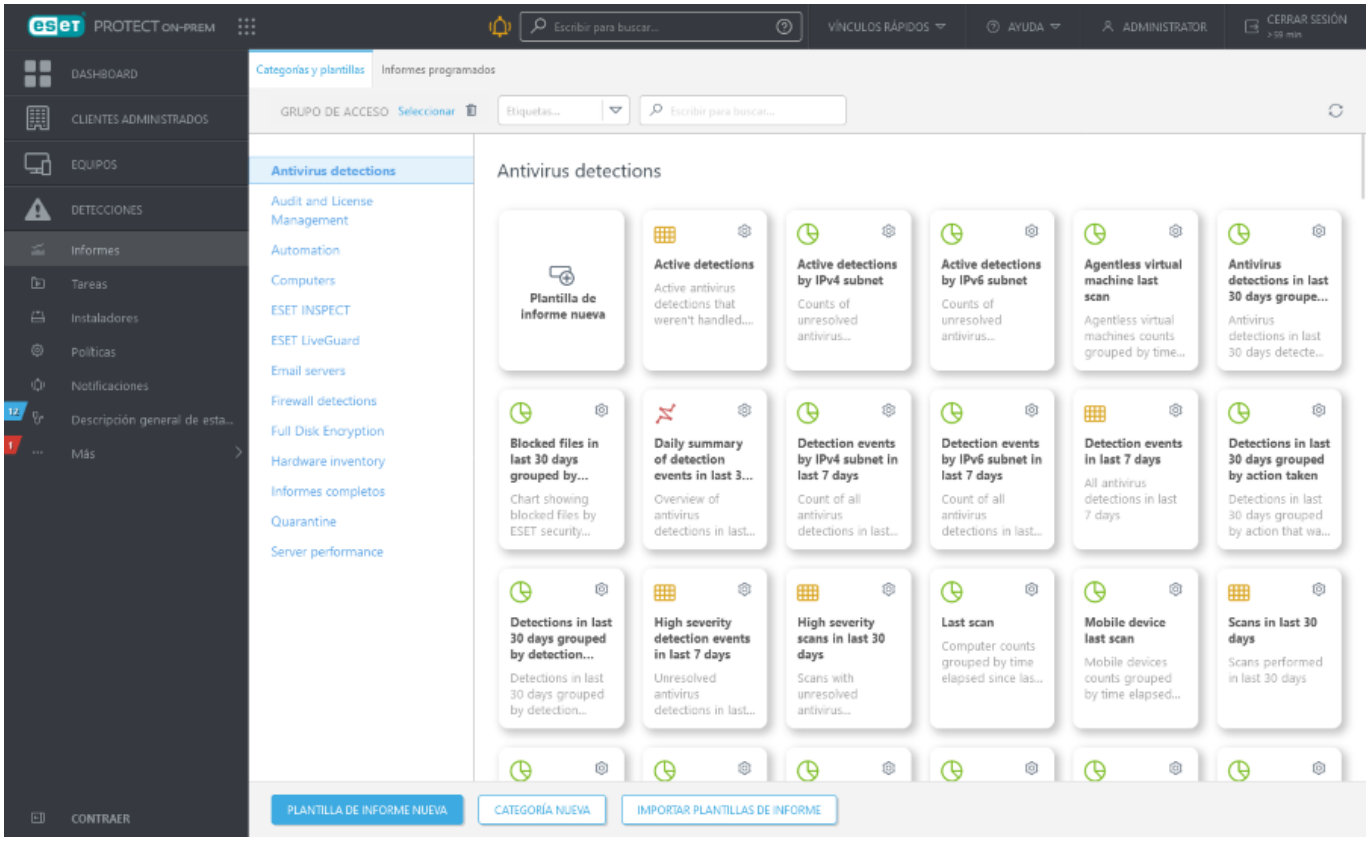
La integración de las detecciones ESET Inspect On-Prem en la consola web de ESET PROTECT le permite administrar las detecciones ESET Inspect directamente desde la consola web de ESET PROTECT sin abrir la consola web de ESET Inspect On-Prem. Por ejemplo, si marca la detección como resuelta en la Consola Web de ESET PROTECT, también se marca como resuelta en la Consola Web de ESET Inspect On-Prem y viceversa.

Informes

Los informes le permiten acceder a los datos y filtrarlos desde la base de datos en forma conveniente. La ventana de informes consta de dos pestañas:

- **Categorías y plantillas**: esta es la pestaña predeterminada para la sección **Informes**. Incluye una descripción general de las categorías de informes y plantillas. Puede crear nuevos informes y categorías o realizar otras acciones relacionadas con el informe aquí.

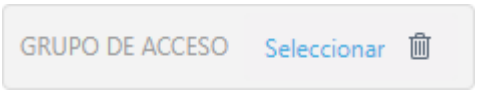
- **Informes programados**: esta pestaña proporciona una descripción general de los informes programados, también puede programar un nuevo informe aquí.



Los informes se generan a partir de plantillas clasificadas por tipo de informe. Se puede generar un informe de inmediato o se puede programar para generarlo más tarde. Para generar y ver el informe de inmediato, haga clic en **Generar ahora** junto a la plantilla de informes deseada. Puede usar plantillas de informe predefinidas de la lista de Categorías y plantillas, o puede crear una plantilla de informe nueva con una configuración personalizada. Haga clic en Plantilla de informe nueva para abrir un asistente de plantilla de informes y especificar la configuración personalizada para el nuevo informe. También puede crear una nueva categoría de informe (**Nueva categoría**) o importar plantillas de informes previamente exportadas (**Importar plantillas de informes**).

Hay una barra de búsqueda en la parte superior de la página. Puede buscar los nombres de la categoría y la plantilla, no las descripciones.

Puede usar etiquetas para filtrar los elementos mostrados.



El botón de filtro **Grupo de acceso** le permite a los usuarios seleccionar un grupo estático y filtrar los objetos mostrados en función del grupo en el que se encuentran.

Usar las plantillas de informes

Seleccione una plantilla de informe y haga clic en el ícono del engranaje del título de la plantilla de informe. Se encuentran disponibles las siguientes opciones:

Generar ahora	Se generará el informe y usted podrá revisar los datos de salida.

Descargar	Haga clic en **Descargar** para generar y descargar el informe. Puede seleccionar entre *.pdf* o *.csv*. CSV es apto únicamente para datos de tablas y usa ; (punto y coma) como delimitador Si descarga un informe de CSV y ve los números en una columna en la que esperaba ver texto, le recomendamos descargar un informe de PDF para ver los valores de texto.
Programar	Programar informe: puede modificar el desencadenador programado, la limitación y la entrega del informe. Puede encontrar todos los informes programados en la **pestaña Informes programados**.
Editar	Edite una plantilla de informe existente. Se aplican las mismas opciones y la misma configuración utilizadas para crear una plantilla de informe nueva.
Registro de auditoría	Ver el registro de auditoría del elemento seleccionado.
Duplicar	Crea un nuevo informe basado en el informe seleccionado (se requiere un nuevo nombre para el duplicado).
Eliminar	Elimina por completo la plantilla de informe seleccionada.
Exportar	La plantilla de informes se exportará a un archivo .dat.

Usar las categorías de informes

Seleccione una categoría de informes y haga clic en el icono en la esquina derecha de la categoría. Se encuentran disponibles las siguientes opciones:

Categoría nueva	Ingrese un **Nombre** y una cree una nueva categoría de plantillas de informes.
Plantilla de informe nueva	Cree una nueva plantilla de informe personalizada.
Eliminar	Elimina, por completo, la plantilla de informes seleccionada.
Editar	Cambia el nombre de la categoría de la plantilla de informes existente.
Registro de auditoría	Ver el registro de auditoría del elemento seleccionado.
Exportar	La categoría de plantilla de informes y todas las plantillas incluidas se exportarán a un archivo *.dat*. Luego, puede importar la categoría con todas las plantillas haciendo clic en **Importar plantillas de informes**. Esto es útil, por ejemplo, cuando desea migrar sus plantillas personalizadas de informes a otro servidor ESET PROTECT.
Grupo de acceso > **Mover**	Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen derechos suficientes para el grupo de destino. Cambiar el grupo de acceso es útil cuando se resuelven problemas de acceso con otros usuarios. El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario.

La función **Importar**/**Exportar plantillas de informe** está diseñada para importar y exportar plantillas de informes solamente, no un informe generado existente con sus datos.

Permisos para informes

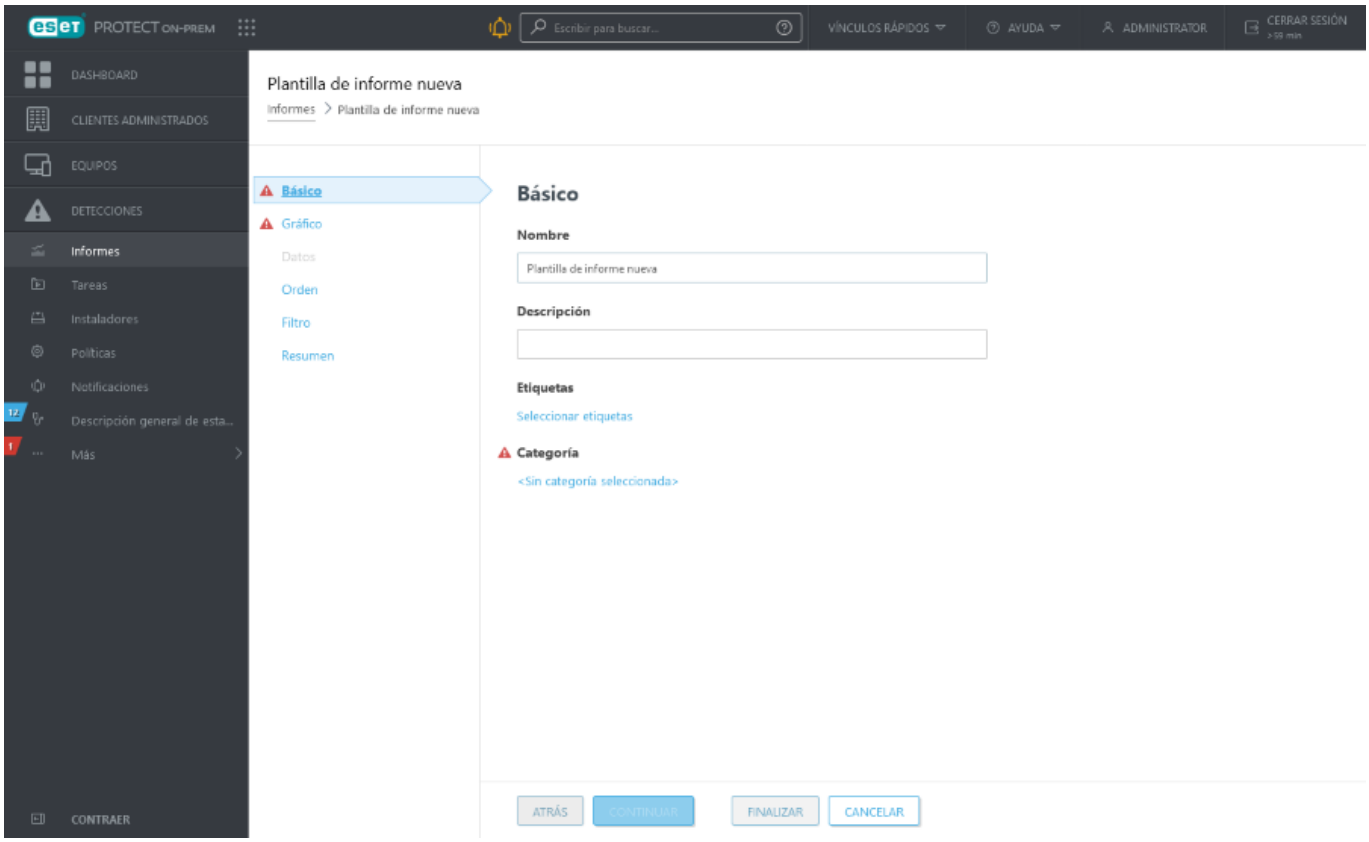
Los informes son objetos estáticos que residen en una estructura de objetos en la base de datos ESET PROTECT. Cada plantilla de informes nueva se almacena en el grupo hogar del usuario que lo creó. Para acceder a un informe, necesita los permisos con la funcionalidad **Informes y dashboard**. También necesita permisos para los objetos que son inspeccionados por el informe. Por ejemplo, si genera el informe **Descripción general de estados del equipo**, solo habrá datos de los equipos donde tenga el permiso de **Lectura**.

- **Lectura**: el usuario puede enumerar las plantillas de informes y sus categorías, generar informes basados en plantillas de informes y leer su tablero
- **Uso**: el usuario puede modificar su propio tablero con las plantillas de informes disponibles
- **Escritura**: crear/modificar/quitar plantillas y sus categorías

Todas las plantillas predeterminadas se encuentran en el grupo **Todos**.

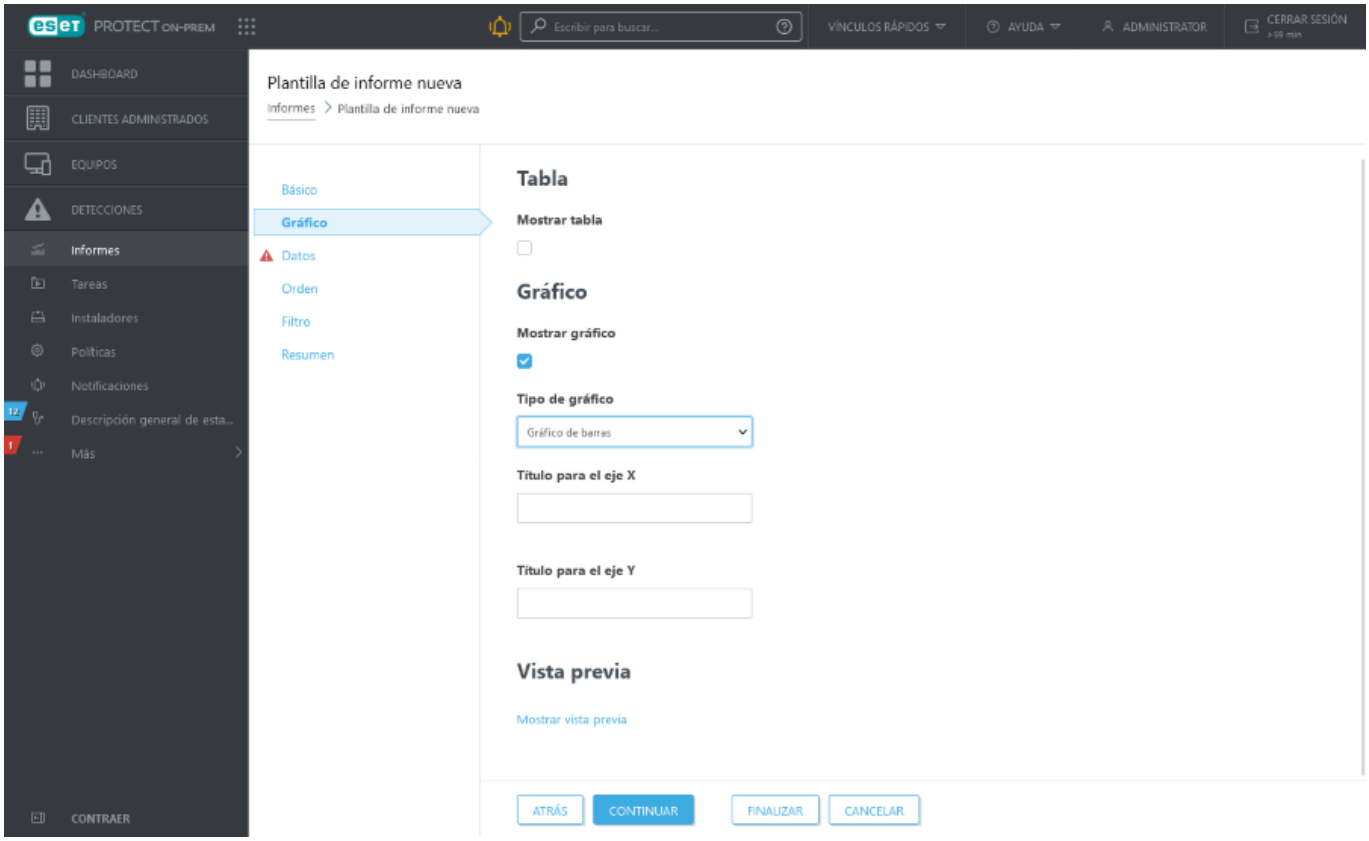
Creación de una plantilla de informe nueva

Vaya a Informes y haga clic en **Nueva plantilla de informe**.



Básica

Edite la información básica sobre la plantilla. Ingrese un **Nombre**, una **Descripción** y una **Categoría**. Solo puede elegir entre categorías predefinidas. Si desea crear una nueva categoría, use la opción **Nueva categoría** (descrita en el capítulo anterior). Haga clic en **Seleccionar etiquetas** para asignar etiquetas.



Gráfico

En la sección **Gráfico**, seleccione el tipo de **Informe**. Ya sea una **Tabla**, donde la información se ordena en filas y columnas, o un **Gráfico**, que representa los datos que usan un eje X e Y.

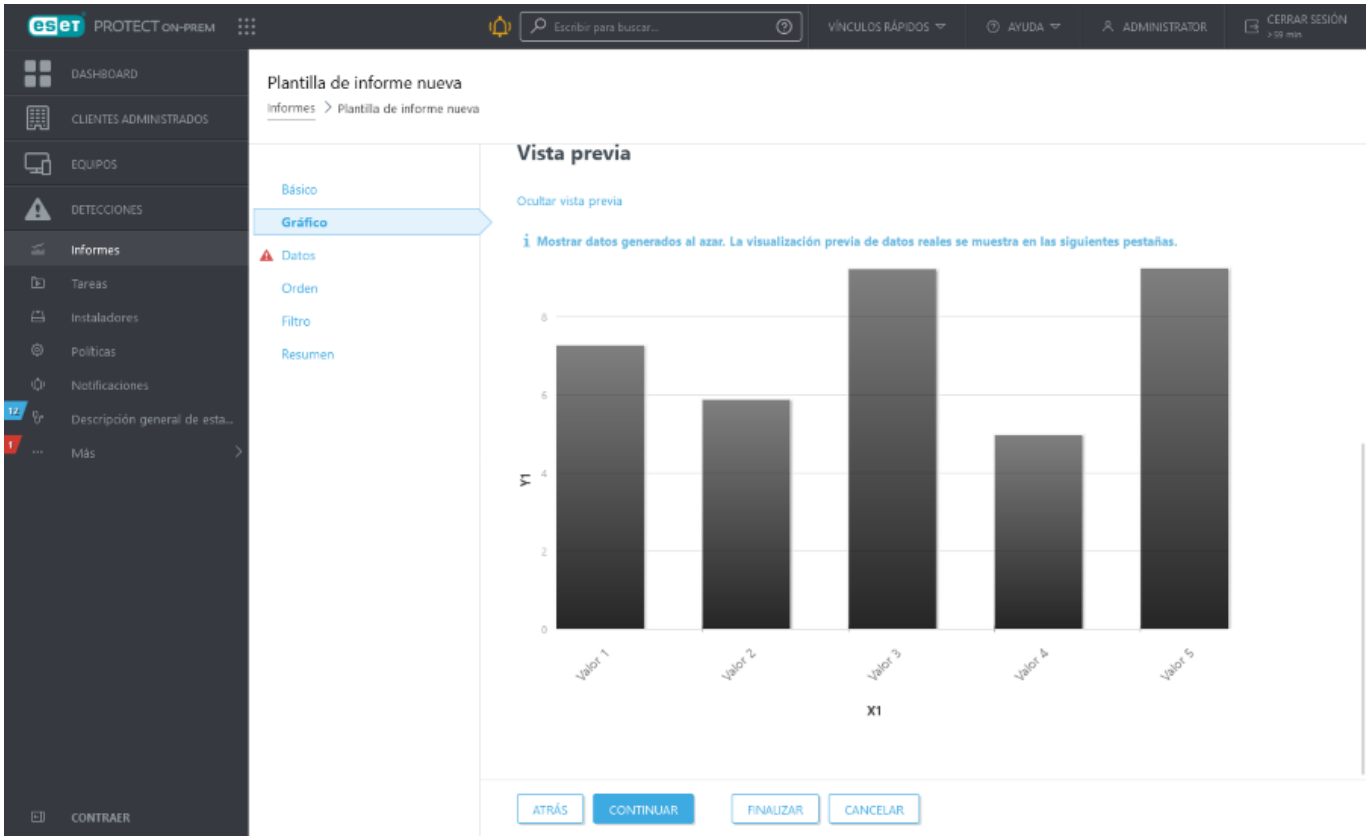
El tipo de gráfico seleccionado se visualizará en la sección **Vista previa**. De esta manera, puede ver cómo se verá el informe en tiempo real.

La selección de un **Gráfico** le ofrece múltiples opciones:

- **Gráfico de barras**: un gráfico con barras rectangulares proporcionales a los valores que representan.
- **Gráfico de puntos**: en este gráfico, los puntos se usan para mostrar valores cuantitativos (similar a un gráfico de barras).
- **Gráfico circular**: es un gráfico circular dividido en sectores proporcionales, que representan valores.
- **Gráfico de anillos**: es similar a un gráfico circular, pero el gráfico de anillos puede contener múltiples tipos de datos.
- **Gráfico de líneas**: muestra la información como una serie de puntos de datos conectados por segmentos de líneas rectas.
- **Gráfico de líneas simples**: muestra la información como una línea basada en valores sin puntos de datos visibles.
- **Gráfico de líneas apiladas**: este tipo de gráfico se usa cuando desea analizar los datos en función de distintas unidades de medición.

• **Gráfico de barras apiladas**: es similar a un gráfico de barras simple, pero hay varios tipos de datos con distintas unidades de medición apilados en las barras.

De manera opcional, puede ingresar un título para el eje **X** e **Y** del gráfico para que le resulte más fácil leer el gráfico y reconocer las tendencias.



Datos

En la sección **Datos**, seleccione la información que desea visualizar:

a.**Columnas de tablas**: La información para la tabla se agrega automáticamente en función del tipo de informe seleccionado. Puede personalizar el **nombre**, la **etiqueta** y el **formato** (consulte a continuación).

b.**Ejes de gráfico**: Seleccione los datos para el eje **X** y el **Y**. Al hacer clic en **Agregar eje**, se abre una ventana con opciones. Las opciones disponibles para el eje **Y** siempre dependen de la información seleccionada para el eje **X** y viceversa, porque el gráfico muestra su relación y los datos deben ser compatibles. Seleccione la información deseada y haga clic en **Aceptar**.

Formato

Haga clic en el símbolo ⤢ en la sección **Datos** para ver las opciones de formato extendidas. Puede cambiar el **Formato** en el que se visualizan los datos. Puede ajustar el formato de **Columnas de tablas** y **Ejes de gráfico**. No todas las opciones están disponibles para cada tipo de datos.

Columna de formato	Elija una columna según la cual se formateará la columna actual. Por ejemplo, al formatear la columna **Nombre**, elija la columna **Severidad** para agregar iconos de gravedad junto a los nombres.
Valor mínimo	Establezca el límite mínimo para los valores mostrados.

Valor máximo	Establezca el límite máximo para los valores que se muestran.
Color	Elija el tema de color para la columna. El color se ajusta de acuerdo con el valor de la columna seleccionada en la **Columna de formato**.
Iconos	 Agregue iconos a la columna formateada según el valor de la **Columna de formato**.

Haga clic en una de las flechas  para cambiar el orden de las columnas.

Ordenación

Si los datos seleccionados en la sección **Datos** contiene un símbolo clasificable, entonces la ordenación está disponible. Haga clic en **Agregar ordenación** para definir la relación entre los datos seleccionados. Seleccione la información de partida (valor de ordenación) y el método de ordenación, **Ascendente** o **Descendente**. Esto definirá el resultado mostrado en el gráfico. Haga clic en **Arriba** o **Abajo** para cambiar el orden de los elementos de clasificación. Haga clic en el icono de la papelera  para eliminar el elemento de la selección.

Filtro

Defina el método de filtrado. Haga clic en **Agregar filtro** y seleccione el elemento de filtrado de la lista y su valor. Esto define qué información se visualizará en el gráfico. Haga clic en el icono de la papelera  para eliminar el elemento de la selección.

Resumen

En el **Resumen**, revise las opciones y la información seleccionadas. Haga clic en **Finalizar** para crear una **plantilla de informe**.

Generar informe

Existen distintas formas de generar un informe desde una plantilla de informe al instante:

- Vaya a **Enlaces rápidos** en la barra superior y haga clic en **Generar informe**. Seleccione una plantilla de informe existente y haga clic en **Generar ahora**.

- Haga clic en **Informes** y selecciona la pestaña **Categorías y plantillas**. Seleccione una plantilla de informe desde donde desea generar un informe. Haga clic en el ícono del engranaje y luego en **Editar** si desea realizar cambios en la plantilla.

  - Puede hacer clic en el título del informe para generar y ver el informe en la consola web de ESET PROTECT. Cuando se haya generado el informe, puede hacer clic en **Generar y descargar** para guardar el informe en el formato que desea. Puede seleccionar entre *.pdf* o *.csv*. CSV es apto únicamente para datos de tablas y usa `;` (punto y coma) como delimitador Si descarga un informe de CSV y ve los números en una columna en la que esperaba ver texto, le recomendamos descargar un informe de PDF para ver los valores de texto.

- Vaya a **Tareas** > **Nueva** > **Tarea de servidor** para crear una nueva tarea Generar informe.

- La tarea se crea y se visualiza en la lista **Tipos de tareas**. Seleccione esta tarea y haga clic en **Ejecutar ahora** en la parte inferior de la página. La tarea se ejecutará de inmediato.
- Configure los valores (como se describe en la tarea Generar informe) y haga clic en **Finalizar**.

> Cuando hace clic en un elemento dentro en un informe en ESET PROTECT Consola web, aparece un menú de exploración en profundidad con opciones adicionales.

Plantilla de informe MDR

El informe MDR es un informe de seguridad para proveedores de detección y respuesta administradas.

Un usuario necesita un conjunto de permisos con la funcionalidad de **Informes completos** (administrador/revisor/conjunto de permisos personalizados) para generar la plantilla de informe MDR:

1. Haga clic en **Informes** y selecciona la pestaña **Categorías y plantillas**.
2. Haga clic en **Informes completos** y haga clic en **Plantilla de informe MDR**.
3. Haga clic en **Generar y descargar**. Puede generar la plantilla de informe MDR solo como un archivo .odt.

Necesita una licencia ESET Inspect On-Prem para ver los incidentes ESET Inspect en la plantilla de informe MDR.

Programación de un informe

Existen distintas formas de programar la generación de informes:

- Vaya a **Tareas** > **Nueva** > **Tarea de servidor** para crear una nueva tarea Generar informe.
- Vaya a **Informes**, seleccione una plantilla de informe desde donde desea generar un informe, haga clic en el ícono en el recuadro de la plantilla y seleccione **Programar**. Puede usar y editar una plantilla de informe predefinida, o crear una plantilla de informe nueva.
- Haga clic en **Programar** en el menú contextual de la plantilla de informe en un tablero.
- Vaya a **Informes** > pestaña**Informes programados** > haga clic en **Programar informe**.

> Cuando programa un informe, tiene múltiples opciones, como se describe en la tarea Generar informe:
> - Puede seleccionar múltiples plantillas de informe para un informe.
> - Los usuarios de MSP pueden filtrar el informe seleccionando el cliente.
> - Configure la entrega de informes en un correo electrónico y/o guárdela en un archivo.
> - Opcionalmente, puede configurar parámetros de desencadenadores y límites.

Luego de que se haya programado el informe, haga clic en **Finalizar**. La tarea se crea y se ejecutará en el intervalo definido en el desencadenador (una vez o en reiteradas ocasiones) y en función de la configuración limitada (opcional).

Pestaña Informes programados.

Puede ver sus informes programados en **Informes > Informes programados**. A continuación, se muestran otras

acciones disponibles en esta pestaña:

Programar	Crea un nuevo programa para un informe existente.
Mostrar detalles	Muestra información detallada acerca del programa seleccionado.
Registro de auditoría	Ver el registro de auditoría del elemento seleccionado.
Etiquetas	Editar etiquetas (asignar, desasignar, crear, quitar).
Ejecutar ahora	Ejecuta el informe programado ahora.
Editar	Edita el programa del informe. Puede agregar o eliminar la selección de plantillas de informes, modificar configuraciones de programas o editar la configuración de límite y entrega del informe.
Duplicar	Crea un programa duplicado en su grupo hogar.
Eliminar	Elimina el programa. La plantilla de informe permanecerá.
Grupo de acceso > **Mover**	Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen derechos suficientes para el grupo de destino. Cambiar el grupo de acceso es útil cuando se resuelven problemas de acceso con otros usuarios. El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario.

Personalización del diseño y de los filtros

Puede personalizar la vista de la pantalla de la consola web actual:

- Administre el panel lateral y la tabla principal.
- Agregar filtro y filtros preestablecidos. Puede usar etiquetas para filtrar los elementos mostrados.

Aplicaciones obsoletas

Use el informe de **aplicaciones obsoletas** (ubicado en **Informes** > categoría **Equipos**) para visualizar cuáles son los componentes de ESET PROTECT que no están actualizados.

Existen dos métodos para ejecutar este informe:

- Agregar un Tablero nuevo o modificar uno de los paneles existentes del tablero.
- Vaya a la categoría **Informes** > **Equipos** > el recuadro **Aplicaciones obsoletas** > haga clic en **Generar ahora**.

Si encontró una aplicación obsoleta, puede:

- Usar la Tarea del cliente ESET PROTECT Actualización de componentes para actualizar el agente ESET Management, servidor y MDM.
- Use la Tarea del cliente Instalación de software para actualizar su producto de seguridad.

Visor de registros de SysInspector

Usando el Visor de registros de SysInspector, podrá ver los registros de SysInspector después de ejecutarlo en un equipo cliente. También puede abrir registros de SysInspector directamente de una Tarea de solicitud de registro de SysInspector después de que se haya ejecutado con éxito. Los archivos de registro se pueden descargar y ver en SysInspector en su máquina local.

ESET SysInspector solo se ejecuta en equipos Windows.

Cómo ver el registro de SysInspector

Desde un tablero

1.Agregue un Tablero nuevo o modificar un informe de tablero existente.

2.Seleccione la plantilla de informe **Automatización** > **Historial de instantáneas de SysInspector en los últimos 30 días**.

3.Abra el informe, seleccione un equipo y, luego, seleccione **Abrir el visor de registros de SysInspector** desde el menú desplegable.

Desde un informe

1.Vaya a la categoría Informes > **Automatización**.

2.Seleccione la plantilla **Historial de instantáneas de SysInspector en los últimos 30 días** de la lista y haga clic en **Generar ahora**.

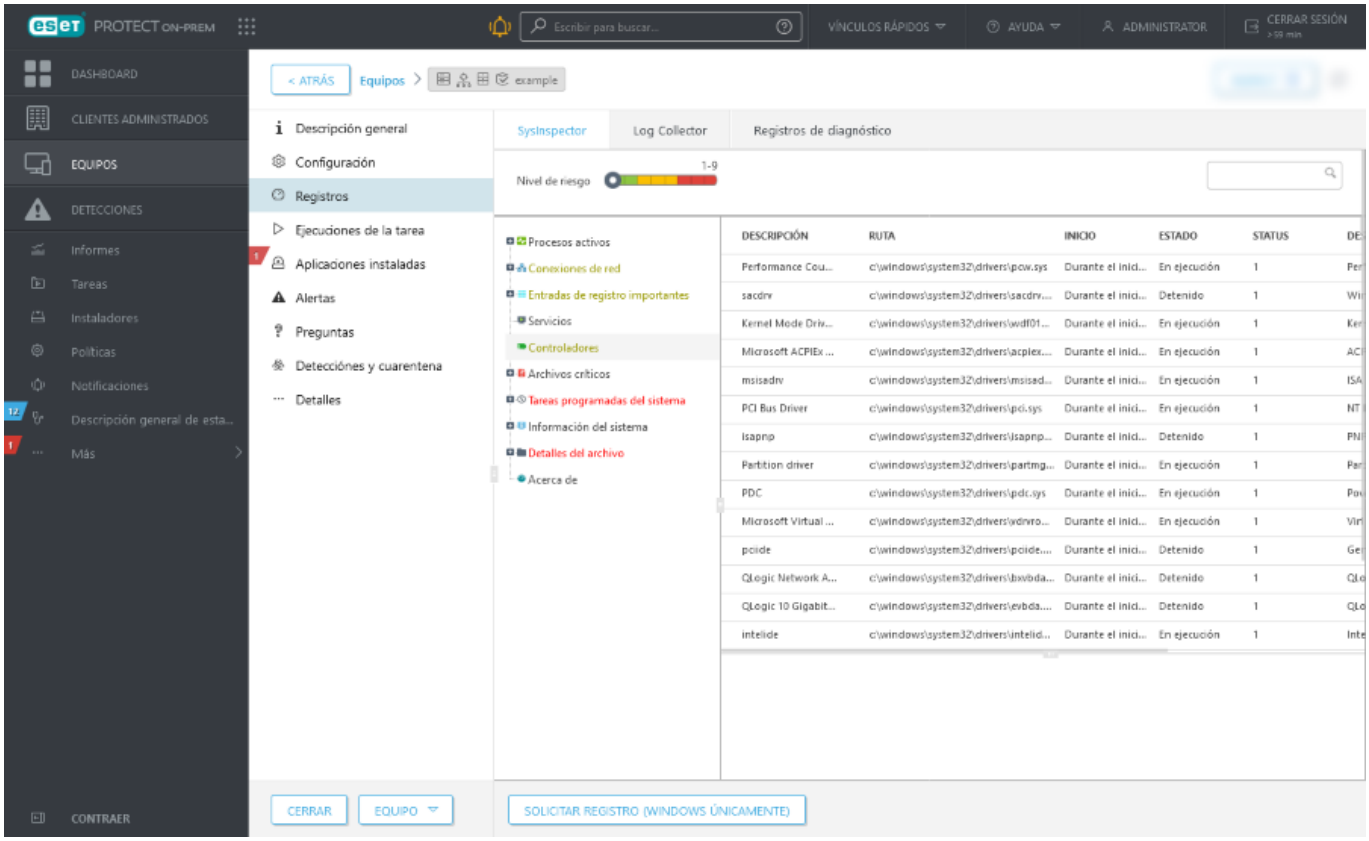
3.Abra el informe, seleccione un equipo y, luego, seleccione **Abrir el visor de registros de SysInspector** desde el menú desplegable.

Desde el menú Equipos

1.Vaya a Equipos.

2.Seleccione un equipo en un grupo estático o dinámico y haga clic en **Mostrar detalles**.

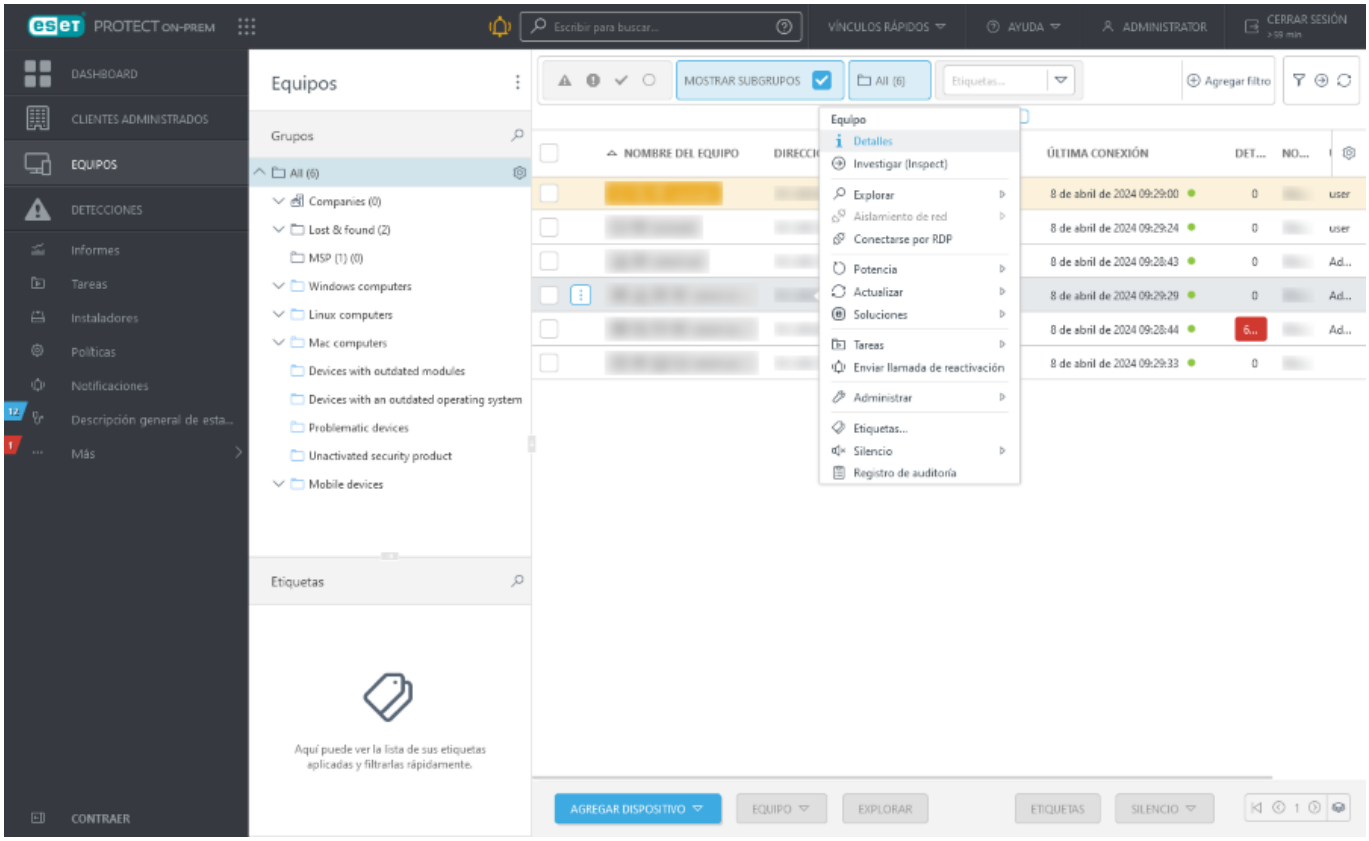
3.Vaya a la sección **Registros** >, pestaña **SysInspector** y haga clic en una entrada de la lista y seleccione **Abrir el Visor de registros de SysInspector**.



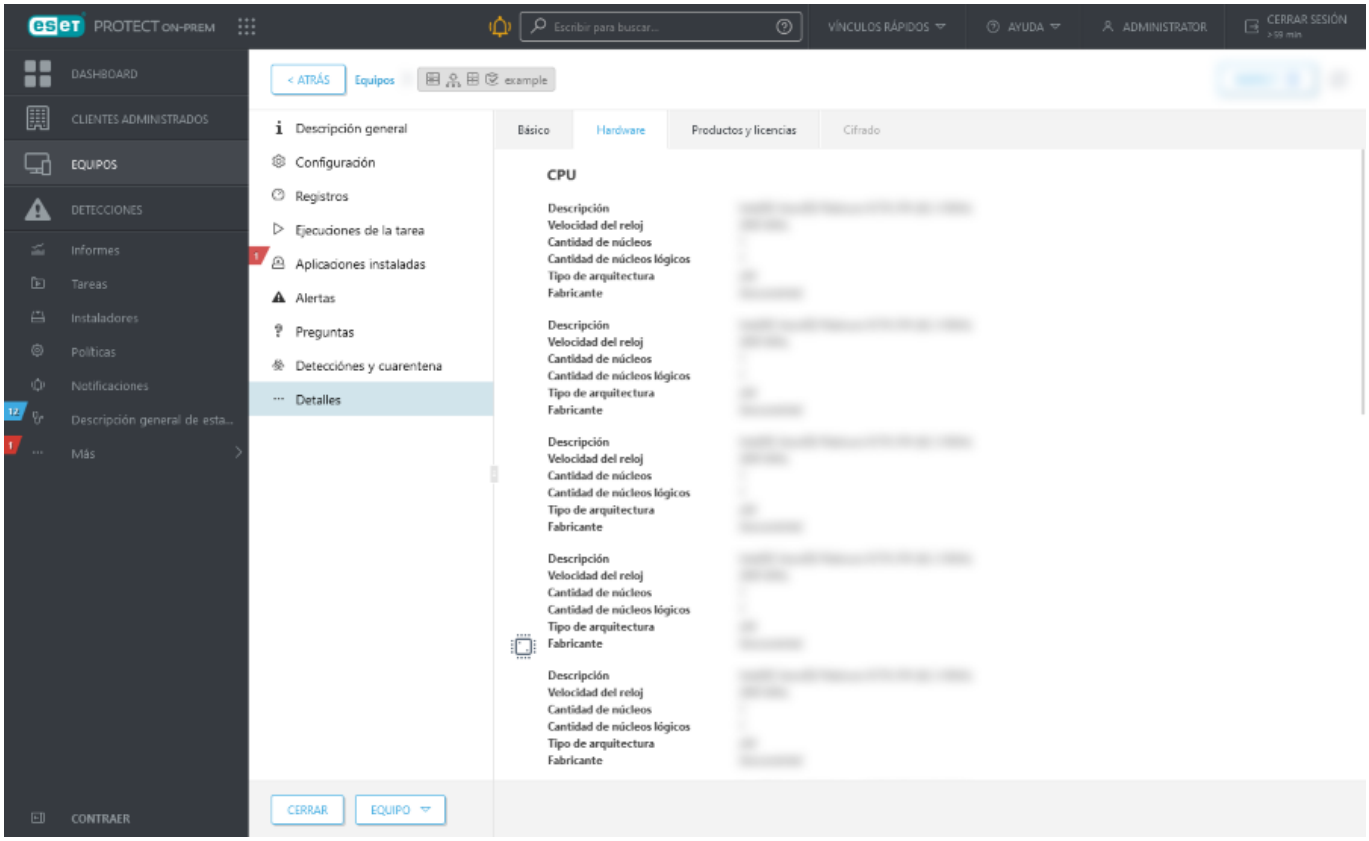
Inventario de hardware

ESET PROTECT On-Prem tiene la capacidad para recuperar detalles de inventario de hardware desde dispositivos conectados, como información sobre la memoria RAM de un dispositivo, su almacenamiento y procesador.

Haga clic en **Equipos**, haga clic en un dispositivo conectado y seleccione **Detalles**.



Haga clic en **Detalles** y seleccione la pestaña **Hardware**.



Informes de inventario de hardware

Puede encontrar informes predefinidos de inventarios de hardware en **Informes** > **Inventario de hardware**. Puede crear informes de inventario de hardware personalizados. Cuando cree una Plantilla de informe nueva, en

Datos, seleccione una subcategoría desde uno de los filtros de **Inventario de hardware**. Cuando agregue la primera columna de la tabla o en el eje X, solo datos compatibles serán elegibles para la selección.

Grupos dinámicos basados en inventario de hardware

Puede crear grupos dinámicos personalizados basados en la información del Inventario de hardware de los dispositivos conectados. Al crear una Plantilla nueva de grupo dinámico, seleccione regla(s) desde las categorías del **inventario de hardware** para filtrar los dispositivos conectados en función de parámetros de hardware.

También puede seleccionar desde las siguientes categorías de Inventario de hardware: Chasis, Información de Dispositivo, Pantalla, Adaptador de Pantalla, Dispositivo de Entrada, Almacenamiento en Masa, Adaptador de Red, Impresora, Procesador, RAM y Dispositivo de Sonido. Por ejemplo, puede crear un grupo dinámico con dispositivos filtrados por la capacidad de su RAM para obtener un resumen de los dispositivos con una cierta cantidad de RAM.

Sistemas operativos compatibles con el inventario de hardware

La función de inventario de hardware está disponible en todos los equipos Windows, Linux* y macOS compatibles.

* 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`

Informe de registro de auditoría

El informe de **registro de auditoría** contiene todas las acciones y cambios realizados por los usuarios en el servidor de ESET PROTECT.

Para ejecutar este informe, haga clic en **Informes** > categoría **Auditoría y administración de licencias** > **Registro de auditoría**.

Puede ver y filtrar un registro de auditoría directamente en la consola web, ubicada debajo de **Más** > **Registro de auditoría**.

Para ver el registro de auditoría, el usuario de la consola web debe tener un conjunto de permisos con la funcionalidad **Registro de auditoría**.

Tareas

Puede utilizar **Tareas** para administrar ESET PROTECT Server, los equipos cliente y sus productos ESET. Las Tareas pueden automatizar trabajos de rutina. Existe un conjunto de tareas predefinidas que abarcan los escenarios más comunes; o puede crear una tarea personalizada con configuraciones específicas. Utilice las tareas para solicitar una acción de los equipos cliente. Para ejecutar una tarea con éxito, es necesario contar con los derechos de

acceso suficientes para la tarea y los objetos (dispositivos) que utiliza la tarea. Consulte la lista de permisos para obtener más información sobre los derechos de acceso.

Existen dos categorías principales de tareas: Tareas de clientes y Tareas del servidor.

- Puede asignar Tareas de clientes a grupos o equipos individuales. Una vez creadas, las tareas son ejecutadas mediante un Desencadenador. Una Tarea de cliente puede tener más desencadenadores configurados. Las Tareas de cliente se distribuyen a los clientes cuando el agente ESET Management en un cliente se conecta al servidor de ESET PROTECT. Por esta razón, puede llevar algún tiempo devolver los resultados de ejecución de tareas al servidor de ESET PROTECT. Puede administrar el intervalo de conexión del agente ESET Management para reducir los tiempos de ejecución de tareas.

- ESET PROTECT Server se ocupa de ejecutar las tareas del servidor en sí mismo o en otros dispositivos. Las tareas del servidor no se pueden asignar a ningún cliente o grupo de clientes específicos. Cada tarea del servidor puede tener un desencadenador configurado. Si la tarea debe ser ejecutada con varios eventos, se necesita contar una tarea del servidor diferente para cada desencadenador.

Puede crear una nueva tarea de dos maneras:

- Haga clic en **Nuevo** > **Tarea de cliente** o **Tarea del servidor**.

- Seleccione el tipo de tarea deseada a la izquierda y haga clic en **Nuevo** > Tarea de cliente o Tarea del servidor.

Para su comodidad se encuentran disponibles las siguientes tareas predefinidas (cada Categoría de tarea posee Tipos de tareas):

Todas las tareas

Tareas de clientes

Producto de seguridad ESET

Buscar actualizaciones del producto
Diagnósticos
Finalizar aislamiento del equipo de la red
Exportación de la configuración de productos administrados
Aislar equipo de la red
Actualización de módulos
Reversión de actualizaciones de módulos
Exploración bajo demanda
Activación del producto
Administración de cuarentena
Ejecución del script de SysInspector
Enviar archivo a ESET LiveGuard
Exploración del servidor
Instalación de software
Solicitud de registro de SysInspector (Windows únicamente)
Carga de archivo en cuarentena

ESET PROTECT

Diagnósticos
Restablecimiento del agente clonado
Restablecimiento de la base de datos del Rogue Detection Sensor
Actualización de componentes de ESET PROTECT
Detener administración (desinstalar agente ESET Management)

Sistema operativo

Visualización de mensajes
Cerrar sesión
Actualización de sistema operativo
Ejecución de comando
Apagar el equipo
Instalación de software
Desinstalación de software
Detener administración (desinstalar agente ESET Management)

Móvil

Acciones Anti-Theft
Visualización de mensajes
Exportación de la configuración de productos administrados
Actualización de módulos
Exploración bajo demanda
Activación del producto
Instalación de software
Detener administración (desinstalar agente ESET Management)

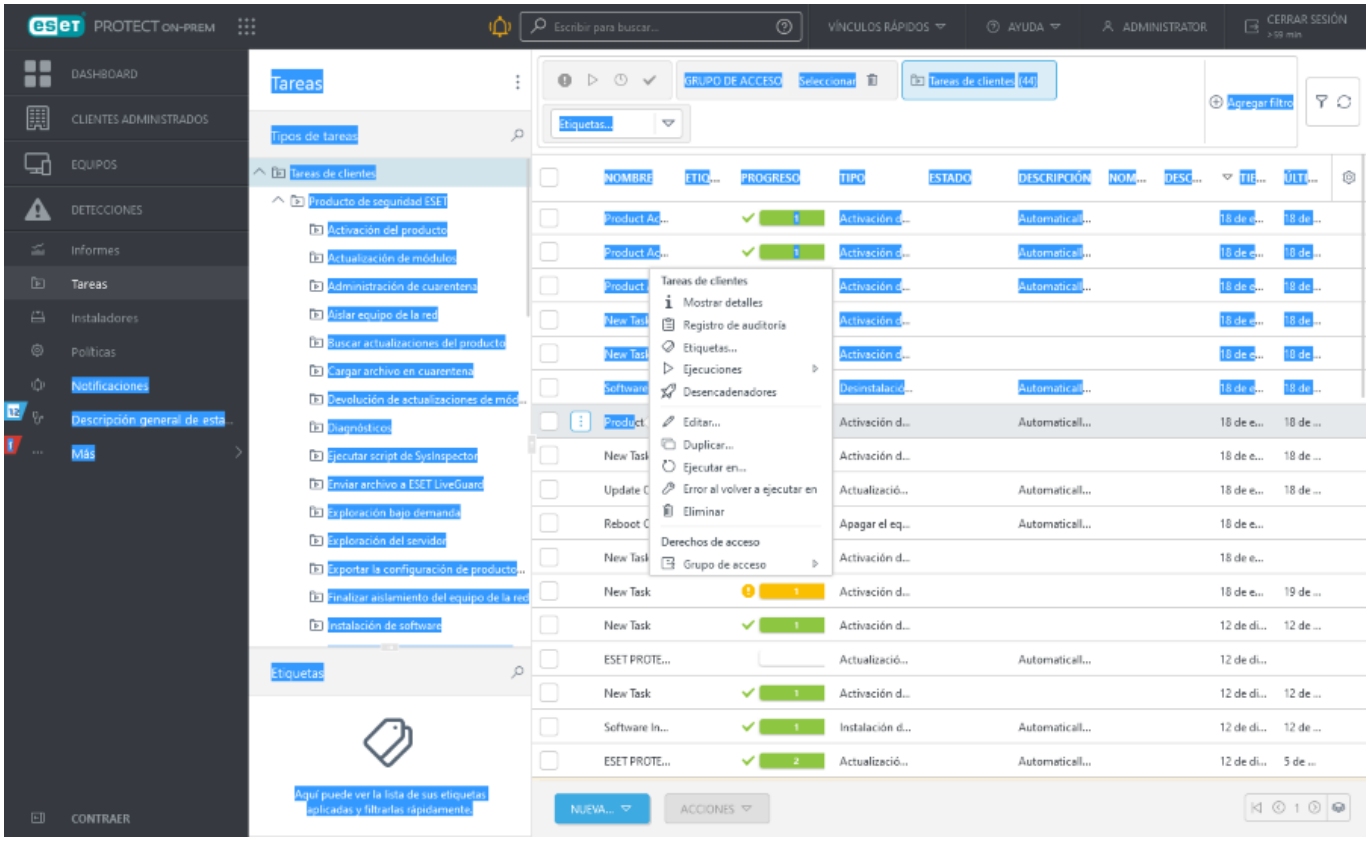
Tareas del servidor

Implementación del agente: distribuye el Agente a los equipos cliente.
Eliminar equipos sin conexión elimina los clientes que ya no se conectan a ESET PROTECT On-Prem desde la consola web.
Generar informe se usa para generar los informes a medida que se los necesita.
Cambiar el nombre de los equipos esta tarea cambiará periódicamente el nombre de los equipos usando el formato FQDN.
Sincronización de grupo estático actualiza la información del grupo para mostrar los datos actuales.
Sincronización de usuarios: actualiza el usuario o grupo de usuarios.

Información general de las tareas

En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Debe crear un Desencadenador para ejecutar una tarea de cliente.



Haga clic en una tarea para realizar otras acciones relacionadas con la tarea:

Mostrar detalles	Ver detalles de la tarea: resumen, ejecuciones, desencadenadores (los detalles del desencadenador se encuentran disponibles únicamente para tareas de clientes).
Registro de auditoría	Ver el registro de auditoría del elemento seleccionado.
Etiquetas	Editar etiquetas (asignar, desasignar, crear, quitar).
Ejecuciones	Solo tareas de cliente: Puede seleccionar desde los resultados de ejecución de la tarea y realizar otras acciones, de ser necesario; para más detalles, consulte Detalles de la tarea.
Desencadenadores	Solo tareas de cliente: Vea la lista de Desencadenadores para la tarea del cliente seleccionada.
Editar	Edite la tarea seleccionada. Editar las tareas existentes es útil solo cuando necesita realizar pequeños ajustes. Para más tareas únicas, puede preferir crear una nueva tarea.
Duplicar	Le permite crear un nueva tarea basada en la tarea seleccionada, se requiere un nuevo nombre para la duplicada.
Ejecutar ahora	Solo tareas del servidor: Ejecute la tarea del servidor seleccionada.
Ejecutar con	Solo tareas de cliente: Agregue un nuevo Desencadenador y seleccione los equipos o grupos de Destino para la tarea de cliente.

Error al volver a ejecutar en	Solo tareas de cliente: Crea un nuevo Desencadenador con todos los equipos que fallaron durante la ejecución de tareas anteriores establecidas como objetivos. Puede editar los parámetros de la tarea, si lo prefiere, o hacer clic en Finalizar para volver a ejecutar la tarea sin cambios.
Eliminar	Quita la(s) tarea(s) seleccionada(s) completamente. • Si se elimina la tarea después de haber sido creada pero antes del inicio programado, se quitará, no se ejecutará y nunca se iniciará. • Si se elimina la tarea después de la ejecución programada, la tarea se completará, pero no se mostrará la información en la Consola Web.
Grupo de acceso > **Mover**	Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen derechos suficientes para el grupo de destino. Cambiar el grupo de acceso es útil cuando se resuelven problemas de acceso con otros usuarios. El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario.

Personalización del diseño y de los filtros

Puede personalizar la vista de la pantalla de la consola web actual:

- Administre el panel lateral y la tabla principal.
- Agregar filtro y filtros preestablecidos. Puede usar etiquetas para filtrar los elementos mostrados.

Indicador de progreso

El indicador de progreso es una barra de color que muestra el estado de ejecución de una tarea. Cada tarea tiene su propio indicador (que se muestra en la fila **Progreso**). El estado de la ejecución de una tarea se muestra en colores diferentes e incluye la cantidad de equipos en dicho estado para una tarea específica:

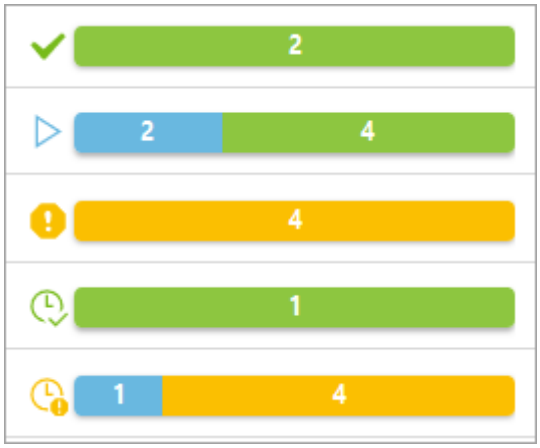
En ejecución (azul)

Finalizado con éxito (verde)

Fallido (naranja)

Tarea creada recientemente (blanco): es posible que el indicador demore un tiempo en cambiar de color, el servidor ESET PROTECT necesita recibir una respuesta de un ESET Management Agent para mostrar el estado de la ejecución. Además, el indicador de progreso estará de color blanco si no hay un Desencadenador asignado.

Una combinación de los anteriores:



Consulte el icono de Estado para obtener información sobre los diferentes tipos y estados de iconos.

El indicador de progreso muestra el estado de una tarea cuando se la ejecutó por última vez. Esta información proviene del agente ESET Management. El indicador de progreso indica exactamente lo que el agente ESET Management informa desde los equipos cliente.

Ícono de estado

El ícono junto al Indicador de progreso provee información adicional. Indica si existen ejecuciones planificadas para una tarea específica, como así también los resultados de las ejecuciones que se hayan completado. Esta información se enumera a través del servidor ESET PROTECT. Se pueden indicar los siguientes estados:

En ejecución	La tarea se está ejecutando en al menos un destino, no hay ejecuciones programadas ni con errores. Esto aplica incluso si la tarea ha finalizado en algunos destinos.
Éxito	La tarea ha finalizado de manera exitosa en todos los destinos, no hay ejecuciones programadas ni en ejecución.
Error	La tarea se ha ejecutado en todos los destinos, pero ha presentado errores en al menos uno. No hay más ejecuciones planificadas (programadas).
Planificada	Se ha planificado la ejecución de la tarea, pero no hay ejecuciones en curso.
Planificada/En ejecución	La tarea tiene ejecuciones programadas (pasadas o futuras). No ha fallado ninguna ejecución y hay al menos una ejecución actualmente en ejecución.
Planificada/Exitosa	La tarea aún tiene ejecuciones programadas (pasadas o futuras), no hay ejecuciones con errores ni en curso y al menos una ejecución ha finalizado exitosamente.
Planificada/Error	La tarea aún tiene ejecuciones programadas (pasadas o futuras), no hay ejecuciones en curso y al menos una ejecución ha finalizado con errores. Esto se aplica incluso si algunas ejecuciones se completaron de forma exitosa.

Detalles de tarea

Haga clic en una tarea y seleccione **Mostrar detalles** para ver los detalles de la tarea en las siguientes fichas:

Resumen

Esta ficha incluye la información general sobre la configuración de la tarea.

Ejecuciones

La pestaña **Ejecuciones** muestra una lista de equipos con los resultados de ejecución de la Tarea del cliente. La pestaña **Ejecuciones** no está disponible para Tareas del servidor.

Si hay demasiadas ejecuciones, puede filtrar la vista para restringir los resultados.

Haga clic en **Agregar filtro** para filtrar las ejecuciones seleccionadas por estado:

- **Planificado**: **sí** (Se ha planificado la ejecución de la Tarea del cliente), **no** (Se completó la ejecución de la Tarea del cliente).
- **Último estado** – **Sin estado**, **En ejecución**, **Finalizado**, **Error**

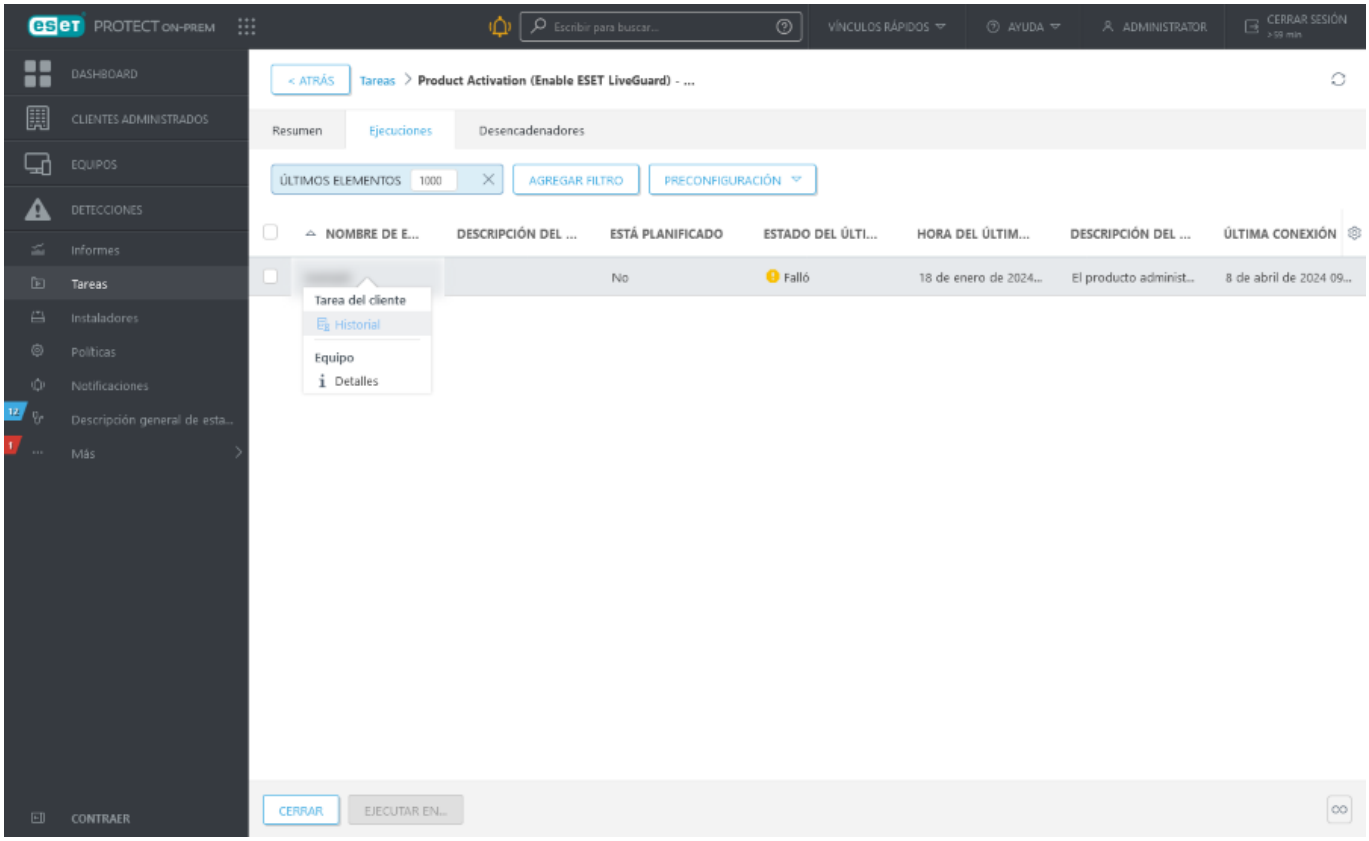
Puede modificar el filtro o apagarlo para ver todos los equipos sin importar su último estado.

Haga clic en una línea bajo el **Nombre del equipo** o **Descripción del equipo** para realizar más acciones:

- **Historial**: vea los detalles de ejecución de la Tarea del cliente, incluso cuándo **Ocurrió** la ejecución, el **Producto**, el **Estado del progreso**, la **Descripción del progreso** y el **Mensaje de seguimiento** (si está disponible). Puede utilizar el **Mensaje de seguimiento** para examinar la salida de la Tarea del cliente que ha fallado.

> - Si no ve ninguna entrada en la tabla **Historial**, intente configurar el filtro **Ocurrió** para acceder a una duración más extensa.
> - Al instalar productos de ESET anteriores, el mensaje de seguimiento mostrará el siguiente informe: **Tarea proporcionada al producto administrado.**

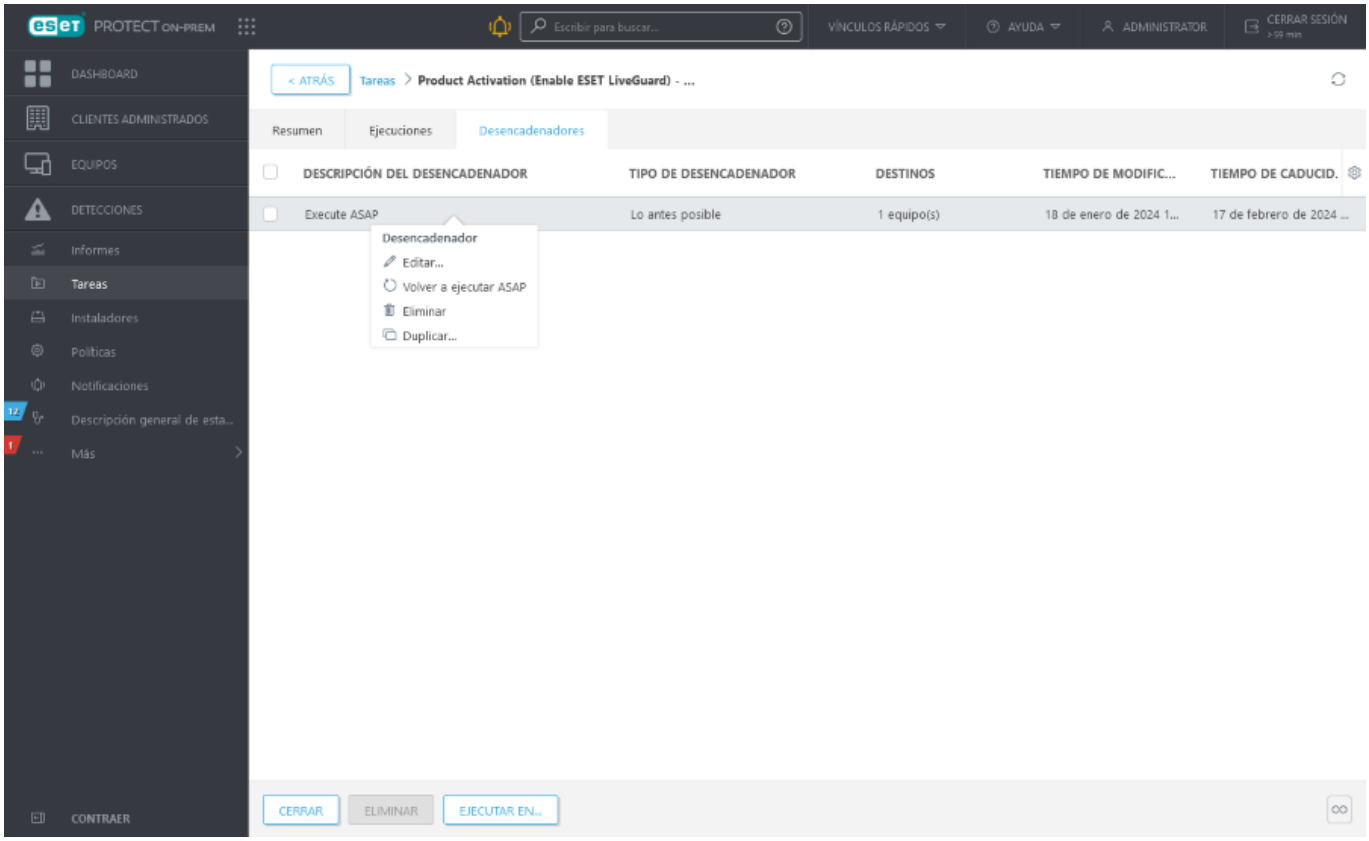
- **Detalles**: ver los detalles del equipo seleccionado.



Desencadenadores

La ficha **Desencadenadores** se encuentra disponible únicamente para tareas de cliente y muestra la lista de Desencadenadores para la tarea de cliente seleccionada. Para administrar el desencadenador, haga clic en el desencadenador y seleccione uno de los siguientes elementos:

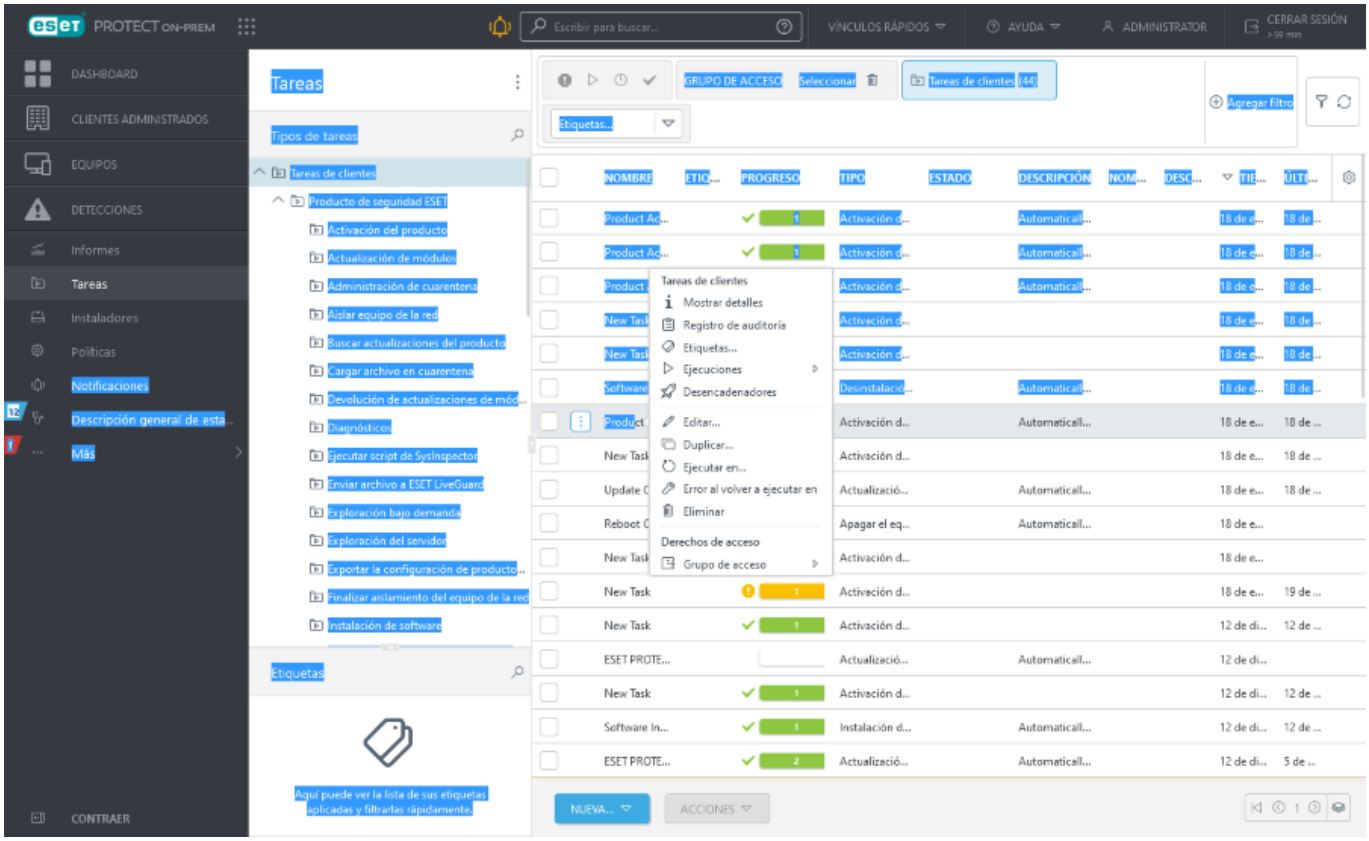
Editar	Edite el desencadenador seleccionado.
Volver a ejecutar ASAP	Ejecute la Tarea de cliente (ASAP) nuevamente mediante un Desencadenador existente directamente sin modificaciones.
Eliminar	Quita el desencadenador seleccionado completamente. Para quitar varios desencadenadores, seleccione las casillas de verificación ubicadas a la izquierda y haga clic en el botón **Quitar**.
Duplicar	Cree un nuevo Desencadenador basado en el seleccionado, se requiere de un nuevo nombre para el duplicado.



Tareas de clientes

Puede asignar Tareas de clientes a grupos o equipos individuales. Una vez creadas, las tareas son ejecutadas mediante un Desencadenador. Una Tarea de cliente puede tener más desencadenadores configurados. Las Tareas de cliente se distribuyen a los clientes cuando el agente ESET Management en un cliente se conecta al servidor de ESET PROTECT. Por esta razón, puede llevar algún tiempo devolver los resultados de ejecución de tareas al servidor de ESET PROTECT. Puede administrar el intervalo de conexión del agente ESET Management para reducir los tiempos de ejecución de tareas.

En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.



Crea una nueva tarea de cliente

1. Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

   - Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
   - Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
   - Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

2. En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

3. Configure la tarea en la sección **Configuración**.

4. Compruebe todos los ajustes de la tarea en la sección **Resumen** y, a continuación, haga clic en **Finalizar**.

5. Haga clic en **Crear desencadenador** para crear un desencadenador para la tarea de cliente o haga clic en **cerrar** y cree el desencadenador más tarde.

Desencadenadores de tarea de cliente

Deberá asignar un desencadenador a una Tarea de cliente para que se pueda ejecutar. Para crear un desencadenador, haga clic en **Tareas** > en la instancia Tarea del cliente en la tabla principal y seleccione > **Ejecutar**

en desde el menú desplegable. Por otro lado, puede asignar una tarea de cliente a un grupo o equipo.

Para definir un desencadenador, seleccione los equipos o grupos de **Destino** en los cuales se debe ejecutar la Tarea del cliente. Habiendo seleccionado los destinos, establezca las condiciones que **desencadenan** la tarea en un momento o evento en particular. Además, puede usar la opción **Configuración avanzada - Límite** para ajustar aún más el desencadenador, si fuese necesario.

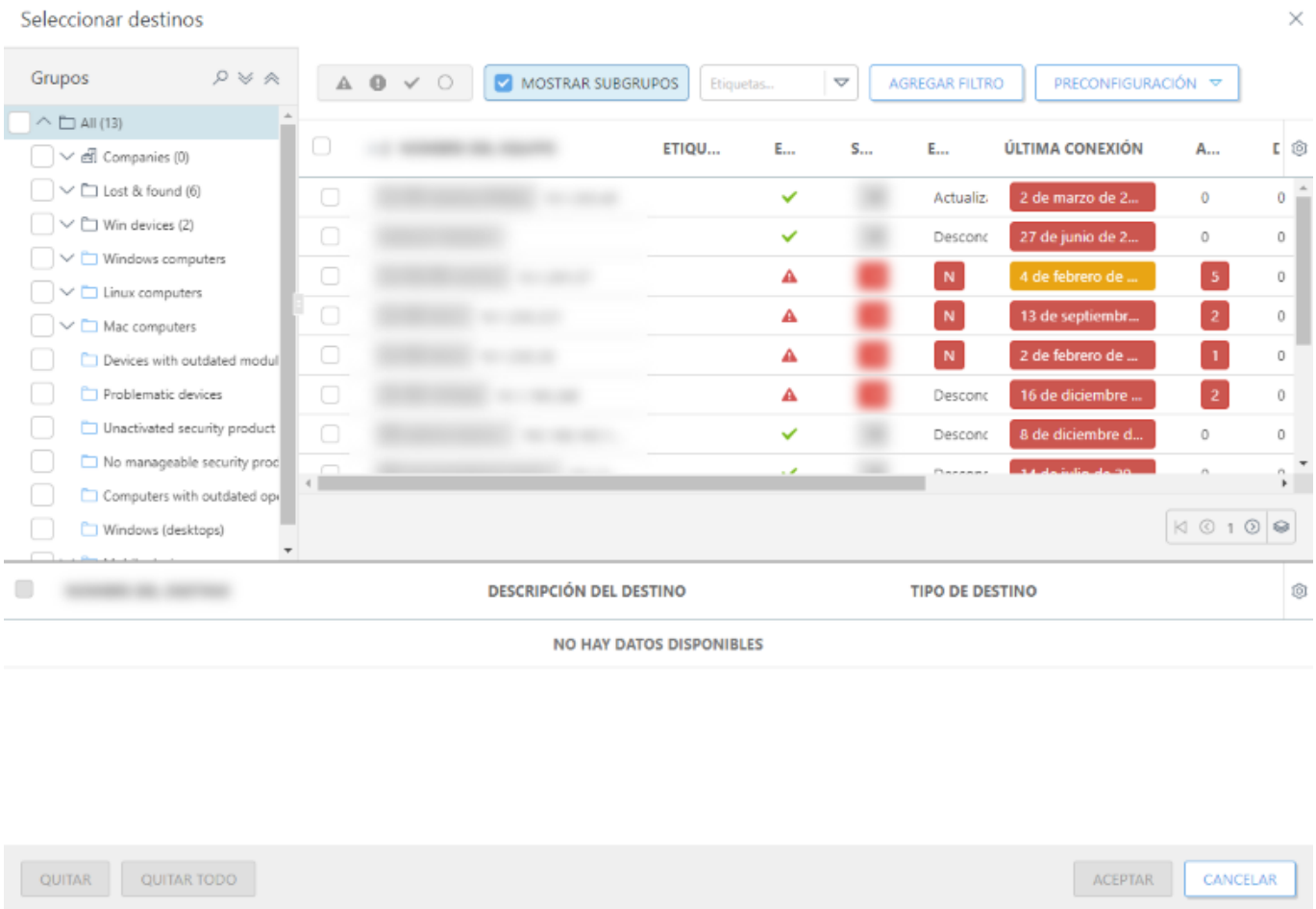
Básica

Ingrese la información básica sobre el **Desencadenador en el campo Descripción** y luego haga clic en **Destino**.

Destino

La ventana **Destino** le permite especificar los clientes (computadoras individuales o grupos) que son los destinatarios de esta tarea. Haga clic en **Agregar destinos** para visualizar todos los Grupos estáticos y dinámicos, sus miembros y los dispositivos o grupos seleccionados.

> Para asignar todos los equipos de un grupo, asigne el grupo en lugar de los equipos individuales para evitar que la consola web se ralentice.
> Si selecciona una gran cantidad de equipos, la consola web muestra una advertencia.



Luego de realizar su selección, haga clic en **Aceptar** y continúe a la sección **Desencadenador**.

Desencadenador

El desencadenador determina qué evento desencadena la tarea.

- **Lo antes posible**: ejecuta la tarea tan pronto como el cliente se conecta al ESET PROTECT On-Prem y recibe la tarea. Si la tarea no se puede realizar hasta la **Fecha de expiración**, se eliminará de la cola; es decir, no se eliminará, pero tampoco se ejecutará.
- **Programado**: ejecuta la tarea en el momento seleccionado.
- **Desencadenador de registro de eventos**: ejecuta la tarea en función de los eventos especificados aquí. Este desencadenador se invoca cuando ocurre un evento determinado en los registros. Defina el **tipo de registro**, el **operador lógico** y los criterios de **filtrado** que desencadenarán la tarea.
- **Desencadenador de grupo dinámico unido**: este desencadenador ejecuta la tarea cuando un cliente se une al Grupo dinámico seleccionado en la opción Destino. Si se ha seleccionado un Grupo estático o clientes individuales, esta opción no estará disponible.
- Expresión CRON: también puede configurar el intervalo de su desencadenador con una Expresión CRON.

> Para obtener más información sobre los desencadenadores, continúe al capítulo Tipos de desencadenadores de tareas.

Configuración avanzada: Umbral

El límite se usa para restringir la ejecución de una tarea si la misma se desencadena por un evento que ocurre con frecuencia, por ejemplo, el **Desencadenador de registro de eventos** o el**Desencadenador de grupo dinámico unido** (consulte arriba). Para obtener más información, consulte el capítulo Configuración avanzada - limitado.

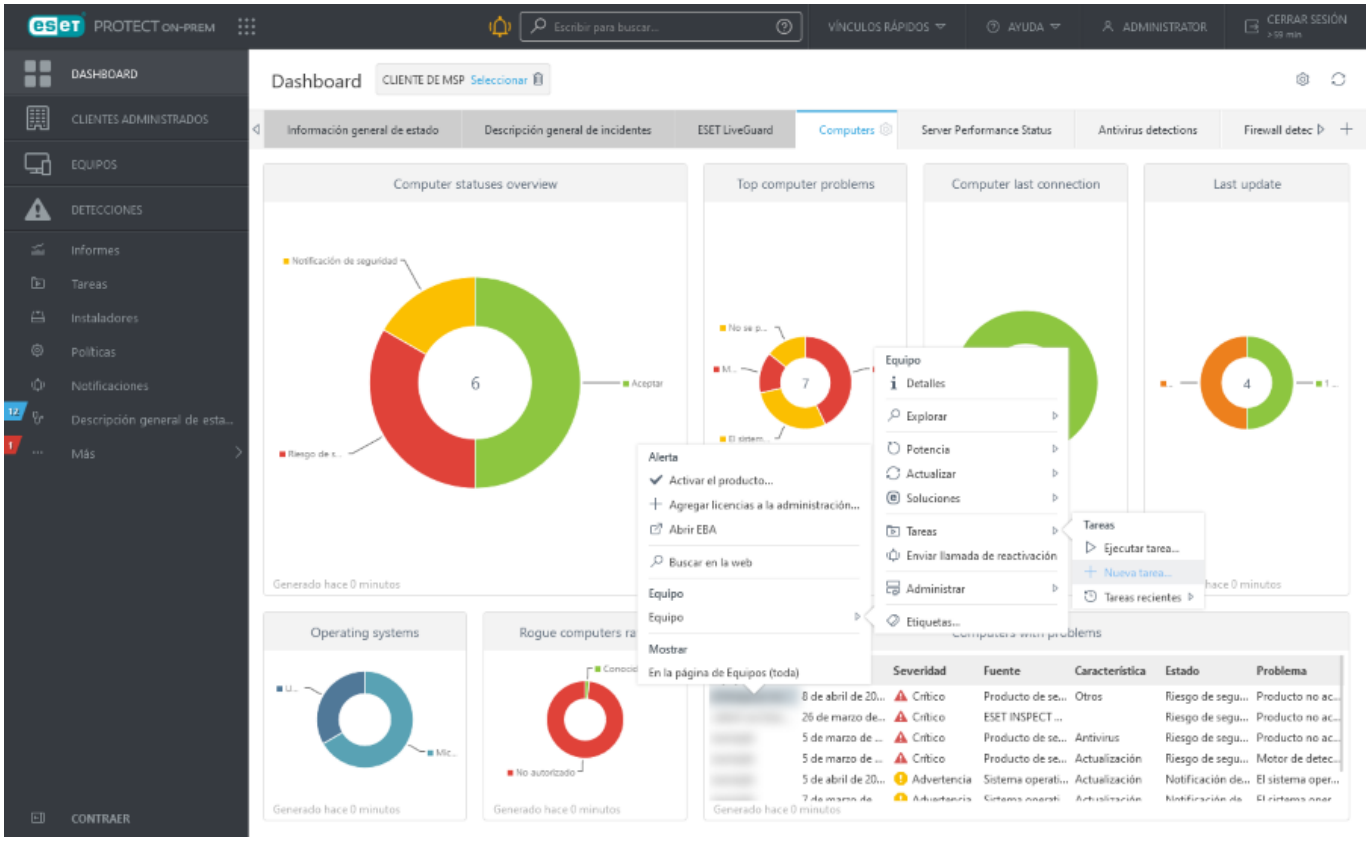
Haga clic en **Finalizar** cuando haya definido los destinatarios de esta tarea y los desencadenadores que la ejecutan.

Asignar tarea de cliente a un grupo o equipo

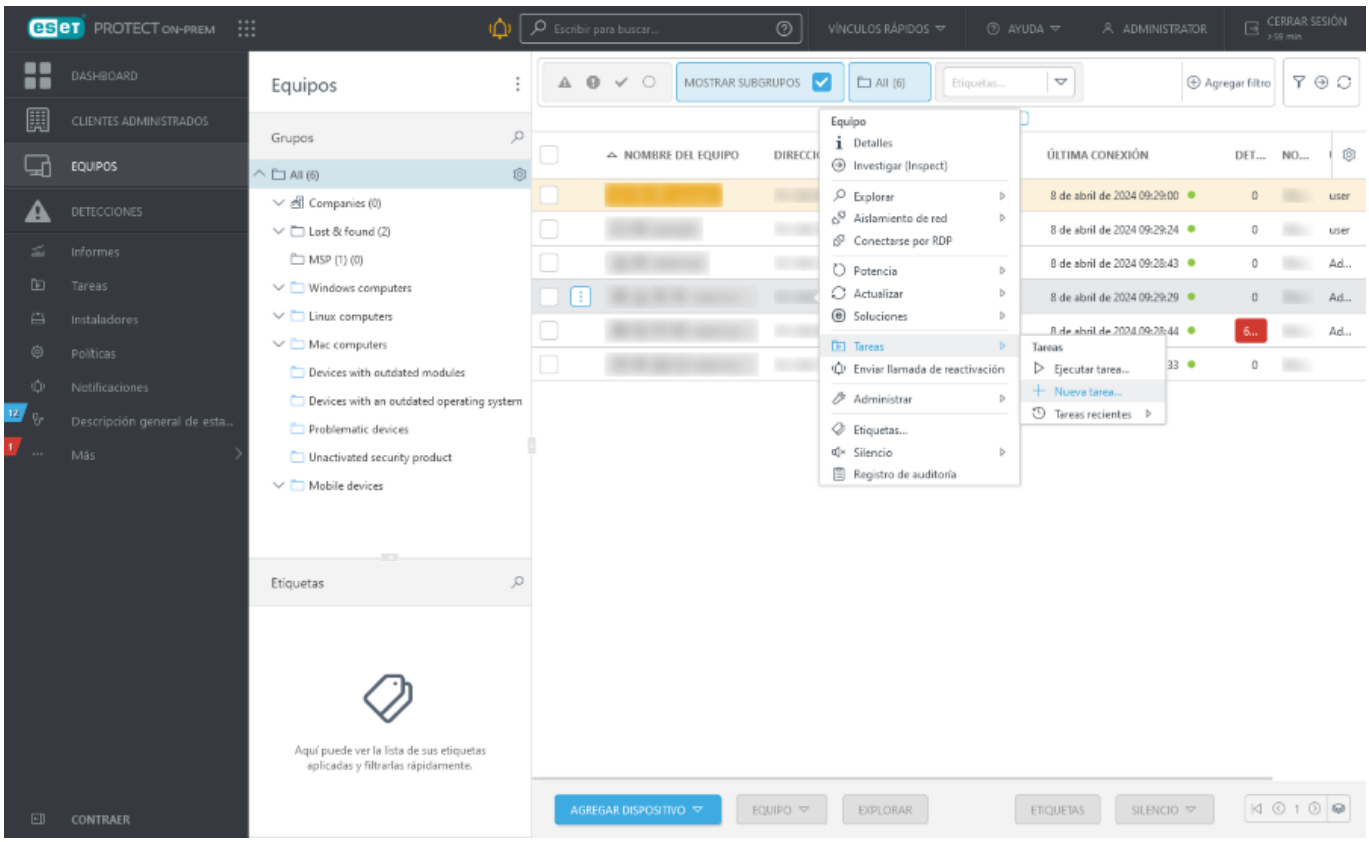
Lea aquí para saber cómo asignar una Tarea de cliente a un grupo.

Hay dos formas de asignar una tarea a un equipo.

1. **Tablero** > **Equipos** > **Equipos con problemas** > seleccione un equipo y haga clic en **Equipo** > **Tareas** > **Nueva tarea**



2.Equipo > seleccione el equipo mediante las casillas de verificación > **Tareas** > **Nueva tarea**.



Se abrirá una nueva ventana del Asistente de nuevas tareas de clientes.

Acciones Anti-Theft

La función **Anti-Theft** protege a los dispositivos móviles de accesos no autorizados.

En caso de que el usuario pierda o le roben su dispositivo móvil (inscrito y administrado por ESET PROTECT On-Prem), algunas acciones se desencadenan automáticamente y otras pueden ejecutarse con las tareas del cliente.

Si una persona no autorizada reemplaza la tarjeta SIM por una nueva (no segura), ESET Endpoint Security para Android **bloqueará** automáticamente el dispositivo y enviará un SMS de alerta a un número de teléfono definido por el usuario. Este mensaje incluirá la siguiente información:

- el número de dispositivo móvil de la tarjeta SIM en uso en la actualidad
- el número **IMSI** (Identidad del suscriptor móvil internacional)
- el número **IMEI** (Identidad del equipo móvil internacional) del dispositivo móvil

El usuario no autorizado no sabrá que se ha enviado este mensaje, porque se eliminará automáticamente del hilo de mensajes del dispositivo. También puede solicitar las coordenadas **GPS** del dispositivo móvil perdido o eliminar en forma remota todos los datos almacenados en este con las tareas del cliente.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

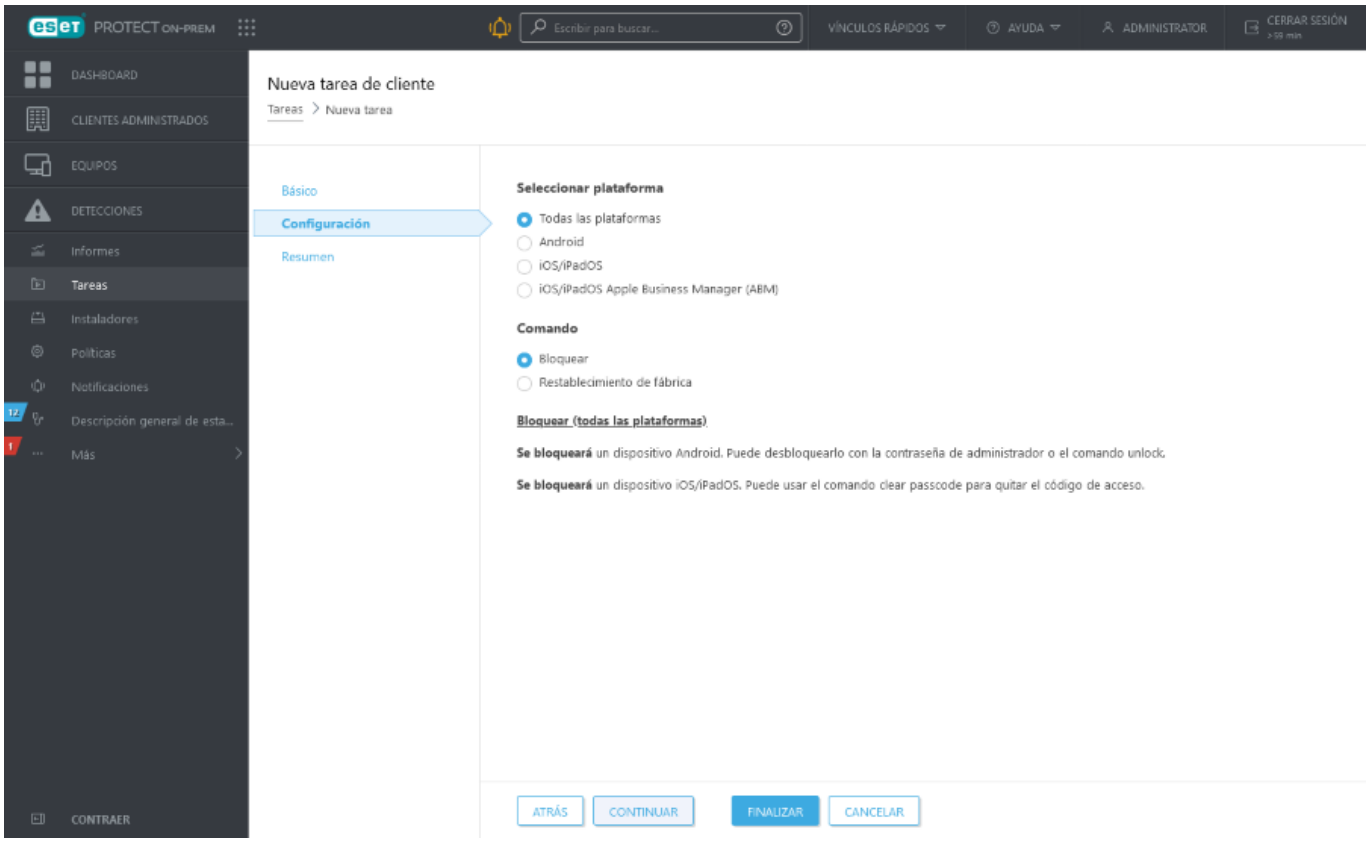
Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**.
Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

Configuración

Acción	Comportamiento en SO móvil	Descripción
Busque		El dispositivo responderá con un mensaje de texto con sus coordenadas GPS. Si existe una ubicación más precisa disponible después de 10 minutos, el dispositivo enviará un mensaje nuevamente. La información recibida se muestra en los detalles del dispositivo. **Buscar** solo funciona si GPS está habilitado en el dispositivo.
		No compatible.
Bloquear		Se bloqueará el dispositivo. Puede desbloquear el dispositivo usando la contraseña del Administrador o con el comando **desbloquear**.
		Se bloqueará el dispositivo. El código de acceso se puede quitar con el comando **clear passcode** (borrar código de acceso).
Desbloquear		Se desbloqueará el dispositivo para que pueda volver a usarse. La tarjeta SIM actual del dispositivo se guardará como tarjeta SIM de confianza.
		No compatible.
Sonido de sirena/modo extraviado		El dispositivo se bloqueará y reproducirá un sonido muy fuerte durante 5 minutos (o hasta ser desbloqueado).
		No compatible.
Borrar el código de acceso		No compatible.
		Quita el código de acceso del dispositivo. Se le solicitará al usuario que configure un nuevo código de acceso una vez que el dispositivo esté activado.
Restablecimiento de fábrica		Se eliminarán todos los datos accesibles en el dispositivo (se destruirán los encabezados de los archivos) y el dispositivo se ajustará a su configuración predeterminada de fábrica. Esto puede demorar unos minutos.
		Se quitarán toda la configuración e información y el dispositivo tendrá la configuración predeterminada de fábrica. Esto puede demorar unos minutos.

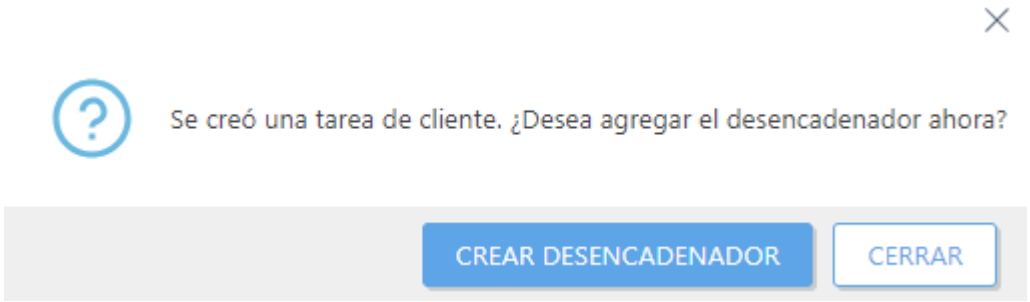
Acción	Comportamiento en SO móvil	Descripción
Activar Modo extraviado y Buscar		Compatible únicamente en iOS ABM. El dispositivo cambiará al «modo extraviado», se bloqueará y se desbloqueará ejecutando la tarea **Apagar el modo extraviado** del ESET PROTECT On-Prem. Puede personalizar el número de teléfono, el mensaje y el pie de página que se mostrará en la pantalla del dispositivo extraviado. El estado de protección del dispositivo cambiará a **Extraviado**.
Desactivar el modo extraviado		Compatible únicamente en iOS ABM. El estado de protección del dispositivo cambiará y volverá a su estado de servicio normal.



Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Buscar actualizaciones del producto

La tarea **Buscar actualizaciones de productos** aplica la verificación de las actualizaciones de productos de seguridad de ESET (actualizaciones automáticas) en los equipos administrados:

> Productos de seguridad de ESET compatible:
> • ESET Endpoint Antivirus/Security para Windows versión 10.1 y posteriores

- Si hay disponible una versión posterior del producto de seguridad de ESET, se descarga.
- La actualización del producto de seguridad de ESET requiere un reinicio del equipo, pero no inmediatamente (el reinicio no es obligatorio). El administrador de ESET PROTECT On-Prem puede aplicar la actualización y el reinicio del equipo de forma remota desde la consola web mediante la tarea Apagar cliente del equipo con la casilla de verificación **Reiniciar equipos** seleccionada.
- El producto de seguridad anterior de ESET sigue siendo completamente funcional hasta el reinicio. La actualización se realiza después del siguiente reinicio del equipo.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

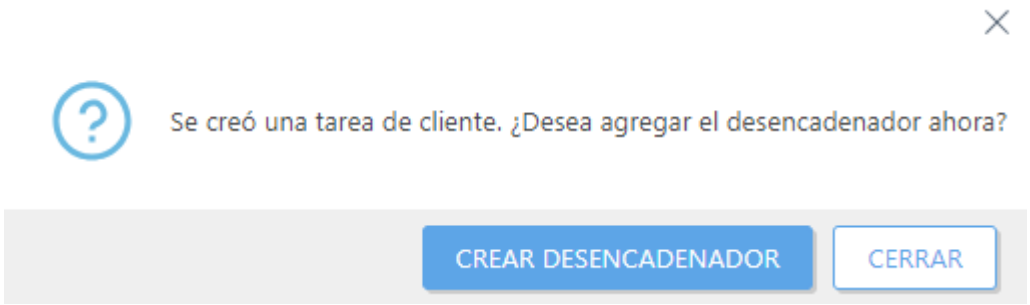
Configuración

> No hay una **configuración** disponible para esta tarea.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Diagnósticos

Use la tarea **Diagnóstico** para solicitar una acción de diagnóstico de un producto de seguridad ESET en un equipo cliente.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**.
Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

Configuración

Acción de diagnóstico

- **Ejecutar recopilación de registros**: recopila datos específicos (como configuraciones y registros) desde una máquina seleccionada a fin de facilitar la recopilación de información desde la máquina del cliente durante una resolución de caso de soporte.

  o**Parámetros de Log Collector**: puede especificar parámetros de Log Collector en Windows, macOS o Linux. Para recopilar todos los datos, deje el campo **Parámetros de recopilación de registros** en blanco. Si especifica los parámetros de Log Collector, seleccione solo los equipos que ejecuten el sistema operativo correspondiente como destinos de la tarea.

El límite de tamaño de archivo para la entrega de registros por dispositivo es de 200 MB. Puede acceder a los registros desde la consola web en la sección **Detalles** > **Registros**. Si los registros recopilados por la tarea son mayores que 200 MB, se producirá un error en la tarea. Si la tarea falla, usted puede:
- Recopilar los registros localmente en el dispositivo.
- Cambiar el nivel de detalle de los registros y repetir la tarea:
  - En el caso de los objetivos de Windows, use el parámetro `/Targets:EraAgLogs` para recopilar solo los registros del agente ESET Management.
  - En el caso de los objetivos de Linux/macOS, use el parámetro `--no-productlogs` para excluir registros del producto de seguridad ESET instalado.

- **Definir Modo de diagnóstico** - El modo de diagnóstico consiste en las siguientes categorías: **Registro de spam**, **Registro de firewall**, **Registro de HIPS**, **Registro de de dispositivo de control** y **Registro de control Web**. El propósito principal del Modo de diagnóstico es recopilar registros cuando se necesita resolver problemas.

  - **Activar**: enciende la generación de registros de todas las aplicaciones de ESET.

  - **Desactivar**: puede desactivar la generación de registros manualmente o se desactivará de manera automática luego del reinicio de un equipo.

Los siguientes prerrequisitos son necesarios para la creación exitosa de los registros de Diagnóstico:

- Los registros del modo diagnóstico pueden recopilarse de los equipos cliente que ejecuten sistemas operativos Windows o macOS.

- El equipo cliente debe tener un Producto de seguridad ESET instalado y activado.

El Agente ESET Management únicamente envía archivos recopilados con un producto de ESET instalado en un equipo de un cliente. La categoría y las palabras en el registro dependen del tipo de producto y la configuración. Configure cada producto (a través de las Políticas) para recopilar registros específicos.

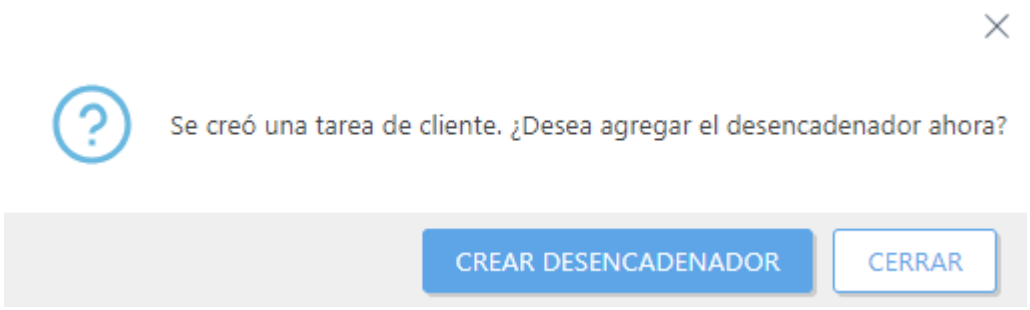
Los registros de diagnóstico de más de 24 horas se eliminarán todos los días durante la limpieza nocturna. Esto evita que la base de datos de ESET PROTECT se cargue en exceso.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.

- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Puede ver los registros creados en Detalles del equipo: **Registros** > **Registro de diagnóstico**.

Visualización de mensajes

La tarea **Mostrar mensaje** le permite enviar un mensaje a cualquier dispositivo administrado (equipo cliente, tableta, móvil, etc.). El mensaje se mostrará en la pantalla para informar al usuario.

- Windows: el mensaje se muestra como notificación.

> En Windows, la Tarea de clientes Mostrar mensaje usa el comando msg.exe, el cual solo está disponible en las ediciones de Windows Empresarial/Profesional. En consecuencia, no puede usar esta tarea para mostrar un mensaje en un equipo cliente que ejecute Windows versión Home.

- En macOS y Linux, el mensaje se muestra únicamente en una terminal.

> Para ver el mensaje en macOS o Linux, primero necesita abrir la terminal.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**.
Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

Configuración

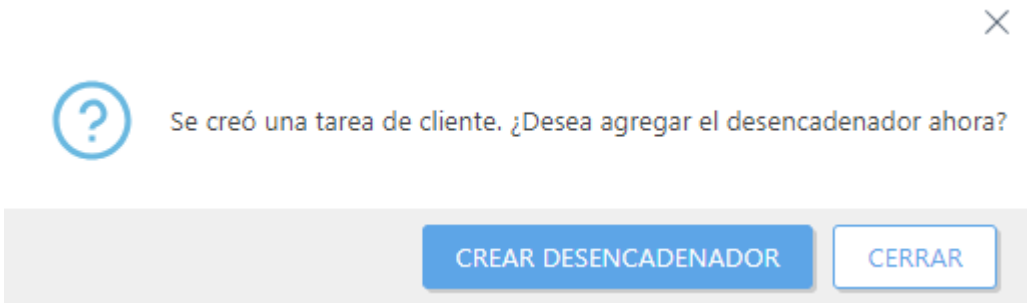
Puede ingresar un **Título** y escribir su **Mensaje**.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del

cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Finalizar aislamiento del equipo de la red

La tarea **Finalizar aislamiento del equipo de la red** finaliza el aislamiento del equipo de la red y permite conexiones del equipo aislado nuevamente. Utilice esta tarea únicamente cuando se haya resuelto el problema de seguridad.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

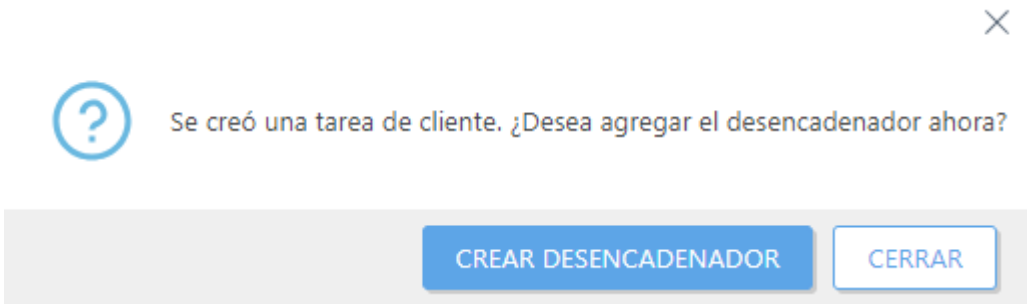
En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

No hay una **configuración** disponible para esta tarea.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Exportación de la configuración de productos administrados

La tarea **Exportar la configuración de productos administrados** se usa para exportar la configuración de componentes individuales de ESET PROTECT o de los productos de seguridad ESET instalados en los clientes.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**.
Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

Configuración

Exportar configuración de productos administrados.

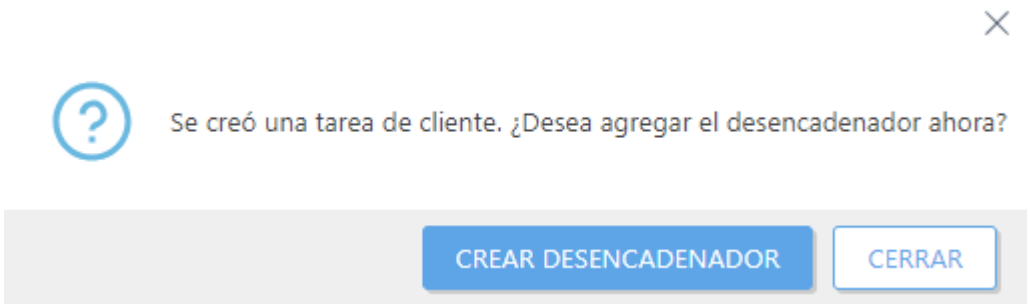
- **Producto**: seleccione un componente de ESET PROTECT o un producto de seguridad ESET del cliente para el que desee exportar la configuración.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.

- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Cuando finalice la tarea, podrá encontrar la configuración exportada en la pestaña **Configuración**, en Detalles del equipo de los equipos de destino.

Aislar equipo de la red

La tarea **Aislar equipo de la red** aísla los equipos seleccionados de la red y se bloquearán todas las conexiones, excepto las que sean necesarias para el funcionamiento adecuado de los productos ESET. Las conexiones permitidas son las siguientes:

- el equipo obtiene una dirección IP
- comunicación de *ekrn.exe*, agente ESET Management, conector ESET Inspect
- inicio de sesión a un dominio

El aislamiento de la red es compatible únicamente con productos de seguridad ESET (Endpoint Antivirus/Security y productos de seguridad del servidor).
Es probable que el aislamiento de la red interrumpa el normal funcionamiento de los equipos. Solo debería usarlo en casos de emergencia (por ejemplo, si se identifica un problema grave de seguridad en un equipo administrado). Puede dar por finalizado el aislamiento con una tarea del cliente.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

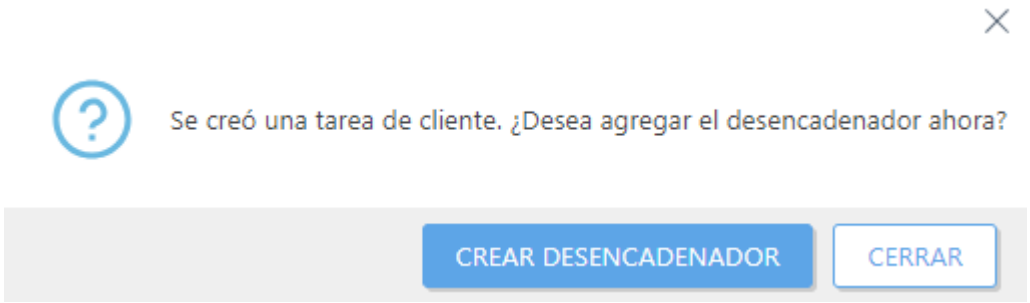
En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

No hay una **configuración** disponible para esta tarea.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Cerrar sesión

La tarea **Cerrar sesión** cierra la sesión de todos los usuarios del equipo de destino. Alternativamente, haga clic en un equipo y seleccione **Alimentación** > **Cerrar sesión**.

El equipo debe ejecutar el agente ESET Management 10.0 o una versión posterior. La tarea del cliente **Cerrar sesión** fallará en un equipo en el que se ejecute una versión del agente anterior.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

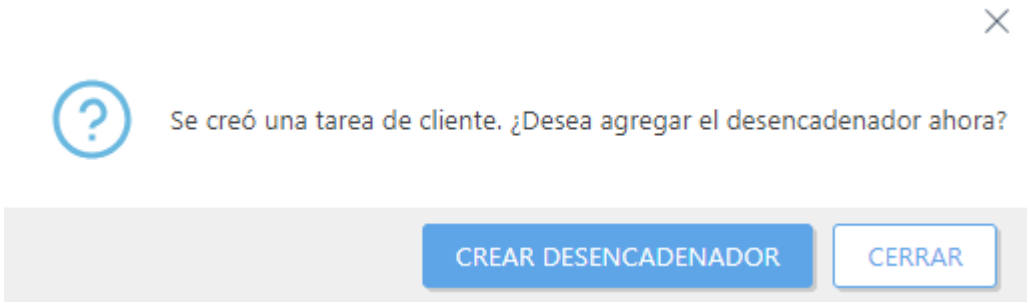
En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

No hay una **configuración** disponible para esta tarea.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Actualización de módulos

La tarea **Actualización de módulos** fuerza la actualización de todos los módulos del producto de seguridad instalado en el dispositivo objetivo. Esta es una tarea general para todos los productos de seguridad en todos los sistemas. Puede encontrar la lista de todos los módulos del producto de seguridad objetivo en la sección **Acerca de** del producto de seguridad.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**.
Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

Configuración

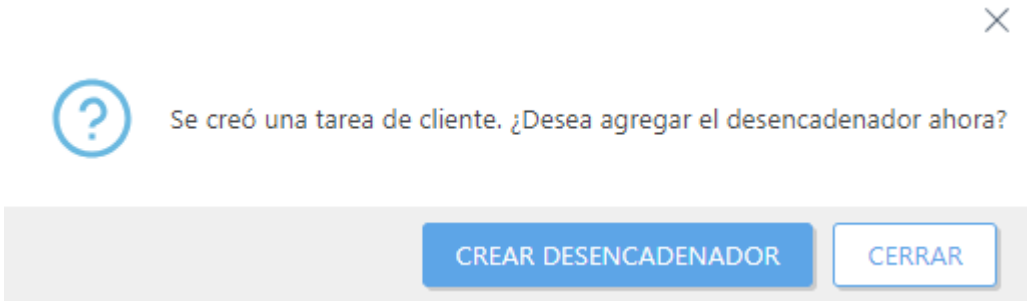
- **Borrar caché de actualización**: esta opción elimina los archivos de actualización temporales de la caché del cliente, y a menudo se usa para reparar los errores de actualización del módulo.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.

- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Configurar un servidor personalizado para las actualizaciones de módulos

Si la actualización de los módulos del producto de seguridad de ESET falla debido a un geobloqueo, use una política para definir un servidor personalizado para las actualizaciones de módulos:

1. En la configuración de la política de productos de seguridad de ESET, seleccione **Actualizar** > **Perfiles** > **Actualizaciones**.
2. En **Actualizaciones de módulos**, desactive **Elegir automáticamente** y escriba la dirección del **servidor personalizado**. Por ejemplo, para usar servidores de actualización de EE. UU. para ESET Endpoint Antivirus/Security 9 para Windows, escriba *http://us-update.eset.com/eset_upd/ep9/* (versión 8: *http://us-update.eset.com/eset_upd/ep8/*).
3. Escriba su **Nombre de usuario** (EAV-XXXXXXXX) y la **Contraseña** de la licencia. Puede obtenerlos de los detalles de la licencia heredados.

Reversión de actualizaciones de módulos

En casos donde una actualización de módulo causa problemas o si no desea aplicar la actualización a todos los clientes (por ejemplo, para realizar pruebas o al utilizar actualizaciones previas al lanzamiento) puede utilizar la tarea **Reversión de actualizaciones de módulo**. Cuando se aplica esta tarea, los módulos se restablecerán a la versión anterior.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.

- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**.
Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

Configuración

Expanda esta sección para personalizar la configuración de la reversión de actualizaciones de módulos.

Acción

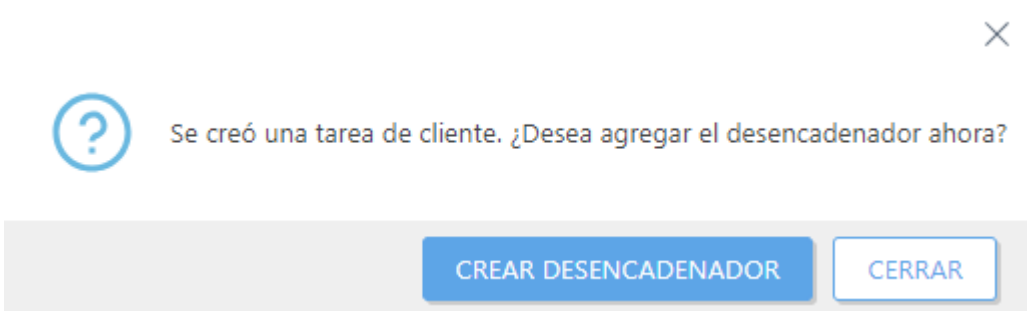
- **Habilitar actualizaciones**: las actualizaciones están habilitadas y el cliente recibirá la próxima actualización del módulo.
- **Revertir y deshabilitar las próximas actualizaciones**: las actualizaciones se deshabilitan durante el período de tiempo determinado en el menú desplegable **Deshabilitar intervalo** (12, 24, 36, 48 horas o hasta que se revoque).

> Sea precavido cuando usa la opción **Hasta que se revoque**, ya que esta opción presenta un riesgo de seguridad.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Exploración bajo demanda

La tarea **Exploración bajo demanda** le permite ejecutar una exploración manual del equipo cliente (además de una exploración programada periódica).

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**.
Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

Configuración

Apagar el equipo tras la exploración: si selecciona esta casilla de verificación, el equipo se apagará después de que finalice la exploración

Puede configurar el comportamiento de reinicio o apagado de los equipos administrados. El equipo debe ejecutar el Agente de ESET Management 9.1 y versiones posteriores, además de un producto de seguridad de ESET compatible con esta configuración.

Perfil de exploración

Puede seleccionar el perfil que desee del menú desplegable:

- **Exploración exhaustiva:** este es un perfil predefinido en el cliente. Se configura para que sea el perfil de exploración más exhaustivo y verifique el sistema en su totalidad, pero también requiere mayor cantidad de tiempo y recursos.
- **Exploración inteligente:** la exploración inteligente le permite iniciar rápidamente una exploración del equipo y limpiar los archivos infectados sin que el usuario intervenga. La ventaja del Análisis inteligente es su facilidad de uso y que no requiere una configuración detallada de la exploración. La exploración inteligente verifica todos los archivos en los discos locales y desinfecta o elimina en forma automática las infiltraciones detectadas. El nivel de desinfección está establecido automáticamente en el valor predeterminado.
- **Exploración desde el menú contextual:** explora un cliente con un perfil de exploración predefinido; puede personalizar los objetos para explorar.
- **Perfil personalizado**: la exploración personalizada le permite especificar los parámetros de exploración tales como los destinos o métodos de exploración. La ventaja de una exploración personalizada es la capacidad de configurar los parámetros detalladamente. Es posible guardar las configuraciones en perfiles

de exploración definidos por el usuario, lo que facilita repetir la exploración con el uso de los mismos parámetros. Se debe crear un perfil antes de ejecutar la tarea con esta opción. Una vez que haya seleccionado un perfil personalizado del menú desplegable, ingrese el nombre exacto del perfil en el campo de texto **Perfil personalizado**.

Desinfección

En forma predeterminada, se selecciona **Exploración con desinfección**. Esta configuración permite la limpieza automática de los archivos infectados encontrados. De no ser posible, se pondrán en cuarentena.

Destinos de exploración

La opción **Explorar todos los destinos** también se encuentra seleccionada en forma predeterminada. Por medio de esta configuración, se exploran todos los destinos especificados en el perfil de exploración. Si anula la selección de esta opción, necesita especificar en forma manual los destinos de exploración en el campo **Agregar destino**. Ingrese el objeto para explorar en el campo de texto y haga clic en **Agregar**. El destino se visualizará en el campo **Destinos de exploración** a continuación. Un destino de exploración puede ser un archivo, una ubicación o puede ejecutar una exploración definida previamente mediante cualquiera de las siguientes cadenas como un **Destino de exploración**:

Explorar objetivo	Ubicaciones exploradas
`${DriveRemovable}`	Todos los dispositivos y unidades extraíbles.
`${DriveRemovableBoot}`	Sectores de inicio de todas las unidades extraíbles.
`${DriveFixed}`	Unidades de discos duros (HDD, SSD)
`${DriveFixedBoot}`	Sectores de inicio de unidades de discos duros.
`${DriveRemote}`	Unidades de red.
`${DriveAll}`	Todas las unidades disponibles.
`${DriveAllBoot}`	Sectores de arranque y UEFI de todas las unidades. Puede obtener más información sobre el Explorador UEFI en el glosario.
`${DriveSystem}`	Unidades del sistema.
`${Share}`	Unidades compartidas (solo para productos del servidor).
`${Boot}`	Sector de inicio principal.
`${Memory}`	Memoria operativa.
`${Registry}`	Registro del sistema (solo para ESET 8 Endpoint y versiones posteriores).
`${Wmi}`	Base de datos WMI (solo para ESET 8 Endpoint y versiones posteriores).

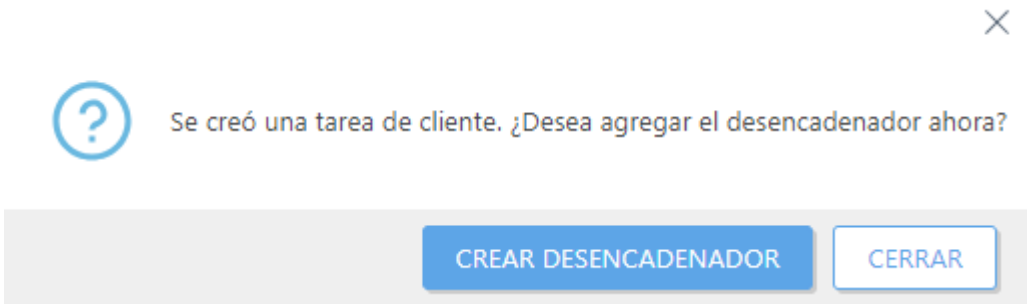
A continuación se muestran ejemplos del modo de uso de los parámetros de destinos de la **Exploración bajo demanda**:
■Archivo: *C:\Users\Data.dat*
■Carpeta *C:\MyFolder*
■Ruta o archivo Unix */usr/data*
■Ubicación UNC de Windows *\\server1\scan_folder*
■Cadena predefinida `${Memory}`

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

• Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.

• Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Actualización de sistema operativo

La tarea Actualización del sistema operativo se usa para actualizar el sistema operativo del equipo cliente. Esta tarea puede activar la actualización de sistema operativo en los sistemas operativos de Windows, macOS y Linux.

- **macOS**: la tarea instala todas las actualizaciones (la actualización de todos los paquetes) mediante el comando:

```
/usr/sbin/softwareupdate --install --all
```

- **Linux**: la tarea instala todas las actualizaciones (la actualización de todos los paquetes). Verifica varios administradores de paquetes, así que cubre la mayoría de las distribuciones. Ejecuta los siguientes comandos:

  Debian/Ubuntu:

  ```
  apt-get update --assume-no && apt-get dist-upgrade --assume-yes
  ```

  CentOS/Red Hat:

  ```
  yum update -y
  ```

  SLES/SLED:

  ```
  zypper --non-interactive update -t patch
  ```

- **Windows**: la tarea instala actualizaciones del sistema operativo al llamar a una API de Windows interna. No instala las actualizaciones de características, lo que actualiza su Windows a una versión más reciente.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

Configuración

- **Aceptar automáticamente EULA** (solo Windows): seleccione esta casilla si desea aceptar el EULA de forma automática. No se mostrará ningún texto al usuario. Si no habilita aceptar EULA, la tarea se salta las actualizaciones que requieran aceptar EULA.

- **Instalar actualizaciones opcionales** (soloWindows): también se instalarán las actualizaciones marcadas como opcionales y que no necesitan del usuario.

- **Permitir reinicio** (Windows y macOS): fuerza el reinicio del equipo cliente tras instalar las actualizaciones que requieren reiniciar.

Puede configurar el comportamiento de reinicio o apagado de los equipos administrados. El equipo debe ejecutar el Agente de ESET Management 9.1 y versiones posteriores, además de un producto de seguridad de ESET compatible con esta configuración. Si el equipo administrado no admite la configuración del comportamiento de reinicio:

- Windows informará al usuario del equipo sobre el reinicio forzado planificado 4 horas antes del reinicio y 10 minutos antes del reinicio.

- macOS se reiniciará inmediatamente después de la actualización.

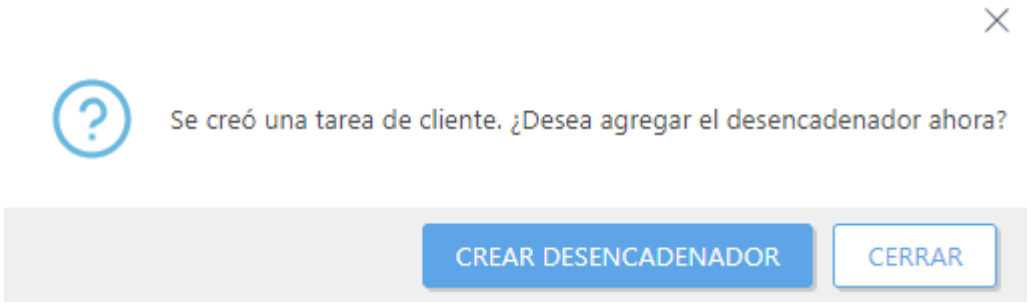
- Se instalarán actualizaciones que requieran reiniciarse, aunque no active la casilla de verificación **Permitir reinicio**.
- La **configuración** no influye en la tarea si el dispositivo de destino está ejecutando un tipo de sistema operativo no compatible.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.

- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Administración de cuarentena

La tarea **Administración de cuarentena** se usa para administrar los objetos en cuarentena del ESET PROTECT On-Prem, objetos infectados o sospechosos encontrados durante la exploración.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

Configuración

Configuración de la administración de cuarentena

Acción: seleccione la acción que debe adoptarse en relación al objeto en cuarentena.

- **Restaurar objeto(s)** restaura el objeto a su ubicación original, pero se explorará y si las razones de la cuarentena persisten, el objeto será puesto en cuarentena nuevamente
- **Restaurar objeto(s) y excluir en el futuro** restaura el objeto a su ubicación original y no se pondrá en cuarentena nuevamente.
- **Eliminar objeto(s)**: elimina el objeto permanentemente.

Tipo de filtro: filtre los objetos en cuarentena en función de los criterios definidos a continuación.

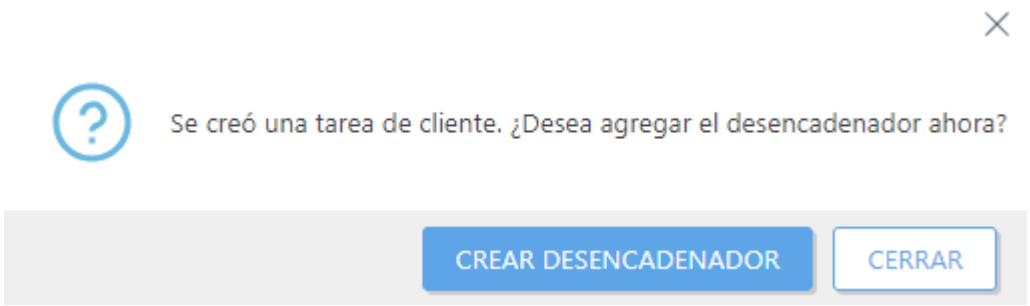
Configuración del filtro:

- **Elementos hash**: agregue elementos hash en un campo. Solo se puede introducir objetos conocidos como, por ejemplo, un objeto que ya haya estado en cuarentena.
- **Ocurrió** > **Ocurrió desde**, **Ocurrió hasta**: defina el rango de tiempo por el que el objeto se haya puesto en cuarentena.
- **Tamaño** > **Tamaño mínimo/máximo (bytes)**: defina el rango de tamaño del objeto en cuarentena (en bytes).
- **Nombre de la detección**: seleccione una detección de la lista de elementos en cuarentena.
- **Nombre del objeto**: seleccione un objeto de la lista de elementos en cuarentena.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Activación del producto

Use la tarea **Activación del producto** para activar un producto de seguridad ESET en un equipo cliente o dispositivo móvil.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

Configuración

Configuraciones de activación del producto – Seleccione la licencia adecuada del producto de la lista de licencias disponibles. Esta licencia se aplicará a los productos que ya estén instalados en el cliente. La lista de licencias disponibles no muestra las licencias vencidas o sobreusadas (aquellas que están en estado **Error** u **Obsoleto**). Puede agregar una licencia a través de uno de los métodos que se describen en Administración de licencias. La adición o eliminación de licencias está restringida al administrador cuyo grupo de pertenencia sea **Todo** y que tenga el permiso de **Escritura** en las licencias.

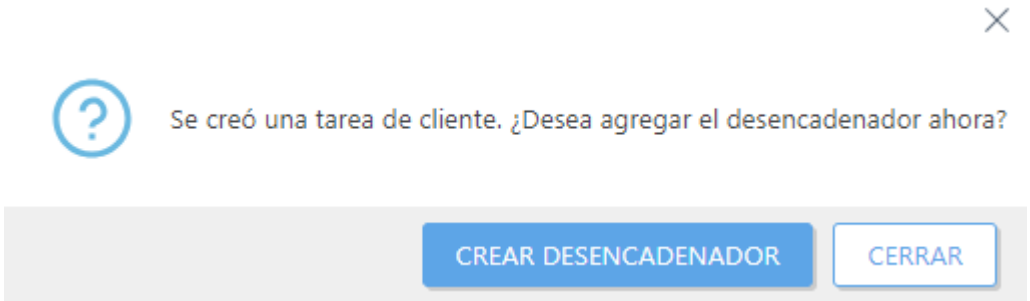
La tarea de **Activación del producto** puede ejecutarse en dispositivos móviles ESET Endpoint para Android con una licencia sin conexión.
La tarea de activación no puede activar los productos de ESET de las versiones 4 y 5 con la licencia sin conexión. Debe activar el producto manualmente o usar una versión del producto compatible (se recomienda usar la versión más reciente).

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.

- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Restablecimiento del agente clonado

Puede distribuir el Agente ESET Management en su red a través de una imagen predefinida, como describe este Artículo de la base de conocimiento. Los agentes clonados poseen el mismo SID, lo cual puede causar problemas (múltiples agentes con el mismo SID). Para resolverlos, use la tarea **Restablecer el agente clonado** para restablecer el SID y asignar Agentes a una única identidad.

ESET Management Agent identifica los equipos cliente clonados que se ejecutan en Windows automáticamente, sin la tarea Restablecer el agente clonado. Solo los equipos cliente con Linux y macOS (y clientes de Windows donde se desactivó la detección de hardware) necesitan la tarea para separar los equipos clonados.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

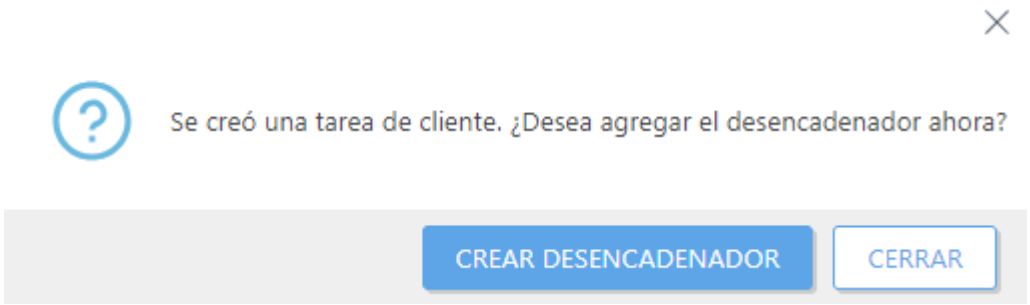
Ejecutar esta tarea con cuidado. Después de restablecer el Agente actual de ESET Management, se abandonará todas las tareas que este esté ejecutando. Es posible que no se tenga en cuenta el estado de ejecución **Finalizado**, **Con error** o **En ejecución** de esta tarea, en función de la replicación de datos.

No hay una **configuración** disponible para esta tarea.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Restablecimiento de la base de datos del Rogue Detection Sensor

La tarea **Restablecimiento de la base de datos del Rogue Detection Sensor** se usa para reiniciar la caché de búsqueda del RD Sensor. La tarea elimina la caché y los resultados de búsqueda se almacenarán nuevamente. Esta tarea no elimina los equipos detectados. Esta tarea es útil cuando los equipos detectados aún están en la caché y no se informan al servidor.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

> No hay una **configuración** disponible para esta tarea.

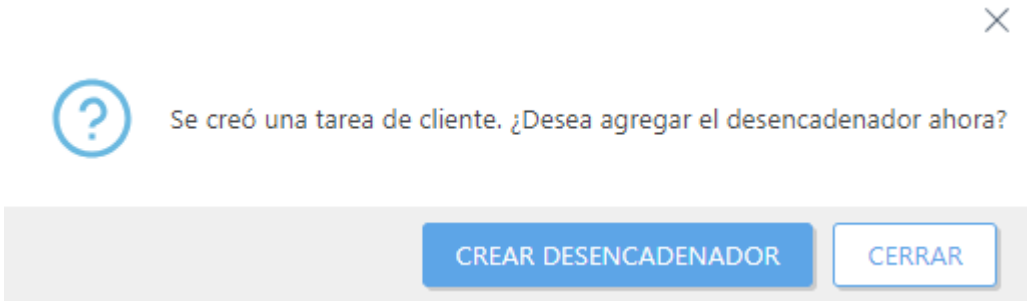
Al crear un desencadenador para esta tarea, oriente la acción a un equipo que tenga RD Sensor instalado.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.

- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Ejecución de comando

La tarea **Ejecutar comando** se puede usar para ejecutar las instrucciones de la línea de comandos específicas en el cliente. El administrador puede especificar la entrada de la línea de comandos a ejecutar.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Los comandos se ejecutan sin acceso al entorno de escritorio. En consecuencia, la ejecución de los comandos con requisitos para la interfaz gráfica del usuario de la aplicación puede fallar.

Puede usar comandos `ecmd` con la tarea Ejecutar comando. Para obtener más información, visite este artículo de la base de conocimiento.

Sistema operativo	El comando se ejecutara como usuario	Directorio de trabajo predeterminado	Ubicaciones accesibles de la red	El comando se ejecutará en
Windows	*Local System*	*C:\Windows\Temp*	Solo ubicaciones en el dominio actual y disponibles para el sistema local	Solicitud de comando (`cmd.exe`)
Linux o macOS	*root*	*/tmp*	Solo si la ubicación está montada y disponible para el usuario raíz	Consola

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**.
Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

Configuración

- **Línea de comandos a ejecutar**: ingrese la línea de comandos que desea ejecutar en los clientes.

• **Directorio en funcionamiento**: ingrese un directorio donde se ejecutará la línea de comandos anterior.

Puede escribir un comando de varias líneas. Restricciones de extensión máxima del comando:
• La consola web puede procesar hasta 32 768 caracteres. Si copia y pega un comando más extenso, se cortará sin aviso al final.
• Linux y macOS pueden procesar la longitud completa del comando. Windows tiene una restricción de 8191 caracteres como máximo.

• Para ejecutar un script local ubicado en un cliente en *C:\Users\user\script.bat*, realice los siguientes pasos:
1.Cree una nueva tarea del cliente y seleccione **Ejecutar comando**.
2.En la sección **Configuración**, ingrese:
Línea de comando para ejecutar: `call script.bat`
Directorio en funcionamiento: *C:\Users\user*
3.Haga clic en **Finalizar**, cree un desencadenador y seleccione los clientes de destino.
• Para ejecutar un comando de varias líneas a fin de reiniciar un servicio de Windows de forma remota (reemplace `service_name` por el nombre de servicio, por ejemplo, `wuauserv` por el servicio Windows Update):

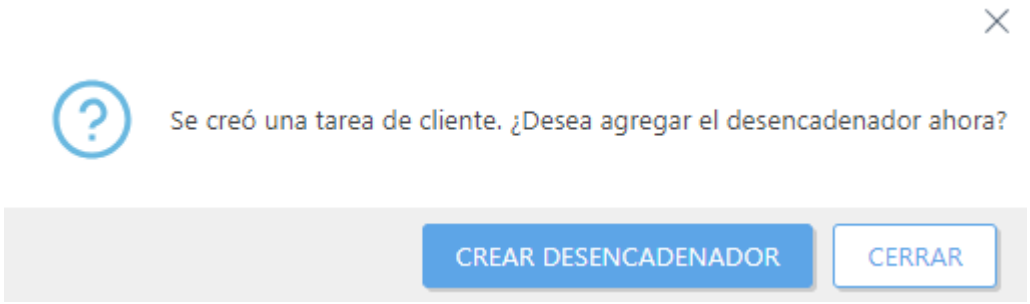
```
net stop service_name
net start service_name
```

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

• Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.

• Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Examine el resultado de la tarea Ejecutar comando

1. Haga clic en **Tareas** > haga clic en la tarea > **Mostrar detalles** > pestaña **Ejecuciones** >, haga clic en una línea de la tabla > **Historial**.

2. La columna **Mensaje de seguimiento** contiene los primeros 255 caracteres del resultado de la tarea Ejecutar comando. Puede crear informes y procesar estos datos desde varios equipos. Puede descargar un resultado más grande como registro de Log Collector en **Detalles** del equipo > **Registros** > Log Collector.

Ejecución del script de SysInspector

La tarea **Ejecutar el script de SysInspector** se usa para eliminar objetos no deseados del sistema. Se necesita exportar un script de SysInspector del SysInspector de ESET antes de usar esta tarea. Después de exportar el script, puede marcar los objetos que desea eliminar y ejecutar el script con los datos modificados; los objetos marcados se eliminarán.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

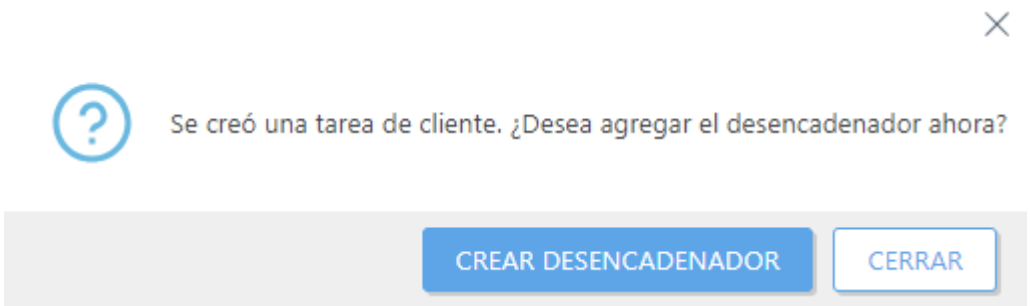
Configuración

- **Script de SysInspector**: haga clic en **Examinar** para navegar al script de servicio. El script de servicio se debe crear antes de ejecutar esta tarea.
- **Acción**: puede **Cargar** o **Descargar** un script desde la consola web de ESET PROTECT.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Una vez finalizada la tarea, puede revisar los resultados en un informe.

Actualización de componentes de ESET PROTECT

La tarea **ESET PROTECT Actualización de los componentes** se usa para actualizar los componentes de ESET PROTECT (agente ESET Management, servidor ESET PROTECT, consola web, ESET Bridge y MDM, pero no Apache Tomcat y Apache HTTP Proxy). La tarea de actualización únicamente puede ejecutarse en una máquina que tenga el Agente ESET Management instalado. El agente solo se requiere en un servidor ESET PROTECT.

ESET PROTECT On-Prem le notifica automáticamente cuando haya una nueva versión del servidor deESET PROTECT disponible.
Puede actualizar a ESET PROTECT On-Prem 11.0 desde ESET PROTECT On-Prem 9.0 y versiones posteriores. No se ha probado una actualización directa desde las versiones 7.2–8.x de fin de ciclo de vida y no se admite. Consulte la Guía de instalación para obtener instrucciones específicas.
Consulte también otras maneras de actualizar ESET PROTECT On-Prem a la versión más reciente.

Para evitar que falle la instalación, agente de ESET Management realiza las siguientes verificaciones antes de instalar o actualizar productor ESET:

- si se puede acceder al repositorio
- si hay suficiente espacio en el equipo del cliente (no disponible para Linux)

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

Configuración

Seleccione la casilla de verificación **Acepto el Acuerdo de licencia de usuario final y confirmo estar de acuerdo con la Política de privacidad**. Consulte el Acuerdo de licencia de usuario final (EULA), los Términos de uso y la Política de privacidad de los productos ESET.

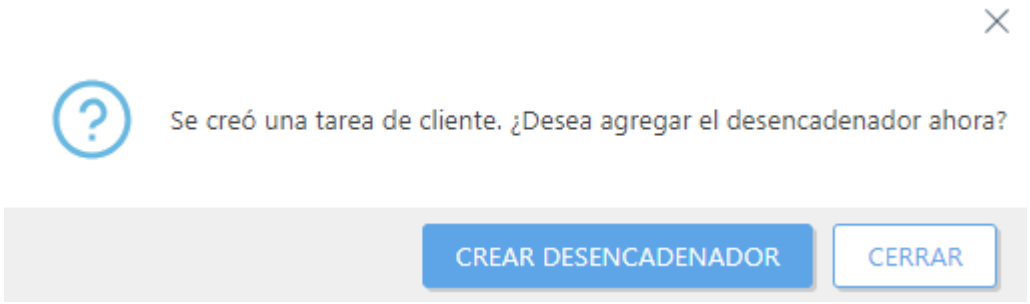
- **Servidor de referencia de ESET PROTECT**: seleccione la versión del servidor ESET PROTECT de la lista. Todos los componentes de ESET PROTECT se actualizarán a versiones compatibles con el servidor seleccionado.

Marque la casilla al lado de **Reiniciar automáticamente cuando sea necesario** si desea que el equipo cliente se reinicie automáticamente luego de la instalación. De manera alternativa, puede dejar esta opción sin seleccionar y el equipo cliente se puede reiniciar manualmente. Puede configurar el comportamiento de reinicio o apagado de los equipos administrados. El equipo debe ejecutar el Agente de ESET Management 9.1 y versiones posteriores, además de un producto de seguridad de ESET compatible con esta configuración.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

La actualización puede llevar más tiempo en función del sistema y la configuración de red. No puede acceder a Web Console durante la actualización del servidor de ESET PROTECT o Web Console. Tras la actualización, inicie sesión en Web Console y compruebe que tiene la versión más reciente de ESET PROTECT On-Prem en **Ayuda** > Acerca de.

Enviar archivo a ESET LiveGuard

Para ejecutar esta tarea, vaya a **Detecciones**.

La función **Enviar el archivo a ESET LiveGuard** se encuentra disponible solo para **archivos bloqueados**. El usuario puede enviar un archivo a análisis de malware (ESET LiveGuard Advanced) desde la ESET PROTECT Consola Web. Puede ver los detalles del análisis de archivos en Archivos enviados. Puede enviar manualmente archivos ejecutables para su análisis desde el producto de punto de conexión ESET ESET LiveGuard Advanced (necesita tener la licencia ESET LiveGuard Advanced).

Exploración del servidor

Puede usar la **tarea** Exploración del servidor para explorar clientes con la solución de ESET Server instalada. El tipo de ejecución de exploración depende de la solución de ESET instalada:

Producto	Explorar	Descripción
ESET Server Security para Windows (anteriormente ESET File Security para Microsoft Windows Server)	**Exploración de Hyper-V**	Este tipo de exploración le permite explorar los discos de un servidor Microsoft Hyper-V, que es una máquina virtual (VM), sin instalar el Agente de ESET Management en la VM.
ESET Security para Microsoft SharePoint Server	**Exploración de base de datos SharePoint, exploración de Hyper-V**	Esta funcionalidad permite que ESET PROTECT On-Prem use el destino de exploración apropiado cuando se ejecuta la tarea de cliente **Exploración del servidor** en un servidor con ESET Security para Microsoft SharePoint.
ESET Mail Security para Microsoft Exchange Server	**Exploración de base de datos de casillas de correo a pedido, exploración de Hyper-V**	Esta funcionalidad permite que ESET PROTECT On-Prem use el destino de exploración apropiado. Cuando ESET PROTECT On-Prem ejecuta una tarea de cliente **Exploración del servidor**, recopilará la lista de objetivos y se le pedirá que seleccione los destinos de exploración para la Exploración de base de datos de casillas de correo a pedido en ese servidor en particular.
ESET Mail Security para IBM Domino	**Exploración de base de datos a pedido, exploración de Hyper-V**	Esta funcionalidad permite que ESET PROTECT On-Prem use el destino de exploración apropiado cuando se ejecuta la tarea de cliente **Exploración del servidor** en un servidor con ESET Mail Security para IBM Domino.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

- Haga clic en **Seleccionar** en **Servidor explorado** y seleccione un equipo con el producto de ESET Server Security instalado. Se le pedirá que seleccione unidades, carpetas o archivos específicos para explorar en ese equipo.
- Seleccione un **Desencadenador** para esta tarea, puede configurar el límite si lo prefiere. De forma

predeterminada, la tarea se ejecuta en ASAP.

Destinos de exploración

ESET PROTECT On-Prem le ofrece una lista de destinos disponibles en el servidor seleccionado. Para usar esta lista, **Generar la lista de destinos** debe estar habilitada en la política para su producto de servidor en **Herramientas** > **Destinos de exploración de ESET Management:**

- **Generar lista de destinos**: habilite esta configuración para permitir que ESET PROTECT On-Prem genere listas de objetivos.
- **Período de actualización [minutos]**: generar la lista de destinos por primera vez llevará aproximadamente la mitad de este período.

Seleccione los destinos para explorar de la lista. Para obtener más información, consulte los destinos de exploración de ESET PROTECT On-Prem.

Resumen

Todas las opciones configuradas se visualizan aquí. Revise la configuración y haga clic **Finalizar**.

En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Apagar el equipo

Puede usar la tarea **Apagar el equipo** para apagar o reiniciar los equipos del cliente.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

Configuración

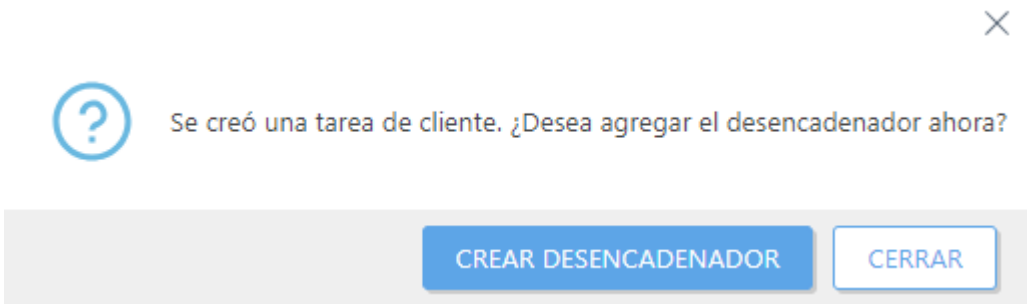
- **Reiniciar equipo(s)**: seleccione esta casilla de verificación si desea reiniciar el equipo de un cliente luego de completar la tarea. Si desea apagar los equipos, no la seleccione.

Puede configurar el comportamiento de reinicio o apagado de los equipos administrados. El equipo debe ejecutar el Agente de ESET Management 9.1 y versiones posteriores, además de un producto de seguridad de ESET compatible con esta configuración.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Instalación de software

Utilice la tarea **Instalación de software** para instalar el software en sus equipos cliente:

- Instale productos de seguridad ESET. También puede usar el menú contextual en **Equipos**. Haga clic en un equipo y seleccione **Soluciones** > **Instalar producto de seguridad** para instalar un producto de seguridad ESET en el equipo.
- Actualizar productos de seguridad de ESET Ejecute la tarea con el último paquete instalador para instalar la versión más reciente sobre su solución existente. Puede ejecutar inmediatamente una actualización del producto de seguridad ESET desde el **dashboard** con acciones con un clic. Vea instrucciones de actualización de ESET Security para Microsoft SharePoint para completar esta actualización.
- Instale software de terceros.

Tanto el servidor ESET PROTECT como el agente ESET Management deben tener acceso a Internet para poder acceder al repositorio y llevar a cabo instalaciones. Si no tiene acceso a Internet, debe instalar el software cliente en forma local, ya que la instalación remota fallará o creará un repositorio fuera de línea. Para evitar que falle la instalación, agente de ESET Management realiza las siguientes verificaciones antes de instalar o actualizar productor ESET:

- si se puede acceder al repositorio
- si hay suficiente espacio en el equipo del cliente (no disponible para Linux)

Al realizar una tarea de Instalación de software en equipos en un dominio con un agente ESET Management en ejecución, el usuario debe contar con permisos de *lectura* para la carpeta donde se almacenan los instaladores. Siga los pasos que se encuentran a continuación para otorgar estos permisos si es necesario.

1.Agregar una cuenta de equipo Active Directory en el equipo que está ejecutando la tarea (por ejemplo, *NewComputer$*).

2.Otorgue permisos de **Lectura** a *NewComputer$* haciendo clic derecho en la carpeta con los instaladores y seleccionando **Propiedades** > **Uso compartido** > **Compartir desde el menú contextual**. Tenga en cuenta que el símbolo "$" debe estar presente al final de la cadena del nombre del equipo.

La instalación desde una ubicación compartida solo es posible si el equipo cliente se encuentra en un dominio.

No use una tarea de Instalación de software para actualizar componentes de ESET PROTECT (agente, Servidor, MDM). Utilice en cambio la Tarea de actualización de componentes. Puede usar una tarea de Instalación de software para actualizar solo el componente Rogue Detection Sensor.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.

En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

Configuración

Paquete para instalar: hay dos opciones:

- **Instalar paquete del depósito**

  oElegir sistema operativo: seleccione el sistema operativo para la instalación del producto.

  oElegir paquete del repositorio: haga clic en **Seleccionar** y seleccione un paquete del instalador del producto de seguridad de ESET en el repositorio (por ejemplo, ESET Endpoint Security). Seleccione el idioma en el menú desplegable **Idioma**. De forma predeterminada, se selecciona previamente la versión más reciente (recomendada). Puede seleccionar una versión anterior. Para actualizar un producto ESET, seleccione la versión más reciente disponible. Si lo desea, haga clic en **Personalizar más ajustes** y

seleccione la versión del producto de ESET. Haga clic en **Ver registro de cambios** para ver el registro de cambios de la versión del producto seleccionada. Haga clic en **OK**.

oInstalar la versión más reciente: marque la casilla de verificación para instalar la versión más reciente del producto de ESET si ya aceptó el EULA del producto.

- **Instalar por URL de paquete directo**: para especificar una URL con el paquete de instalación, escriba o copie y pegue la URL en el campo de texto (no utilice una URL que requiera autenticación):

o*http://server_address/ees_nt64_ENU.msi*: si realiza la instalación desde un servidor web público o desde su propio servidor HTTP.

o*file://\\pc22\install\ees_nt64_ENU.msi*: si realiza la instalación desde una ruta de red.

o*file://C:\installs\ees_nt64_ENU.msi*: si realiza la instalación desde una ruta local.

Licencia de ESET Seleccione la licencia adecuada del producto de la lista de licencias disponibles. La licencia activará el producto de seguridad de ESET durante la instalación. La lista de licencias disponibles no muestra las licencias vencidas o sobreusadas (aquellas que están en estado **Error** u **Obsoleto**). Si no selecciona una licencia, puede instalar el producto de seguridad de ESET sin la licencia y activar el producto más tarde. Puede agregar una licencia a través de uno de los métodos que se describen en Administración de licencias. La adición o eliminación de licencias está restringida al administrador cuyo grupo de pertenencia sea **Todo** y que tenga el permiso de **Escritura** en las licencias.

- Seleccione una licencia únicamente cuando instale o actualice productos que no estén activos, o si desea cambiar la licencia que usa actualmente a una licencia diferente.

- No seleccione una licencia al actualizar un producto ya activado.

Activar ESET LiveGuard: la casilla de verificación está disponible si tiene una licencia ESET LiveGuard Advanced y ha seleccionado un producto de seguridad ESET compatible con ESET LiveGuard Advanced y la licencia del producto. Marque la casilla de verificación para activar ESET LiveGuard Advanced en los equipos de destino de la tarea Instalación de software. Luego de la activación puede administrar la configuración de ESET LiveGuard Advanced mediante una política.

Seleccione la casilla de verificación **Acepto el Acuerdo de licencia de usuario final y confirmo estar de acuerdo con la Política de privacidad**. Consulte el Acuerdo de licencia de usuario final (EULA), los Términos de uso y la Política de privacidad de los productos ESET.

Si ha seleccionado un producto de seguridad ESET para Windows:Marque la casilla de verificación que se encuentra junto a la configuración para habilitarla para el instalador:

oHabilite el sistema de respuesta ESET LiveGrid® (recomendado)

oHabilite la detección de aplicaciones potencialmente no deseadas: obtenga más información en nuestro artículo de la base de conocimiento.

Parámetros de instalación (opcional):

- Use los parámetros de instalación de líneas de comando únicamente con las configuraciones de interfaz del usuario **reducida**, **básica** y **ninguna**.

- Consulte la documentación de la versión **msiexec** usada para las modificaciones de líneas de comandos

correspondientes.

- Lea la ayuda en línea correspondiente con respecto a la instalación desde la línea de comandos de los productos de punto de conexión de ESET y los productos de servidor de ESET.

Marque la casilla al lado de **Reiniciar automáticamente cuando sea necesario** si desea que el equipo cliente se reinicie automáticamente luego de la instalación. De manera alternativa, puede dejar esta opción sin seleccionar y el equipo cliente se puede reiniciar manualmente. Puede configurar el comportamiento de reinicio o apagado de los equipos administrados. El equipo debe ejecutar el Agente de ESET Management 9.1 y versiones posteriores, además de un producto de seguridad de ESET compatible con esta configuración.

Instalación de software de terceros

Puede usar la tarea **Instalación de software** para instalar software que no sea de ESET (terceros).

Sistema operativo	Tipos de archivo de instalación compatibles	Compatibilidad con los parámetros de instalación
Windows	*.msi*	La tarea Instalación de software realiza la instalación silenciosa de paquetes *.msi*. No es posible especificar parámetrosmsiexec. Sólo puede especificar parámetros usados por el paquete de instalación mismo (único para cada paquete de instalación de software).
Linux	*.deb*, *.rpm*, *.sh*	Solo puede usar parámetros con archivos *.sh* (*.deb* y *.rpm* no son compatibles con los parámetros).
macOS	*.pkg*, *.dmg* (contiene el archivo *.pkg*	Los parámetros de instalación no son compatibles.
Android	*.apk*	Los parámetros de instalación no son compatibles.
iOS	*.ipa*	Los parámetros de instalación no son compatibles.

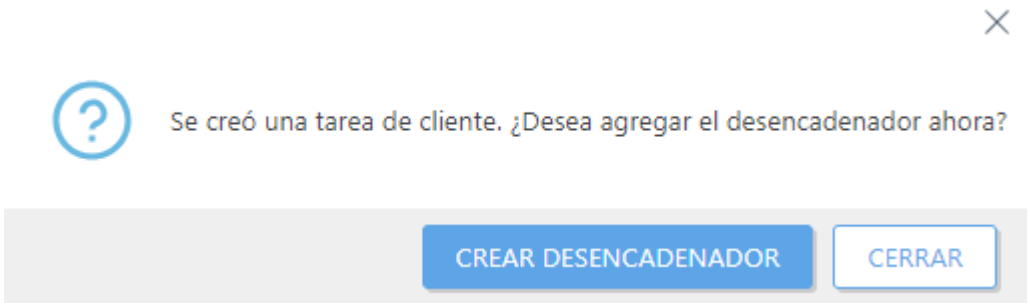
Usted desea instalar software en Linux con el archivo *install_script.sh* que tiene dos parámetros: `-a` es el primer parámetro, `-b` es el segundo parámetro.
Instalación en la terminal (como usuario raíz en la carpeta donde *se encuentra install_script.sh*):
`./install_script.sh -a parameter_1 -b parameter_2`
Instalación mediante la tarea de Instalación de software:
- Ingrese la ruta del archivo en **Instalar por URL de paquete directo**, por ejemplo: *file:///home/user/Desktop/install_script.sh*
- Ingrese los **parámetros de instalación**: `-a parameter_1 -b parameter_2`.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.

- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Listado de problemas cuando falla la instalación

- No se encontró el paquete de instalación.

- Se requiere una versión más reciente del servicio Windows Installer.

- Ya se encuentra instalada otra versión o un producto conflictivo.

- Se está realizando otra instalación. Complete esa instalación antes de continuar con esta.
- La instalación o desinstalación finalizó correctamente, pero debe reiniciar el equipo.
- Error de la tarea: se ha producido un error. Debe revisar el registro de seguimiento del Agente y verificar el código de devolución del instalador.

Software Safetica

¿Qué es Safetica?

Safetica es una empresa de software de terceros y miembro de ESET Technology Alliance. Safetica ofrece una solución de seguridad de TI para la prevención de pérdida de datos y es adicional a las soluciones de seguridad de ESET. Las características principales del software de Safetica incluyen:

- Prevención de pérdida de datos - controla todos los discos duros, unidades USB, transferencias de archivos de red, correos electrónicos e impresoras, así como el acceso a archivos de aplicaciones
- Generación de informes y bloqueo de actividades - para operaciones de archivos, sitios web, correos electrónicos, mensajería instantánea, uso de aplicaciones y palabras clave buscadas

Cómo funciona Safetica

Safetica implementa un agente, Safetica Endpoint Client, en los endpoints (puntos finales) deseados y mantiene una conexión regular con ellos a través del servidor, Safetica Management Service. Este servidor crea una base de datos de la actividad de las estaciones de trabajo y distribuye nuevas políticas y normas de protección de datos a cada estación de trabajo.

Integración de Safetica en ESET PROTECT On-Prem

El Agente ESET Management detecta e informa el software de Safetica como software de ESET en **Detalles del equipo** > Aplicaciones instaladas. La consola web de ESET PROTECT actualizará el agente de Safetica si hay alguna versión nueva disponible.

Implementar el agente Safetica

Puede implementar el agente de Safetica directamente desde la consola web de ESET PROTECT desde el repositorio del software de ESET utilizando la tarea Instalación del software y escribiendo `STSERVER=Server_name` en los **Parámetros de instalación** (`Server_name` es el nombre de host o la dirección IP del servidor en el que está instalado el **servicio de administración de Safetica**) .

También puede instalar el agente de Safetica con la tarea del cliente Ejecutar comando.

Usar la tarea Ejecutar comando

```
msiexec /i safetica_agent.msi STSERVER=Server_name
```

Puede usar el parámetro `/silent` al final del comando para ejecutar la instalación de forma remota en un modo «silencioso»: `msiexec /i safetica_agent.msi STSERVER=Server_name /silent`
Para realizar la instalación mencionada, el paquete .msi ya debe encontrarse en el dispositivo. Para ejecutar la tarea de instalación cuando el paquete *.msi* está en una ubicación compartida, especifique la ubicación en el comando de la siguiente manera: `msiexec /i Z:\sharedLocation\safetica_agent.msi STSERVER=Server_name`

Actualizar Safetica agente

Para actualizar el agente de Safetica en un equipo administrado, vaya a **Detalles del equipo** > Aplicaciones instaladas > seleccione **agente** de **Safetica** y haga clic en **Actualizar productos ESET**.

Desinstalar el Agente Safetica

Para desinstalar el agente de Safetica de un equipo administrado, vaya a **Detalles del equipo** > Aplicaciones instaladas > seleccione **agente** de **Safetica** y haga clic en **Desinstalar**.

Desinstalación de software

La tarea **Desinstalación de software** se usa para desinstalar los productos de ESET de los equipos de los clientes, cuando ya no se desean o necesitan más.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**.
Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

Configuración

Configuración de desinstalación de software

Seleccione una opción en el menú desplegable **Desinstalar**:

Aplicación de la lista

- **Nombre del paquete**: Seleccione un componente de ESET PROTECT, un producto de seguridad del cliente o una aplicación de terceros. Puede activar los informes de aplicaciones de terceros (que no son de ESET) a

través de la configuración de la política del agente. Todos los paquetes que pueden desinstalarse de los clientes seleccionados se visualizan en esta lista.

Cuando desinstala el agente ESET Management del equipo del cliente, el dispositivo ya no es administrado por ESET PROTECT On-Prem:
• El producto de seguridad de ESET puede conservar algunas configuraciones después de desinstalar el agente ESET Management.
• Si el agente ESET Management está protegido por contraseña, debe proporcionar la contraseña para desinstalar, reparar o actualizar (con cambios). 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.

• **Versión del paquete:** puede eliminar una versión específica del paquete (a veces, una versión específica puede causar problemas) o **desinstalar todas las versiones de un paquete**.

• **Parámetros de desinstalación**: Puede especificar parámetros para la desinstalación.

• Marque la casilla al lado de **Reiniciar automáticamente cuando sea necesario** si desea que el equipo cliente se reinicie automáticamente luego de la instalación. De manera alternativa, puede dejar esta opción sin seleccionar y el equipo cliente se puede reiniciar manualmente. Puede configurar el comportamiento de reinicio o apagado de los equipos administrados. El equipo debe ejecutar el Agente de ESET Management 9.1 y versiones posteriores, además de un producto de seguridad de ESET compatible con esta configuración.

Software antivirus de terceros (fabricado con OPSWAT)

Puede activar los informes de aplicaciones de terceros (que no son de ESET) a través de la configuración de la política del agente.

Para ver un listado de Software AV compatible, consulte nuestro Artículo de la base de conocimiento. Esta eliminación es diferente de la desinstalación desde **Agregar o quitar programas**. Usa métodos alternativos para quitar software antivirus de terceros en su totalidad, incluidas las entradas de registro residuales y otros rastros.

Siga las instrucciones paso a paso del artículo Eliminar software antivirus de terceros de los equipos cliente usando ESET PROTECT On-Prem para enviar una tarea para quitar software de antivirus de terceros de equipos cliente.

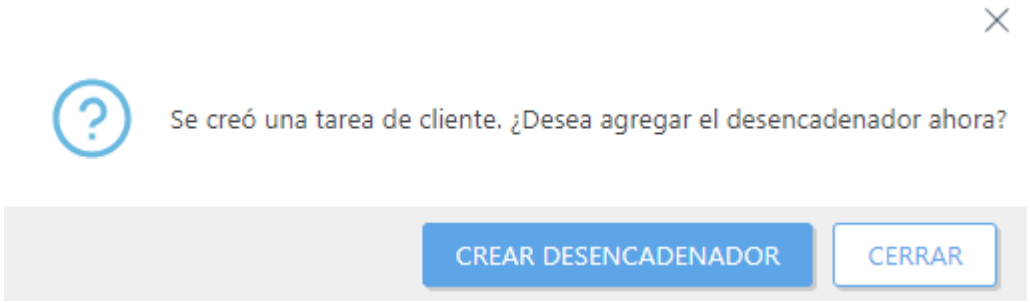
Si desea permitir la no desinstalación de aplicaciones protegidas por contraseña, consulte nuestro artículo en la Base de conocimiento.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

• Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.

• Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

La tarea de desinstalación del producto de seguridad ESET puede fallar debido a un error relacionado con la contraseña, por ejemplo: **Producto: ESET Endpoint Security -- Error 5004. Ingrese una contraseña válida para proseguir con la desinstalación**. Esto se debe a una configuración de protección con contraseña habilitada en el producto de seguridad ESET. Aplicar una política al equipo del cliente para elliminar la protección con contraseña. Luego puede desinstalar el producto de seguridad ESET mediante la tarea de desinstalación de software.

Detener administración (desinstalar agente ESET Management)

Esta tarea desinstala el agente ESET Management de los dispositivos destino seleccionados. Si se selecciona un equipo, la tarea eliminará el agente ESET Management. Si se selecciona un dispositivo móvil, esta tarea cancelará la inscripción de MDM de su dispositivo.

Cuando desinstala el agente ESET Management del equipo del cliente, el dispositivo ya no es administrado por ESET PROTECT On-Prem:
• El producto de seguridad de ESET puede conservar algunas configuraciones después de desinstalar el agente ESET Management.
• Si el agente ESET Management está protegido por contraseña, debe proporcionar la contraseña para desinstalar, reparar o actualizar (con cambios). 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.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

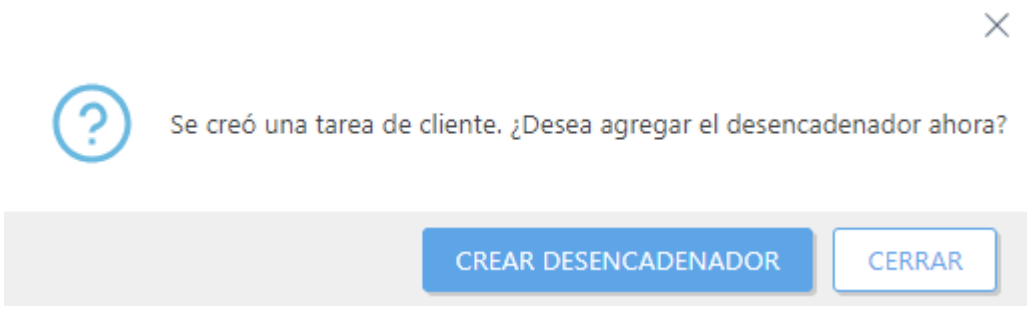
En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

No hay una **configuración** disponible para esta tarea.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Solicitud de registro de SysInspector (Windows únicamente)

La tarea **Solicitud de registro de SysInspector** se usa para solicitar el registro de SysInspector de un producto de seguridad del cliente.

ESET SysInspector solo se ejecuta en equipos Windows.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**. Puede

ejecutar esta tarea también desde **Equipos**, haga clic en un equipo > **Detalles** > **Registros** > **Solicitar registro (Windows únicamente).**

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

Configuración

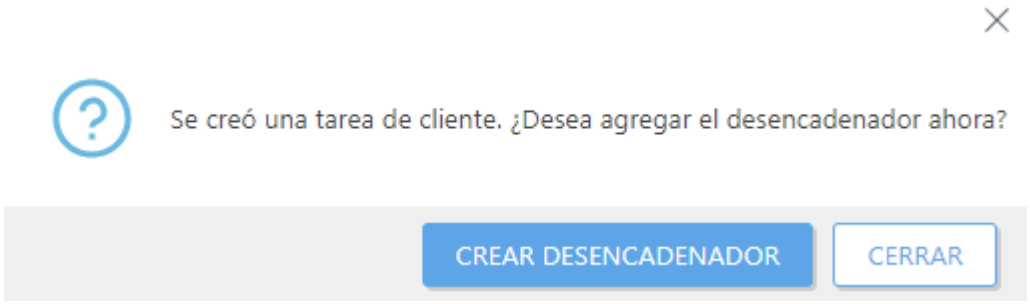
- **Almacenar el registro en el cliente**: seleccione esta opción si desea almacenar el registro de SysInspector en el cliente así como en el servidor de ESET PROTECT. Por ejemplo, cuando un cliente tiene ESET Endpoint Security instalado, el registro se suele almacenar en *C:\Program Data\ESET\ESET Security\SysInspector*.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.

- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Una vez completada la tarea, se muestra una nueva entrada en la lista de registros de ESET SysInspector. Haga clic en un registro de la lista para explorarlo.

Carga de archivo en cuarentena

La tarea **Cargar archivo en cuarentena** se usa para administrar archivos en cuarentena en los clientes. Puede cargar un archivo en cuarentena a una ubicación específica para investigar más a fondo.

Seleccione una de las siguientes opciones para crear una nueva tarea del cliente:

- Haga clic en **Tareas** > **Nueva** > **Tarea de cliente**.
- Haga clic en **Tareas** > seleccione el tipo de tarea deseada y haga clic en **Nueva** > **Tarea de cliente**.
- Haga clic en el dispositivo de destino en **Ordenadores** y seleccione **Tareas** > **Nueva tarea**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

Configuración

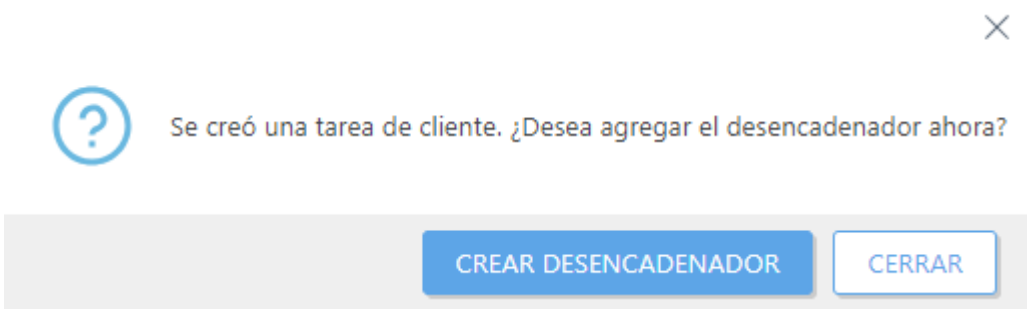
- **Objeto en cuarentena**: seleccione un objeto específico de la cuarentena.
- **Contraseña del objeto**: escriba una contraseña para cifrar el objeto por motivos de seguridad. ingrese una contraseña para cifrar el objeto por razones de seguridad. Tenga en cuenta que la contraseña se mostrará en el informe correspondiente.
- **Cargar ruta**: ingrese una ruta a la ubicación donde desea cargar el objeto. Use la siguiente sintaxis: *smb://server/share*
- **Cargar nombre de usuario/contraseña**: en caso de que la ubicación requiera autenticación (recurso compartido de red, etc.), ingrese las credenciales para acceder a esta ruta. Si el usuario está en un dominio, utilice el formato `DOMAIN\username`.

> En el desencadenador, asegúrese de seleccionar el destino en el que se pondrá el archivo en cuarentena.

Resumen

Revise el resumen de la configuración y haga clic en **Finalizar**. Se crea la Tarea de cliente u se abrirá una ventana pequeña:

- Haga clic en Crear desencadenador (recomendado) para especificar destinos de la tarea del cliente (equipos o grupos) y el desencadenador.
- Si hace clic en **Cerrar**, puede crear un Desencadenador más tarde: haga clic en la instancia Tarea del cliente y seleccione **Ejecutar en** del menú desplegable.



En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Una vez que el archivo puesto en cuarentena se carga en la ubicación de la **Ruta de carga** seleccionada:

- El archivo se almacena en un archivo *.zip* protegido por contraseña. La contraseña es el nombre del archivo *.zip* (hash del archivo puesto en cuarentena).
- El archivo puesto en cuarentena no tiene extensión de archivo. Para restaurar el archivo, agregue la extensión del archivo original.

Tareas del servidor

ESET PROTECT Server se ocupa de ejecutar las tareas del servidor en sí mismo o en otros dispositivos. Las tareas del servidor no se pueden asignar a ningún cliente o grupo de clientes específicos. Cada tarea del servidor puede tener un desencadenador configurado. Si la tarea debe ser ejecutada con varios eventos, se necesita contar una tarea del servidor diferente para cada desencadenador.

Tareas del servidor

- Implementación del agente
- Eliminar equipos sin conexión
- Generar informe
- Cambiar el nombre de los equipos
- Sincronización de grupos estáticos
- Sincronización de usuario

Tareas y permisos del servidor

La tarea y el desencadenador necesitan de un usuario ejecutor. Este es el usuario que modifica la tarea (y el desencadenador). Este usuario debe contar con los permisos suficientes para la tarea seleccionada. Durante la ejecución, la tarea siempre toma el usuario ejecutador del desencadenador. Si la tarea se ejecuta con la configuración **Ejecutar la tarea inmediatamente luego de finalizar**, el usuario ejecutador es el usuario conectado a la consola web ESET PROTECT. Un usuario tiene permisos (**Lectura**, **Uso**, **Escritura**) para la instancia de **tarea del servidor** seleccionada si cuenta con esos permisos seleccionados en su conjunto de permisos (**Más** > **Conjuntos de permisos**) y tiene estos conjuntos para el grupo estático donde se encuentra la tarea de servidor. Consulte la lista de permisos para obtener más información sobre los derechos de acceso.

John, cuyo grupo hogar es *Grupo de John*, desea eliminar la *Tarea del servidor 1:* **Generar informe**. La tarea fue creada originalmente por *Larry*, por lo que automáticamente se encuentra en el grupo hogar de Larry, *Grupo de Larry*. Se deben cumplir las siguientes condiciones para que *John* pueda eliminar la tarea:
- *John* debe tener un conjunto de permisos con permisos de **Escritura** para **Tareas y desencadenadores del servidor** - **Generar informes**.
- El conjunto de permisos debe contener al *Grupo de Larry* en **Grupos estáticos**.

Permisos necesarios para ciertas acciones de tareas de servidor

- Para crear una nueva tarea del servidor, el usuario necesita permisos de **escritura** para el tipo de tarea seleccionada y derechos de acceso para los objetos referenciados (equipos, licencias, grupos).

- Para modificar una nueva tarea del servidor, el usuario necesita permisos de **escritura** para el tipo de instancias de tarea del servidor y derechos de acceso adecuados para los objetos referenciados (equipos, licencias, grupos).

- Para eliminar una tarea del servidor, el usuario necesita permisos de **escritura** para la instancia de tarea del servidor seleccionada.

- Para ejecutar una tarea del servidor, el usuario necesita permisos de **uso** para la instancia de tarea del servidor seleccionada.

Crear una nueva tarea del servidor

1. Para crear una nueva tarea del servidor, haga clic en **Tareas** > **Nueva** > **Tarea de servidor** o seleccione el tipo de tarea deseada a la izquierda y haga clic en **Nueva** > **Tarea de servidor**.

2. En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

También puede seleccionar de la siguiente configuración del desencadenador de tareas:

- **Ejecutar tarea inmediatamente luego de finalizar**: seleccione esta opción para que la tarea se ejecute luego de hacer clic en Finalizar.

- **Configurar desencadenador**: seleccione esta opción para habilitar la sección Desencadenador, donde puede configurarlo.

Para configurar el desencadenador más adelante, deje las casillas de verificación sin marcar.

3. Configure la tarea en la sección **Configuración**.

4. Configure el desencadenador en la sección **Desencadenador**, si está disponible.

5. Verifique todas las configuraciones para esta tarea en la sección **Resumen** y, luego, haga clic en **Finalizar**.

> Se recomienda que los usuarios que utilicen tareas del servidor normalmente para crear sus propias tareas en lugar de compartirlas con otros usuarios. Cada vez que se ejecuta la tarea utiliza los permisos del usuario ejecutor. Esto puede ser confuso para algunos usuarios.

Implementación del agente

La tarea del servidor de instalación de agente se ocupa de la instalación remota del agente de ESET Management.

> La tarea de implementación de agente ejecuta la instalación del agente ESET Management en equipos de destino uno por uno (de forma secuencial). Como resultado, cuando ejecuta la tarea de instalación de agente en muchos equipos cliente, puede tardar mucho tiempo en completarse. Por lo tanto, le recomendamos usar, en cambio, ESET Remote Deployment Tool. Ejecuta la instalación del agente de ESET Management en todos los equipos de destino al mismo tiempo (en paralelo), y además ahorra ancho de banda de la red mediante el uso de archivos de instalación locales; sin acceder al repositorio en línea.

Para crear una nueva tarea del servidor, haga clic en **Tareas** > **Nueva** > **Tarea de servidor** o seleccione el tipo de tarea deseada a la izquierda y haga clic en **Nueva** > **Tarea de servidor**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**.
Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

También puede seleccionar de la siguiente configuración del desencadenador de tareas:

- **Ejecutar tarea inmediatamente luego de finalizar**: seleccione esta opción para que la tarea se ejecute luego de hacer clic en Finalizar.
- **Configurar desencadenador**: seleccione esta opción para habilitar la sección Desencadenador, donde puede configurarlo.

Para configurar el desencadenador más adelante, deje las casillas de verificación sin marcar.

Configuración de implementación del agente

Destinos: haga clic aquí para seleccionar los clientes que recibirán esta tarea.

> Si se agregaron equipos de destino a ESET PROTECT On-Prem usando la tarea Sincronización de grupos estáticos, asegúrese de que los nombres de los equipos sean sus nombres de dominio completos. Estos nombres se utilizan como direcciones del cliente durante la implementación; si no son correctos, la implementación falla. Use el atributo `dNSHostName` como **Atributo de nombre de host del equipo** durante la sincronización para fines de implementación del agente.

Nombre de host del servidor (opcional): puede ingresar un nombre de host del servidor si es diferente del lado del cliente y del lado del servidor.

Credenciales de equipos de destino

Nombre de usuario y contraseña: el nombre de usuario y la contraseña para el usuario con los derechos suficientes como para realizar una instalación remota del agente.

Configuración de certificados

Certificado de pares:

- **certificado ESET PROTECT**: se seleccionan automáticamente un certificado de pares para la instalación del agente y la autoridad de certificación de ESET PROTECT. Para utilizar un certificado diferente, haga clic en **Descripción del certificado de ESET PROTECT** para seleccionarlo en el menú desplegable de los certificados disponibles.

- **Certificado personalizado**: si utiliza un certificado personalizado para la autenticación, haga clic en **Certificado personalizado** > **Seleccionar**, cargue el certificado .pfx y selecciónelo al instalar el agente. Para obtener más información, consulte Certificados.

Frase de contraseña del certificado: escriba la frase de contraseña del certificado si es necesario: si especificó la contraseña durante la instalación del servidor ESET PROTECT (en el paso en el que creó una autoridad certificadora) o si utiliza un certificado personalizado con contraseña. De lo contrario, deje el campo **Frase de contraseña del certificado** en blanco.

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

El servidor ESET PROTECT puede seleccionar el paquete de instalación del agente adecuado para los sistemas operativos de forma automática:

- Linux: seleccione un usuario con permiso para usar el comando `sudo` o el usuario `root`. Si se utiliza `root`, el servicio `ssh` debe permitirle iniciar sesión como `root`.

- Linux o macOS: asegúrese de que el equipo de destino tenga el daemon SSH habilitado y en ejecución en el puerto 22, y que no haya un firewall que bloquee esta conexión. Use el siguiente comando (reemplace la dirección IP con la IP de su servidor ESET PROTECT) para agregar una excepción en el firewall de Linux:
```
iptables -A INPUT -s 10.0.0.1 -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

- Para evitar que la tarea de implementación de agente falle, consulte la Resolución de problemas de implementación de agente.

Otra configuración

Seleccione la casilla de verificación **Participar en el programa de mejora del producto** para 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).

Desencadenador

La sección **Desencadenador** contiene información sobre los desencadenadores que ejecutarán una tarea. Cada **Tarea del servidor** puede tener hasta un desencadenador. Cada desencadenador solo puede ejecutar una **Tarea del servidor**. Si no se selecciona **Configurar desencadenador** en la sección **Básico**, no se crea un desencadenador. Se puede crear una tarea sin un desencadenador. Dicha tarea se puede ejecutar manualmente o se puede agregar un desencadenador en otro momento.

Configuración avanzada: Umbral

Al configurar un límite, puede establecer reglas avanzadas para el desencadenador creado. Establecer un límite es opcional.

Resumen

Todas las opciones configuradas se visualizan aquí. Revise la configuración y haga clic **Finalizar**.

En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Solución de problemas

Si la tarea de implementación de agente falla, consulte la Resolución de problemas de implementación de agente.

> ⚠ Para volver a implementar el agente ESET Management, no quite nunca el agente instalado actualmente. Ejecute la tarea de implementación de agente en el agente instalado actualmente. Cuando quita el agente, el agente nuevo puede comenzar a ejecutar tareas antiguas después de la nueva implementación.

Eliminar equipos sin conexión

La tarea **Eliminar equipos sin conexión** le permite eliminar equipos de acuerdo con el criterio especificado. Por ejemplo, si el agente ESET Management en un equipo cliente no se conectó durante 30 días, se eliminará de la consola web ESET PROTECT.

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

- Amarillo (error): hace de 2 a 14 días que el equipo no se conecta.
- Rojo (advertencia): hace más de 14 días que no se conecta el equipo.

Para crear una nueva tarea del servidor, haga clic en **Tareas** > **Nueva** > **Tarea de servidor** o seleccione el tipo de tarea deseada a la izquierda y haga clic en **Nueva** > **Tarea de servidor**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

También puede seleccionar de la siguiente configuración del desencadenador de tareas:

- **Ejecutar tarea inmediatamente luego de finalizar**: seleccione esta opción para que la tarea se ejecute luego de hacer clic en Finalizar.

- **Configurar desencadenador**: seleccione esta opción para habilitar la sección Desencadenador, donde puede configurarlo.

Para configurar el desencadenador más adelante, deje las casillas de verificación sin marcar.

Configuración

Nombre de grupo - seleccione un grupo estático o cree un nuevo grupo estático donde se cambiará el nombre de los equipos.

Número de días sin conexión del equipo: escriba el número de días después del que se eliminarán los equipos.

Desactivar licencia: marque esta casilla para desactivar las licencias de los equipos que se han quitado.

Eliminar equipos no administrados:: marque esta casilla de verificación para quitar también los equipos no administrados.

Desencadenador

La sección **Desencadenador** contiene información sobre los desencadenadores que ejecutarán una tarea. Cada **Tarea del servidor** puede tener hasta un desencadenador. Cada desencadenador solo puede ejecutar una **Tarea del servidor**. Si no se selecciona **Configurar desencadenador** en la sección **Básico**, no se crea un desencadenador. Se puede crear una tarea sin un desencadenador. Dicha tarea se puede ejecutar manualmente o se puede agregar un desencadenador en otro momento.

Configuración avanzada: Umbral

Al configurar un límite, puede establecer reglas avanzadas para el desencadenador creado. Establecer un límite es opcional.

Resumen

Todas las opciones configuradas se visualizan aquí. Revise la configuración y haga clic **Finalizar**.

En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Generar informe

La tarea **Generar informe** sirve para generar informes a partir de plantillas de informe creadas o predefinidas anteriormente.

Para crear una nueva tarea del servidor, haga clic en **Tareas** > **Nueva** > **Tarea de servidor** o seleccione el tipo de tarea deseada a la izquierda y haga clic en **Nueva** > **Tarea de servidor**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.

En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

También puede seleccionar de la siguiente configuración del desencadenador de tareas:

- **Ejecutar tarea inmediatamente luego de finalizar**: seleccione esta opción para que la tarea se ejecute luego de hacer clic en Finalizar.
- **Configurar desencadenador**: seleccione esta opción para habilitar la sección Desencadenador, donde puede configurarlo.

Para configurar el desencadenador más adelante, deje las casillas de verificación sin marcar.

Configuración

Plantillas de informe: haga clic en Agregar plantilla de informe para seleccionar una plantilla de informe de la lista. El usuario que crea la tarea podrá ver y seleccionar solo las plantillas de informe disponibles en su grupo. Puede seleccionar múltiples plantillas de informe para un informe.

Los usuarios de MSP pueden filtrar el informe seleccionando el cliente.

Seleccione Enviar correo electrónico o Guardar en archivo para obtener el informe generado.

Envío de informes

Enviar correo electrónico

Para enviar o recibir mensajes de correo, debe establecer las configuraciones del SMTP en **Más** > Configuración > **Configuraciones avanzadas**.

- **Enviar a**: ingrese las direcciones de correo electrónico de los receptores para correos electrónicos de informes. Separe múltiples direcciones con una coma (,). También puede agregar un campo CC y BCC; estos funcionan exactamente de la misma forma que para los clientes de correo.
- ESET PROTECT On-Prem escribe previamente el asunto y el cuerpo del correo electrónico basado en la plantilla de informe seleccionada. Puede seleccionar la casilla de verificación debajo de **Personalizar mensaje** para personalizar el **asunto** y el **mensaje**:
  - **Asunto**: asunto del mensaje de informe. Ingrese un asunto específico, para que se puedan clasificar los mensajes entrantes. Esta es una configuración opcional, pero le recomendamos que no la deje vacía.
  - **Mensaje**: defina el cuerpo del mensaje de informe.
- **Enviar correo electrónico si el informe está vacío**: use esta opción si desea enviar el informe incluso si no contiene ningún dato.

Haga clic en **Mostrar opciones de impresión** para visualizar la siguiente configuración:

- **Formato de salida**: seleccione el formato de archivo adecuado. Puede seleccionar entre *.pdf* o *.csv*. CSV es apto únicamente para datos de tablas y usa ; (punto y coma) como delimitador Si descarga un informe de CSV y ve los números en una columna en la que esperaba ver texto, le recomendamos descargar un informe

de PDF para ver los valores de texto.

> Seleccionar CSV hace que los valores de fecha y hora de su informe se almacenen en formato UTC. Si selecciona PDF, el informe usará la hora local del servidor.

- **Idioma de salida**: seleccione el idioma del mensaje. El idioma predeterminado se basa en el idioma seleccionado para la consola web ESET PROTECT.

- **Tamaño de página/Resolución/Orientación del papel/Formato de color/Unidades de margen/Márgenes**: seleccione las opciones adecuadas en función de sus preferencias de impresión. Estas opciones son relevantes si desea imprimir el informe, y solo se aplican al formato PDF, no al formato CSV.

Guardar en archivo

- **Ruta de archivo relativo**: el informe se generará en un directorio específico, por ejemplo:

  *o*Para Windows, los informes se colocan normalmente en*C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Data\GeneratedReports*

  *o*Para Linux, los informes se colocan normalmente en/var/opt/eset/RemoteAdministrator/Server/GeneratedReports/

> En Windows, algunos caracteres especiales (`: ? \`) no se interpretarán correctamente en el nombre del archivo almacenado.

- **Guardar archivo si el informe está vacío**: use esta opción si desea guardar el informe incluso si no contiene ningún dato.

Haga clic en **Mostrar opciones de impresión** para visualizar la siguiente configuración:

- **Formato de salida**: seleccione el formato de archivo adecuado. Puede seleccionar entre *.pdf* o *.csv*. CSV es apto únicamente para datos de tablas y usa `;` (punto y coma) como delimitador Si descarga un informe de CSV y ve los números en una columna en la que esperaba ver texto, le recomendamos descargar un informe de PDF para ver los valores de texto.

> Seleccionar CSV hace que los valores de fecha y hora de su informe se almacenen en formato UTC. Si selecciona PDF, el informe usará la hora local del servidor.

- **Idioma de salida**: seleccione el idioma del mensaje. El idioma predeterminado se basa en el idioma seleccionado para la consola web ESET PROTECT.

- **Tamaño de página/Resolución/Orientación del papel/Formato de color/Unidades de margen/Márgenes**: seleccione las opciones adecuadas en función de sus preferencias de impresión. Estas opciones son relevantes si desea imprimir el informe, y solo se aplican al formato PDF, no al formato CSV.

Desencadenador

La sección **Desencadenador** contiene información sobre los desencadenadores que ejecutarán una tarea. Cada **Tarea del servidor** puede tener hasta un desencadenador. Cada desencadenador solo puede ejecutar una **Tarea**

del servidor. Si no se selecciona **Configurar desencadenador** en la sección **Básico**, no se crea un desencadenador. Se puede crear una tarea sin un desencadenador. Dicha tarea se puede ejecutar manualmente o se puede agregar un desencadenador en otro momento.

Configuración avanzada: Umbral

Al configurar un límite, puede establecer reglas avanzadas para el desencadenador creado. Establecer un límite es opcional.

Resumen

Todas las opciones configuradas se visualizan aquí. Revise la configuración y haga clic **Finalizar**.

En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Cambiar el nombre de los equipos

Puede usar la tarea **Cambiar el nombre de los equipos** para cambiar el nombre de los equipos a formato FQDN en ESET PROTECT On-Prem. Puede usar una tarea de servidor existente que esté predeterminada con su instalación de ESET PROTECT On-Prem. Si el nombre de un dispositivo cliente es diferente del que se encuentra en la información del dispositivo, ejecutar esta tarea puede restaurar el nombre adecuado.

La tarea cambia automáticamente el nombre de sus equipos sincronizados en el grupo **Perdidos y encontrados** cada hora.

Para crear una nueva tarea del servidor, haga clic en **Tareas** > **Nueva** > **Tarea de servidor** o seleccione el tipo de tarea deseada a la izquierda y haga clic en **Nueva** > **Tarea de servidor**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**.
Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

También puede seleccionar de la siguiente configuración del desencadenador de tareas:

- **Ejecutar tarea inmediatamente luego de finalizar**: seleccione esta opción para que la tarea se ejecute luego de hacer clic en Finalizar.
- **Configurar desencadenador**: seleccione esta opción para habilitar la sección Desencadenador, donde puede configurarlo.

Para configurar el desencadenador más adelante, deje las casillas de verificación sin marcar.

Configuración

Nombre del grupo: seleccione un grupo estático o dinámico, o cree un Nuevo grupo estático o dinámico para los equipos a los que se les cambió el nombre.

Cambiar el nombre según:

- **Nombre del equipo**: cada equipo se identifica en la red local por su nombre único de equipo
- **FQDN (nombre de dominio completamente calificado) del equipo**: empieza con el nombre de host y continúa con los nombre de dominio hasta el nombre de dominio de nivel superior.

Desencadenador

La sección **Desencadenador** contiene información sobre los desencadenadores que ejecutarán una tarea. Cada **Tarea del servidor** puede tener hasta un desencadenador. Cada desencadenador solo puede ejecutar una **Tarea del servidor**. Si no se selecciona **Configurar desencadenador** en la sección **Básico**, no se crea un desencadenador. Se puede crear una tarea sin un desencadenador. Dicha tarea se puede ejecutar manualmente o se puede agregar un desencadenador en otro momento.

Configuración avanzada: Umbral

Al configurar un límite, puede establecer reglas avanzadas para el desencadenador creado. Establecer un límite es opcional.

Resumen

Todas las opciones configuradas se visualizan aquí. Revise la configuración y haga clic **Finalizar**.

En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Sincronización de grupos estáticos

La tarea **Sincronización de grupos estáticos** buscará equipos en su red (Active Directory, open Directory, LDAP, red local o VMware) y los pondrá en un grupo estático. Si seleccionó **Sincronizar con Active Directory** durante la Instalación del servidor, los equipos detectados se agregarán al grupo **Todos**. Para sincronizar equipos Linux unidos al dominio Windows, siga estas instrucciones detalladas.

ESET PROTECT On-Prem es compatible con firma de LDAP asegurada.

Hay 3 **Modos de sincronización**:

- Active Directory/Open Directory/LDAP: ingrese la información básica de conexión del servidor.

Puede ejecutar la tarea del servidor Instalación de agente para instalar el ESET Management agente a los equipos sincronizados desde Active Directory.

• Red de MS Windows: Ingrese un **Grupo de trabajo** para usar y las credenciales de usuario correspondientes.

Es posible que el modo de sincronización de **red de MS Windows** no funcione porque faltan requisitos (SMBv1) necesarios para su correcto funcionamiento. ESET quitará este modo de sincronización en el futuro.

• VMware: ingrese la información de conexión al servidor VMware vCenter.

Modo de sincronización - Active Directory/Open Directory/LDAP

Para crear una nueva tarea del servidor, haga clic en **Tareas** > **Nueva** > **Tarea de servidor** o seleccione el tipo de tarea deseada a la izquierda y haga clic en **Nueva** > **Tarea de servidor**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**.
Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

También puede seleccionar de la siguiente configuración del desencadenador de tareas:

• **Ejecutar tarea inmediatamente luego de finalizar**: seleccione esta opción para que la tarea se ejecute luego de hacer clic en Finalizar.

• **Configurar desencadenador**: seleccione esta opción para habilitar la sección Desencadenador, donde puede configurarlo.

Para configurar el desencadenador más adelante, deje las casillas de verificación sin marcar.

Configuración

Configuraciones comunes

Haga clic en **Seleccionar** en **Nombre de grupo estático**: por defecto, se utilizará el grupo hogar del usuario ejecutador para los equipos sincronizados. Alternativamente, puede crear un **Grupo estático nuevo**.

• **Objeto a sincronizar**: ya sean **Equipos y grupos** o **Solo equipos**.

• **Manejo de colisiones de creación de equipos**: si la sincronización agrega equipos que ya son miembros del Grupo estático, puede seleccionar un método de resolución de conflictos:

- **Omitir** (no se agregarán los equipos sincronizados)
- **Mover** (los equipos nuevos se moverán a un subgrupo)
- **Duplicar** (se crea un nuevo equipo con nombre diferente)

- **Manejo de extinciones de equipos**: si un equipo ya no existe, puede **Eliminar** u **Omitir** este equipo.
- **Manejo de extinciones de grupos**: si un grupo ya no existe, puede **Eliminar** u **Omitir** este grupo.

> Si establece el **Manejo de extinciones de grupos** en **Omitir** y elimina un grupo (Unidad organizativa) de Active Directory, los equipos que pertenecían al grupo en ESET PROTECT On-Prem no se eliminarán, ni siquiera si establece su **Manejo de extinciones de equipos** en **Quitar**.

- **Modo de sincronización** - **Active Directory/Open Directory/LDAP**

Lea nuestro artículo de la base de conocimiento sobre la administración de equipos con sincronización con Active Directory en ESET PROTECT On-Prem.

Configuración de conexión del servidor

- **Servidor** - Ingrese el nombre del servidor o la dirección IP de su controlador de dominio.
- **Iniciar sesión** - Ingrese el nombre de usuario para su controlador de dominio con el siguiente formato:
  - Servidor de `DOMAIN\username` (ESET PROTECT ejecutándose en Windows)
  - Servidor de `username@FULL.DOMAIN.NAME` o `username` (ESET PROTECT ejecutándose en Linux).

> Asegúrese de escribir el dominio en letras mayúsculas, ya que es el formato requerido para autenticar consultas correctamente en un servidor de Active Directory.

- **Contraseña**: ingrese la contraseña usada para ingresar al controlador de dominio.

El servidor de ESET PROTECT en Windows usa el protocolo de cifrado LDAPS (LDAP por sobre SSL) de manera predeterminada para todas las conexiones de Active Directory (AD). También puede configurar LDAPS en el aparato virtual de ESET PROTECT.
Para realizar correctamente una conexión de AD a través de LDAPS, configure lo siguiente:
1. El controlador de dominio debe tener instalado un certificado de la máquina. Para emitir un certificado para su controlador de dominio, siga los pasos indicados a continuación:
a)Abra el **Administrador de servidores** y haga clic en **Administrar** > **Agregar roles y características**, e instale **Servicios certificados de Active Directory** > **Autoridad de certificación**. Se creará una nueva autoridad de certificación en **Autoridades de certificación raíz de confianza**.
b)Diríjase a **Iniciar** >tipo `certmgr.msc` y presione **Aceptar** para ejecutar la extensión **Certificados** Consola de administración de Microsoft > **Certificados - Equipo local** > **Personal** > haga clic con el botón secundario en el panel vacío > **Todas las tareas** > **Solicitar un nuevo certificado** > rol **Inscribir controlador de dominio**.
c)Compruebe que el certificado emitido contenga la FQDN del controlador de dominio.
d)En su servidor ESET PROTECT, importe la CA que generó a la tienda de cert. (usando la herramienta `certmgr.msc`) a la carpeta CA de confianza.
2. Cuando proporcione la configuración de conexión al servidor de AD, escriba el FQDN del controlador de dominio (como se indica en el certificado del controlador de dominio) en el campo **Servidor** o **Host**. La dirección IP ya no es suficiente para LDAPS.

Para habilitar la reserva al protocolo LDAP, seleccione la casilla de verificación **Usar LDAP en lugar de Active Directory** e introduzca los atributos específicos que se ajusten con su servidor. De manera alternativa, puede seleccionar **Valores predeterminados** al hacer clic en **Seleccionar** y los atributos se completarán automáticamente:

- **Active Directory**
- **macOS Server Open Directory (Nombres de host del equipo)**
- **macOS Server Open Directory (Direcciones IP del equipo)**
- **OpenLDAP con registros del equipo Samba**: para configurar los parámetros del nombre DNS en Active Directory.

Cuando seleccione **Usar LDAP en lugar de Active Directory** y la preconfiguración de **Active Directory**, puede ingresar los atributos de su estructura de Active Directory para completar los detalles del equipo. Solo se pueden usar atributos del tipo `DirectoryString`. Puede usar una herramienta (por ejemplo, *ADExplorer*) para inspeccionar los atributos en su controlador de dominio. Seleccione los campos correspondientes en la siguiente tabla:

Campos de detalles del equipo	Campos de tarea de sincronización
Nombre	**Atributo de nombre de host del equipo**
Descripción	**Atributo de descripción del equipo**

Configuración de sincronización

- **Nombre distinguido**: ruta (nombre distinguido) al nodo en el árbol de Active Directory. Dejar esta opción vacía sincronizará el árbol del AD completo. Haga clic en **Navegar** junto a **Nombre distinguido**. Aparecerá el árbol de Active Directory. Seleccione la entrada superior para sincronizar todos los grupos con ESET PROTECT On-Prem o seleccione solo los grupos específicos que desea agregar. Solo se sincronizan los equipos y las unidades organizativas. Haga clic en **Aceptar** cuando haya finalizado.

Determinar el nombre distinguido

1.Abra la aplicación **Usuarios y equipos de Active Directory**.
2.Haga clic en **Ver** y seleccione **Características avanzadas**.
3.Haga clic con el botón derecho del ratón en el dominio > **Propiedades** >, seleccione la ficha **Editor de atributos**.
4.Ubique **distinguishedName** la línea. Debe tener el mismo aspecto que el de este ejemplo: `DC=ncop,DC=local`.

- **Nombres distinguidos excluidos**: puede optar por excluir (ignorar) nodos específicos en el árbol del Active Directory.

- **Ignorar equipos deshabilitados (solo en Active Directory)**: puede optar por ignorar los equipos deshabilitados en el Active Directory; la tarea omitirá estos equipos.

Si recibe un error: `Server not found in Kerberos database` luego de hacer click en **Navegar**, use AD FQDN del servidor en lugar de la dirección IP.

Sincronización desde el servidor de Linux

El servidor de ESET PROTECT que se ejecuta en Linux ejecuta la sincronización de forma diferente a las máquinas con Windows. El proceso es el siguiente:
1. Se deben completar las credenciales y el nombre de host del controlador de dominio.
2. El servidor verifica las credenciales y las convierte en un comprobante de Kerberos.
3. El servidor detecta el nombre distinguido del dominio si no está presente.
4. A) Si no está seleccionada la opción **Usar LDAP en lugar de Active Directory**:
Varias llamadas a `ldapsearch` enumeran el árbol. Un ejemplo simplificado para el proceso de obtención de registros del equipo:

```
kinit <username>
```

(Se trata de un comando dividido en dos líneas:)

```
ldapsearch -LLL -Y GSSAPI -h ad.domain.com -b 'DC=domain,DC=com' \
'(&(objectCategory=computer))' 'distinguishedName' 'dNSHostName'
```

B) Si está seleccionada la opción **Usar LDAP en lugar de Active Directory**:
Se convoca el mismo proceso como en la opción 4A, pero el usuario puede configurar los parámetros.
5. Kerberos usa un mecanismo de protocolo de enlace para autenticar el usuario y generar un comprobante que puede usarse posteriormente con otros servicios para obtener autorización sin enviar una contraseña en texto no cifrado (distinto de la opción **Usar autenticación simple**).
6. Luego, la utilidad `ldapsearch` usa GSSAPI para realizar la autenticación respecto de Active Directory con el comprobante de Kerberos obtenido.
7. Los resultados de búsqueda se devuelven a través de un canal no cifrado.

Desencadenador

La sección **Desencadenador** contiene información sobre los desencadenadores que ejecutarán una tarea. Cada **Tarea del servidor** puede tener hasta un desencadenador. Cada desencadenador solo puede ejecutar una **Tarea del servidor**. Si no se selecciona **Configurar desencadenador** en la sección **Básico**, no se crea un desencadenador. Se puede crear una tarea sin un desencadenador. Dicha tarea se puede ejecutar manualmente o se puede agregar un desencadenador en otro momento.

Configuración avanzada: Umbral

Al configurar un límite, puede establecer reglas avanzadas para el desencadenador creado. Establecer un límite es

opcional.

Resumen

Todas las opciones configuradas se visualizan aquí. Revise la configuración y haga clic **Finalizar**.

En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

> Puede ejecutar la tarea del servidor Instalación de agente para instalar el ESET Management agente a los equipos sincronizados desde Active Directory.

Modo de sincronización: red de MS Windows

> Es posible que el modo de sincronización de **red de MS Windows** no funcione porque faltan requisitos (SMBv1) necesarios para su correcto funcionamiento. ESET quitará este modo de sincronización en el futuro.

Para crear una nueva tarea del servidor, haga clic en **Tareas** > **Nueva** > **Tarea de servidor** o seleccione el tipo de tarea deseada a la izquierda y haga clic en **Nueva** > **Tarea de servidor**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**.
Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

También puede seleccionar de la siguiente configuración del desencadenador de tareas:

- **Ejecutar tarea inmediatamente luego de finalizar**: seleccione esta opción para que la tarea se ejecute luego de hacer clic en Finalizar.
- **Configurar desencadenador**: seleccione esta opción para habilitar la sección Desencadenador, donde puede configurarlo.

Para configurar el desencadenador más adelante, deje las casillas de verificación sin marcar.

Configuración

Configuraciones comunes

Haga clic en **Seleccionar** en **Nombre de grupo estático**: por defecto, se utilizará el grupo hogar del usuario ejecutador para los equipos sincronizados. Alternativamente, puede crear un **Grupo estático nuevo**.

- **Objeto a sincronizar**: ya sean **Equipos y grupos** o **Solo equipos**.
- **Manejo de colisiones de creación de equipos**: si la sincronización agrega equipos que ya son miembros

del Grupo estático, puede seleccionar un método de resolución de conflictos:

- **Omitir** (no se agregarán los equipos sincronizados)
- **Mover** (los equipos nuevos se moverán a un subgrupo)
- **Duplicar** (se crea un nuevo equipo con nombre diferente)

- **Manejo de extinciones de equipos**: si un equipo ya no existe, puede **Eliminar** u **Omitir** este equipo.
- **Manejo de extinciones de grupos**: si un grupo ya no existe, puede **Eliminar** u **Omitir** este grupo.
- **Modo de sincronización** - **Red de MS Windows**

En la sección Configuración de sincronización de red de Microsoft Windows escriba la siguiente información:

- **Grupo de trabajo**: escriba el dominio o grupo de trabajo que contiene los equipos que se sincronizarán. Si no especifica un grupo de trabajo, todos los equipos visibles se sincronizarán.
- **Inicio de sesión**: escriba las credenciales de inicio de sesión usadas para la sincronización en su red de Windows.
- **Contraseña**: escriba la contraseña usada para iniciar sesión su red de Windows.

El servidor de ESET PROTECT se ejecuta con privilegios de **servicio de red** que pueden no ser suficientes para leer todos los equipos cercanos. Si no hay credenciales de usuario, el servidor lee todos los equipos cercanos desde las carpetas de red disponibles en Windows que completa automáticamente el sistema operativo. Si hay credenciales, el servidor las usa para la sincronización directa.

Es posible que el modo de sincronización de **red de MS Windows** no funcione porque faltan requisitos (SMBv1) necesarios para su correcto funcionamiento. ESET quitará este modo de sincronización en el futuro.

Desencadenador

La sección **Desencadenador** contiene información sobre los desencadenadores que ejecutarán una tarea. Cada **Tarea del servidor** puede tener hasta un desencadenador. Cada desencadenador solo puede ejecutar una **Tarea del servidor**. Si no se selecciona **Configurar desencadenador** en la sección **Básico**, no se crea un desencadenador. Se puede crear una tarea sin un desencadenador. Dicha tarea se puede ejecutar manualmente o se puede agregar un desencadenador en otro momento.

Configuración avanzada: Umbral

Al configurar un límite, puede establecer reglas avanzadas para el desencadenador creado. Establecer un límite es opcional.

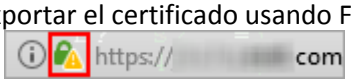
Resumen

Todas las opciones configuradas se visualizan aquí. Revise la configuración y haga clic **Finalizar**.

En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Modo de sincronización - VMware

Se puede sincronizar máquinas virtuales que se ejecutan en el servidor VMware vCenter.

> Para ejecutar esta tarea con éxito, necesita importar la AC de vCenter en su servidor ESET PROTECT. Puede exportarlo mediante su navegador web.
> Por ejemplo, para exportar el certificado usando Firefox, haga clic en el ícono de la conexión segura en la barra de direcciones 

y, luego, haga clic en **Mostrar detalles de conexión** > **Más información** > **Ver certificado** > **Detalles** > **Exportar** > **Guardar**.

Para crear una nueva tarea del servidor, haga clic en **Tareas** > **Nueva** > **Tarea de servidor** o seleccione el tipo de tarea deseada a la izquierda y haga clic en **Nueva** > **Tarea de servidor**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**.
Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

También puede seleccionar de la siguiente configuración del desencadenador de tareas:

- **Ejecutar tarea inmediatamente luego de finalizar**: seleccione esta opción para que la tarea se ejecute luego de hacer clic en Finalizar.
- **Configurar desencadenador**: seleccione esta opción para habilitar la sección Desencadenador, donde puede configurarlo.

Para configurar el desencadenador más adelante, deje las casillas de verificación sin marcar.

Configuración

Configuraciones comunes

Haga clic en **Seleccionar** en **Nombre de grupo estático**: por defecto, se utilizará el grupo hogar del usuario ejecutador para los equipos sincronizados. Alternativamente, puede crear un **Grupo estático nuevo**.

- **Objeto a sincronizar**: ya sean **Equipos y grupos** o **Solo equipos**.
- **Manejo de colisiones de creación de equipos**: si la sincronización agrega equipos que ya son miembros del Grupo estático, puede seleccionar un método de resolución de conflictos:
  - **Omitir** (no se agregarán los equipos sincronizados)
  - **Mover** (los equipos nuevos se moverán a un subgrupo)

- **Duplicar** (se crea un nuevo equipo con nombre diferente)

- **Manejo de extinciones de equipos**: si un equipo ya no existe, puede **Eliminar** u **Omitir** este equipo.

- **Manejo de extinciones de grupos**: si un grupo ya no existe, puede **Eliminar** u **Omitir** este grupo.

- **Modo de sincronización** - **VMWare**

Configuración de conexión del servidor

- **Servidor**: escriba el DNS o dirección de IP del servidor VMware vCenter. La dirección debe ser exactamente la misma que el valor **CN** de la AC de vCenter importada. Puede encontrar este valor en la columna **Asunto** de la ventana **Más** > **Autoridades de certificación**.

- **Inicio de sesión**: escriba las credenciales de inicio de sesión para el servidor VMware vCenter.

- **Contraseña**: ingrese la contraseña usada para ingresar a su servidor VMware vCenter.

Configuración de sincronización

- **Vista de la estructura**: seleccione el tipo de vista de estructura, **Carpetas** o **Reserva de recursos**.

- **Ruta de la estructura**: haga clic en **Examinar y navegue hacia la** carpeta que desea sincronizar. Si el campo se deja vacío, toda la estructura se sincronizará.

- **Vista del equipo**: seleccione si mostrar los equipos por **Nombre**, **Nombre del host** o **Dirección IP luego de la sincronización**.

Si recibe un error: `Server not found in Kerberos database` luego de hacer click en **Navegar**, use AD FQDN del servidor en lugar de la dirección IP.

Desencadenador

La sección **Desencadenador** contiene información sobre los desencadenadores que ejecutarán una tarea. Cada **Tarea del servidor** puede tener hasta un desencadenador. Cada desencadenador solo puede ejecutar una **Tarea del servidor**. Si no se selecciona **Configurar desencadenador** en la sección **Básico**, no se crea un desencadenador. Se puede crear una tarea sin un desencadenador. Dicha tarea se puede ejecutar manualmente o se puede agregar un desencadenador en otro momento.

Configuración avanzada: Umbral

Al configurar un límite, puede establecer reglas avanzadas para el desencadenador creado. Establecer un límite es opcional.

Resumen

Todas las opciones configuradas se visualizan aquí. Revise la configuración y haga clic **Finalizar**.

En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Sincronización de grupos estáticos: equipos Linux

Un equipo Linux unido a un dominio de Windows no muestra texto en Usuarios y Equipos de Active Directory (ADUC) de las propiedades del equipo, por lo tanto, debe insertarse el texto en forma manual.

Consulte los Requisitos previos del servidor y los siguientes requisitos previos:

- Los equipos Linux están en el Active Directory.
- El controlador de dominios tiene instalado un servidor DNS.
- ADSI Edit instalado.

1. Abra un símbolo del sistema y ejecute `adsiedit.msc`
2. Vaya a **Acción** > **Conectarse a**. Aparecerá la ventana Configuración de conexión.
3. Haga clic en **Seleccionar un contexto de nomenclatura conocido**.
4. Expanda el siguiente cuadro combinado y seleccione el contexto de nomenclatura **Predeterminado**.
5. Haga clic en **Aceptar**: el valor ADSI a la izquierda debe tener el nombre de su controlador de dominios. Contexto de nomenclatura predeterminado (su controlador de dominios).
6. Haga clic en el valor **ADSI** y expanda su subgrupo.
7. Haga clic en el **subgrupo** y vaya al CN (Nombre común) o a la OU (Unidad organizativa) donde se muestran los equipos Linux.
8. Haga clic en el **nombre de host** del equipo Linux y seleccione **Propiedades** en el menú contextual. Vaya al parámetro **dNSHostName** y haga clic en **Editar**.
9. Cambie el valor **no establecido** a un texto válido (por ejemplo, `ubuntu.TEST`).
10. Haga clic en **Aceptar** > **Aceptar**. Abra **ADUC** y seleccione las **propiedades** del equipo Linux (aquí debería mostrarse el texto nuevo).

Sincronización de usuario

Esta Tarea de servidor sincroniza la información de los usuarios y grupos de usuarios desde una fuente como Active Directory, parámetros LDAP, etc.

Para crear una nueva tarea del servidor, haga clic en **Tareas** > **Nueva** > **+Tarea de servidor** o seleccione el tipo de tarea deseada a la izquierda y haga clic en **Nueva** > **+Tarea de servidor**.

Básica

En la sección **Básico**, introduzca la información básica sobre la tarea, como **Nombre y Descripción (opcional)**.
Haga clic en **Seleccionar etiquetas** para asignar etiquetas.
En el menú desplegable **Tarea**, seleccione el tipo de tarea que desea crear y configurar. Si seleccionó un tipo de

tarea específico antes de crear una nueva tarea, se preselecciona **Tarea** en función de la elección anterior que haya hecho. **Tarea** (vea la lista de Todas las tareas) define las configuraciones y el comportamiento para la tarea.

También puede seleccionar de la siguiente configuración del desencadenador de tareas:

- **Ejecutar tarea inmediatamente luego de finalizar**: seleccione esta opción para que la tarea se ejecute luego de hacer clic en Finalizar.
- **Configurar desencadenador**: seleccione esta opción para habilitar la sección Desencadenador, donde puede configurarlo.

Para configurar el desencadenador más adelante, deje las casillas de verificación sin marcar.

Configuración

Configuraciones comunes

Nombre del grupo de usuarios: de forma predeterminada, se usará la raíz para usuarios sincronizados (por defecto, es el grupo **Todos**). Alternativamente, puede crear un nuevo grupo de usuarios.

Manejar la colisión en la creación de usuarios: se pueden generar dos tipos de conflictos:

- Hay dos usuarios con el mismo nombre en el mismo grupo.
- Hay un usuario con el mismo SID (en cualquier lugar del sistema).

Puede establecer el manejo de colisión en:

- **Omitir**: el usuario no se agrega a ESET PROTECT On-Prem durante la sincronización con Active Directory.
- **Sobrescribir**: se sobrescribe el usuario existente en ESET PROTECT On-Prem con el usuario de Active Directory; en caso de un conflicto SID, el usuario existente en ESET PROTECT On-Prem es eliminado de su ubicación anterior (incluso si el usuario se encontraba en un grupo diferente).

Manejo de extinción de usuario: si un usuario ya no existe, puede **Eliminarlo** o **Omitirlo.**

Manejo de extinción de grupo de usuarios: si un grupo de usuarios ya no existe, puede **Eliminarlo** o **Omitirlo**.

> Si usa atributos personalizados para un usuario, establezca el **Manejo de colisión de creación de usuarios** a **Omitir**. En caso contrario, el usuario (y sus detalles) se sobrescribirá con los datos de Active Directory y perderá los atributos personalizados. Si desea sobrescribir el usuario, cambie el **Manejo de extinciones de usuarios** a **Omitir**.

Configuración de conexión del servidor

- **Servidor** - Ingrese el nombre del servidor o la dirección IP de su controlador de dominio.
- **Iniciar sesión** - Ingrese el nombre de usuario para su controlador de dominio con el siguiente formato:
  - Servidor de `DOMAIN\username` (ESET PROTECT ejecutándose en Windows)
  - Servidor de `username@FULL.DOMAIN.NAME` o `username` (ESET PROTECT ejecutándose en Linux).

Asegúrese de escribir el dominio en letras mayúsculas, ya que es el formato requerido para autenticar consultas correctamente en un servidor de Active Directory.

- **Contraseña**: ingrese la contraseña usada para ingresar al controlador de dominio.

El servidor de ESET PROTECT en Windows usa el protocolo de cifrado LDAPS (LDAP por sobre SSL) de manera predeterminada para todas las conexiones de Active Directory (AD). También puede configurar LDAPS en el aparato virtual de ESET PROTECT.
Para realizar correctamente una conexión de AD a través de LDAPS, configure lo siguiente:
1. El controlador de dominio debe tener instalado un certificado de la máquina. Para emitir un certificado para su controlador de dominio, siga los pasos indicados a continuación:
a)Abra el **Administrador de servidores** y haga clic en **Administrar** > **Agregar roles y características**, e instale **Servicios certificados de Active Directory** > **Autoridad de certificación**. Se creará una nueva autoridad de certificación en **Autoridades de certificación raíz de confianza**.
b)Diríjase a **Iniciar** >tipo `certmgr.msc` y presione **Aceptar** para ejecutar la extensión **Certificados** Consola de administración de Microsoft > **Certificados - Equipo local** > **Personal** > haga clic con el botón secundario en el panel vacío > **Todas las tareas** > **Solicitar un nuevo certificado** > rol **Inscribir controlador de dominio**.
c)Compruebe que el certificado emitido contenga la FQDN del controlador de dominio.
d)En su servidor ESET PROTECT, importe la CA que generó a la tienda de cert. (usando la herramienta `certmgr.msc`) a la carpeta CA de confianza.
2. Cuando proporcione la configuración de conexión al servidor de AD, escriba el FQDN del controlador de dominio (como se indica en el certificado del controlador de dominio) en el campo **Servidor** o **Host**. La dirección IP ya no es suficiente para LDAPS.

Para habilitar la reserva al protocolo LDAP, seleccione la casilla de verificación **Usar LDAP en lugar de Active Directory** e introduzca los atributos específicos que se ajusten con su servidor. De manera alternativa, puede seleccionar **Valores predeterminados** al hacer clic en **Seleccionar** y los atributos se completarán automáticamente:

- **Active Directory**
- **macOS Server Open Directory (Nombres de host del equipo)**
- **OpenLDAP con registros del equipo Samba:** configura los parámetros del nombre DNS en Active Directory.

Configuración de sincronización

- **Nombre distinguido**: ruta (nombre distinguido) al nodo en el árbol de Active Directory. Dejar esta opción vacía sincronizará el árbol del AD completo. Haga clic en **Navegar** junto a **Nombre distinguido**. Aparecerá el árbol de Active Directory. Seleccione la entrada superior para sincronizar todos los grupos con ESET PROTECT On-Prem o seleccione solo los grupos específicos que desea agregar. Solo se sincronizan los equipos y las unidades organizativas. Haga clic en **Aceptar** cuando haya finalizado.

Determinar el nombre distinguido

1.Abra la aplicación **Usuarios y equipos de Active Directory**.
2.Haga clic en **Ver** y seleccione **Características avanzadas**.
3.Haga clic con el botón derecho del ratón en el dominio > **Propiedades** >, seleccione la ficha **Editor de atributos**.
4.Ubique **distinguishedName** la línea. Debe tener el mismo aspecto que el de este ejemplo: `DC=ncop,DC=local`.

- **Grupo de usuarios y atributos de usuarios**: los atributos predeterminados de un usuario son específicos al directorio al que pertenece el usuario. Si desea sincronizar los atributos de Active Directory, seleccione el parámetro AD del menú plegable en los campos adecuados o ingrese un nombre personalizado para el atributo. Junto a cada campo sincronizado se encuentra un marcador de ESET PROTECT On-Prem (por ejemplo: `${display_name}`) que representa a este atributo en ciertas configuraciones de la política de ESET PROTECT On-Prem.

- **Atributos de usuarios avanzados**: si desea usar atributos personalizados avanzados, seleccione **Agregar nuevo**. Estos campos heredarán la información del usuario, que se puede abordar en un editor de política para MDM de iOS como marcador.

Si recibe un error: `Server not found in Kerberos database` luego de hacer click en **Navegar**, use AD FQDN del servidor en lugar de la dirección IP.

Desencadenador

La sección **Desencadenador** contiene información sobre los desencadenadores que ejecutarán una tarea. Cada **Tarea del servidor** puede tener hasta un desencadenador. Cada desencadenador solo puede ejecutar una **Tarea del servidor**. Si no se selecciona **Configurar desencadenador** en la sección **Básico**, no se crea un desencadenador. Se puede crear una tarea sin un desencadenador. Dicha tarea se puede ejecutar manualmente o se puede agregar un desencadenador en otro momento.

Configuración avanzada: Umbral

Al configurar un límite, puede establecer reglas avanzadas para el desencadenador creado. Establecer un límite es opcional.

Resumen

Todas las opciones configuradas se visualizan aquí. Revise la configuración y haga clic **Finalizar**.

En **Tareas**, puede ver la barra indicadora de progreso, el ícono de estado y los detalles de cada una de las tareas creadas.

Tipos de desencadenadores de tareas

Los desencadenantes son básicamente sensores que reaccionan a ciertos eventos de una manera predefinida. Se utilizan para ejecutar la tarea a la que se los asigna. Pueden activarse a través de las Tareas programadas (eventos de tiempo) o cuando se produce cierto evento del sistema.

No puede reutilizar un desencadenador. Cada tarea debe desencadenarse con un desencadenador diferente. Cada desencadenador solo puede ejecutar una tarea.

El desencadenador no ejecuta de forma inmediata las tareas nuevas que se le asignan (a excepto del desencadenador ASAP); la tarea se ejecuta en cuanto el desencadenador se dispara. La sensibilidad del desencadenador puede disminuirse configurando el límite.

Tipos de desencadenadores

• **Lo antes posible**: disponible solo para tareas de clientes. La tarea se ejecutará en cuanto haga clic en **Finalizar**. El valor de **Fecha de vencimiento** especifica la fecha a partir de la cual ya no se ejecutará la tarea.

Programado

El desencadenador programado ejecutará la tarea en función de la configuración de fecha y hora. Las tareas pueden programarse para que **se ejecuten una vez**, en base repetitiva o en expresión CRON.

• **Programado una vez**: este desencadenador se invoca una vez en la fecha y la hora programada. Se puede retrasar por un intervalo aleatorio.

• **A diario**: este disparador se invoca cada día seleccionado. Puede establecer el inicio y el final del intervalo. Por ejemplo, puede ejecutar una tarea durante diez fines de semana consecutivos.

• **Semanalmente**: el desencadenador se invoca un día de la semana seleccionado. Por ejemplo, ejecute una tarea todos los lunes y viernes entre el 1 de julio y el 31 de agosto.

• **Mensualmente**: este desencadenador se invoca días específicos en la semana específica de un mes, durante el período de tiempo establecido. El valor **Repetir en** establece el día de la semana en el mes (por ejemplo, el segundo lunes) cuando se debe ejecutar la tarea.

• **Anualmente**: el desencadenador se invoca cada año en la fecha de **inicio** especificada.

La configuración **Intervalo de retraso aleatorio** se encuentra disponible para desencadenadores de tipo Programados. Define el rango de retraso máximo para la ejecución de la tarea. La aleatorización puede evitar la sobrecarga del servidor.

Si *John* configura la **Tarea** para que se desencadene **Semanalmente** el *lunes* e **Inicie** el *10 de febrero de 2017 a las 8:00:00*, con el **Intervalo de retraso aleatorio** configurado en *1 hora*, y la **finalización configurada para el** *6 de abril de 2017 a las 00:00:00,* la tarea se ejecutará con un retraso aleatorio de una hora entre las 8:00 y las 9:00 cada lunes hasta la fecha de finalización especificada.

• Seleccione la casilla de verificación **Invocar lo antes posible si se perdió el evento** para ejecutar la tarea inmediatamente si no se ejecutó en el tiempo definido
• Al configurar un desencadenador, la zona horaria de la Consola web de ESET PROTECT se usa de forma predeterminada. De forma alternativa, puede seleccionar la casilla de verificación **Usar la hora local de destino** para usar la zona horaria local del dispositivo de destino, en lugar de la zona horaria de la consola web de ESET PROTECT para el desencadenador.

Grupo dinámico

Los desencadenadores de grupo dinámico se encuentran disponibles solo para tareas del servidor:

• **Cambio en los miembro del** grupo dinámico: este desencadenador se invoca cuando cambia el contenido de un grupo dinámico. Por ejemplo, si un cliente se une o abandona un grupo dinámico específico.

• **Cambio del tamaño del grupo dinámico según el umbral límite**: este desencadenador se invoca cuando el número de clientes en un grupo dinámico es mayor o menor que el umbral especificado. Por ejemplo, si más de 100 equipos están en un grupo específico.

• **Cambio de tamaño del grupo dinámico durante un período de tiempo** - Este desencadenador se invoca cuando el número de clientes en un grupo dinámico cambia a lo largo de un período de tiempo definido. Por ejemplo, si el número de equipos en cierto grupo aumenta en un 10 % en una hora.

• **Cambio del tamaño de un grupo dinámico en comparación con otro** - Este desencadenador se invoca cuando el número de clientes en un grupo dinámico observado cambia con respecto a otro grupo con el que se lo compara (estático o dinámico). Por ejemplo, si más del 10 % de todos los equipos están infectados (el grupo **Todos** en comparación con el grupo **Infectado**).

Otro

• **Se inició el servidor**: disponible únicamente para tareas del servidor. Evocado cuando se inicia el servidor. Por ejemplo, este desencadenador se usa para la tarea de sincronización de grupos estáticos.

• **Desencadenador de grupo dinámico unido**: disponible únicamente para tareas del cliente. Se invoca cada vez que un dispositivo se une a un grupo dinámico.

> El **desencadenador de grupo dinámico unido** se encuentra disponible solo si un grupo dinámico se selecciona en la sección Objeto. El desencadenador ejecutará la tarea solo en los dispositivos que se unan al grupo dinámico luego de haberse creado el desencadenador. Para todos los dispositivos que ya están en el grupo dinámico deberá ejecutar la tarea manualmente.

• **Desencadenador de registro de evento:** este desencadenador se invoca cuando ocurre un evento determinado en los registros. Por ejemplo, si hay una detección en el registro de **análisis**. Este tipo de desencadenante brinda un conjunto de ajustes especiales en la configuración de límite.

• **Expresión CRON**: este desencadenador se invoca en cierta fecha y hora.

Intervalo de expresión cron

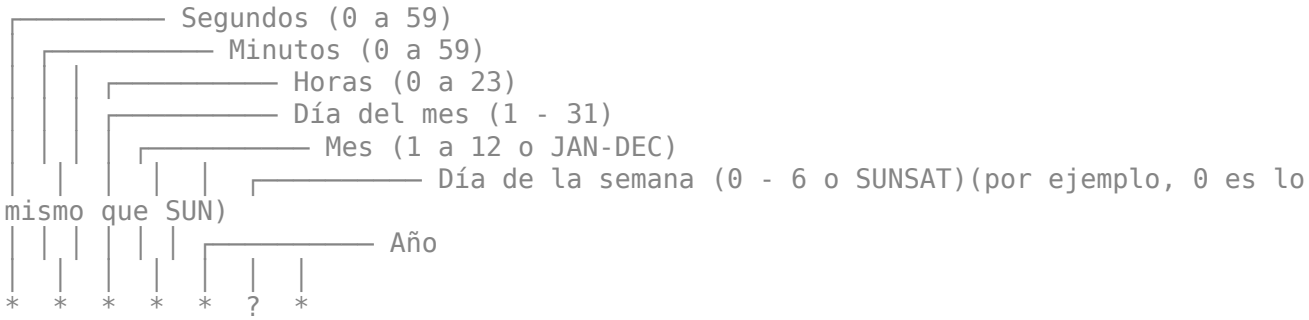
Se usa una expresión CRON para configurar casos específicos de un desencadenador. Generalmente para desencadenadores repetitivos programados. Es una cadena que consiste en 6 o 7 campos que representan valores individuales de las tareas programadas. Estos campos están separados por un espacio y contienen cualquiera de los valores permitidos con distintas combinaciones.

La expresión CRON puede ser tan simple como: `* * * * ? *` o mas compleja como: `0/5 14,18,3-39,52 * ? JAN,MAR,SEP MON-FRI 2012-2020`

Lista de valores que puede usar en la expresión CRON:

Nombre	Requerido	Valor	Caracteres especiales permitidos
Segundos	Sí	0-59	`, - * / R`
Minutos	Sí	0-59	`, - * / R`
Horas	Sí	0-23	`, - * / R`
Día del mes	Sí	1-31	`, - * / ? L W`
Mes	Aceptar	1-12 o JAN-DEC	`, - */`
Día de la semana	Aceptar	0-6 o SUN-SAT	`, - / ? L #`
Año	Aceptar	1970-2099	`, - * /`

La sintaxis de la expresión CRON es la siguiente:



- Los 0 0 0 significan medianoche (segundos, minutos, horas).
- Use ? cuando no se puede definir una valor porque está definido en otro campo (día del mes o día de la semana).
- El * significa todo (segundos, minutos, horas, día del mes, mes, día de la semana, año).
- El SUN significa el domingo.

> **i** Los nombres de los meses y los días de la semana no distinguen entre mayúsculas y minúsculas. Por ejemplo, MON es igual a mon o JAN es igual a jan.

Caracteres especiales:

Coma (,)

Las comas se usan para separar los elementos de una lista. Por ejemplo, el uso de "MON,WED,FRI" en el 6to campo (día de la semana) significa lunes, miércoles y viernes.

Guion (-)

Define los rangos. Por ejemplo, 2012-2020 indica cada año entre 2012 y 2020 inclusive.

Carácter comodín (*)

Se usa para seleccionar todos los valores posibles dentro de un campo. Por ejemplo, el * en el campo minutos significa cada minuto. El carácter comodín no se puede usar en el campo de día de la semana.

Signo de interrogación (?)

Cuando se elige un día específico, puede especificar un día del mes o un día de la semana. No puede especificar ambos. Si especifica un día del mes, debe usar ? para el día de la semana y viceversa. Por ejemplo, si desea que el desencadenador se accione un día del mes en particular (digamos, el 10) pero no le importa qué día de la semana sea, escriba 10 en el campo del día del mes y ? en el campo del día de la semana.

Hash (#)

Se usa para especificar el día "N" del mes. Por ejemplo, el valor de 4#3 en el campo del día de la semana significa el tercer jueves del mes (día 4 = jueves y #3 = el tercer jueves en el mes). Si especifica #5 y no existe el 5to del día de la semana dada en el mes, entonces el desencadenador no se accionará ese mes.

Barra diagonal (/)

Describe los incrementos de un rango. Por ejemplo, 3-59/15 en el 2do campo (minutos) indica el tercer minuto de la hora y cada 15 minutos a partir de ahí.

Último (L)

Cuando se usa en el campo del día de la semana, le permite especificar construcciones como el último viernes (5L) de un mes dado. En el campo del día del mes, especifica el último día del mes. Por ejemplo, día 31 para enero, día 28 para febrero en años no bisiestos.

Día de la semana (W)

Se admite el carácter W para el campo del día del mes. Este carácter se usa para especificar el día de la semana (lunes-viernes) más cercano al día dado. Como ejemplo, si especifica 15W como el valor para el campo del día del mes, el significado es el día de la semana más cercano al 15 del mes. Entonces, si el 15 es sábado, el desencadenador se accionará el viernes 14. Si el 15 es domingo, el desencadenador se accionará el lunes 16. Sin embargo, si especifica 1W como el valor para el día del mes, y el 1 es sábado, el desencadenador se accionará el lunes 3, ya que no salta por encima del límite de los días del mes.

Los caracteres L y W también se pueden combinar en el campo del día del mes que resulta en LW, que se traduce como el último día de entre semana del mes.

Aleatorio (R)

El R es un carácter de la expresión ESET PROTECT On-Prem CRON que le permite especificar momentos de tiempos aleatorios. Por ejemplo, el desencadenador R 0 0 * * ? * se acciona todos los días a las 00:00 pero en un segundo aleatorio (0-59).

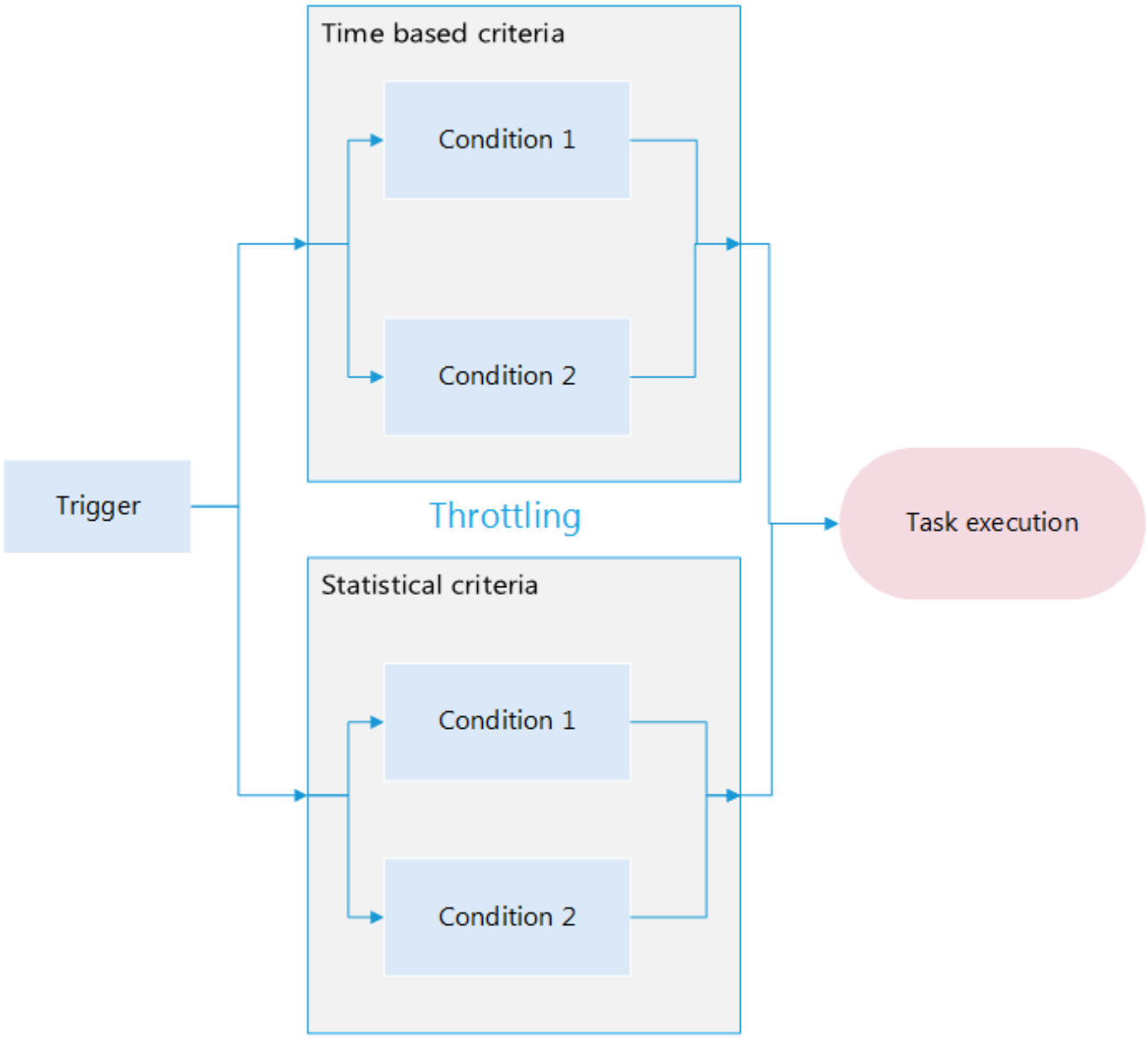
Recomendamos que use los momentos de tiempo aleatorios para evitar que todos los agentes ESET Management se conecten al mismo tiempo al servidor de ESET PROTECT.

Ejemplos reales que ilustran algunas variaciones de la expresión CRON:

Expresión CRON	Significado
`0 0 12 * * ? *`	Accionar a las 12:00 p.m. (mediodía) todos los días.
`R 0 0 * * ? *`	Se acciona a las 00:00 pero en un segundo aleatorio (0-59) todos los días.
`R R R 15W * ? *`	Se acciona el 15 de cada mes en tiempo aleatorio (segundos, minutos, horas). Si el 15 es sábado, el desencadenador se accionará el viernes 14. Si el 15 es domingo, el desencadenador se accionará el lunes 16.
`0 15 10 * * ? 2016`	Accionar a las 10:15 a.m. todos los días durante el año 2016.
`0 * 14 * * ? *`	Accionar a cada minuto a partir de las 2 p.m. y hasta las 2:59 p.m., todos los días.
`0 0/5 14 * * ? *`	Accionar cada 5 minutos a partir de las 2 p.m. y hasta las 2:55 p.m., todos los días.
`0 0/5 14,18 * * ? *`	Accionar cada 5 minutos a partir de las 2 p.m. y hasta las 2:55 p.m., y accionar cada 5 minutos a partir de las 6 p.m. y hasta las 6:55 p.m., todos los días.
`0 0-5 14 * * ? *`	Accionar a cada minuto a partir de las 2 p.m. y hasta las 2:05 p.m., todos los días.
`0 10,44 14 ? 3 WED *`	Accionar a las 2:10 p.m. y a las 2:44 p.m. todos los miércoles de marzo.
`0 15 10 ? * MON-FRI *`	Accionar a las 10:15 a.m. cada día de la semana (lunes, martes, miércoles, jueves y viernes).
`0 15 10 15 * ? *`	Accionar a las 10:15 a.m. el día 15 de cada mes.
`0 15 10 ? * 5L *`	Accionar a las 10:15 a.m. el último viernes de cada mes.
`0 15 10 ? * 5L 2016-2020`	Accionar a las 10:15 a.m. el último viernes de cada mes desde el año 2016 al año 2020, inclusive.
`0 15 10 ? * 5#3 *`	Accionar a las 10:15 a.m. el tercer viernes de cada mes.
`0 0 * * * ? *`	Fuego cada hora, todos los días.

Configuración avanzada: Umbral

El límite se utiliza para restringir la ejecución de una tarea. Normalmente, se utilizan límites cuando una tarea se desencadena por un evento frecuente. En ciertos casos, el límite puede evitar que se accione un desencadenador. Cada vez que se desencadena el desencadenador, se evalúa según el siguiente esquema. Solo aquellos desencadenantes que cumplen con las condiciones especificadas harán que se ejecute la tarea. Si no se establecen condiciones límites, todos los eventos desencadenantes ejecutarán la tarea.



Existen tres tipos de condiciones para los límites:

- **Criterios basados en el tiempo**
- **Criterios estadísticos**
- **Criterios de registro de eventos**

Para que se ejecute una tarea:

- Deben ocurrir todos los tipos de condiciones
- Las condiciones se deben configurar; si una condición está vacía, se omite
- Se deben pasar todas las condiciones basadas en el tiempo, ya que son evaluadas con el operador AND
- Todas las condiciones estadísticas evaluadas con el operador Y deben pasar; al menos una condición estadística con el operador O debe pasar
- Las condiciones estadísticas y temporadas configuradas juntas deben pasar, ya que se las evalúa con el

operador AND; solo en ese caso se ejecuta la tarea

Si se cumple alguna de las condiciones definidas, se restablece la información apilada para todos los observadores (la cuenta inicia desde 0). Esto funciona para las condiciones basadas en tiempo así como para las condiciones estadísticas. Esta información también se restablece si se reinicia el agente o el servidorESET PROTECT. Toda modificación hecha sobre un desencadenador reinicia su estado. Recomendamos que use una sola condición estadística y múltiples condiciones basadas en el tiempo. Tener múltiples condiciones estadísticas puede causar una complicación innecesaria y puede alterar los resultados del desencadenador.

Preconfiguración

Hay tres preconfiguraciones disponibles. Cuando selecciona una preconfiguración, su configuración actual del límite se borra y reemplaza por valores preconfigurados. Se pueden modificar y usar estos valores, aunque no es posible crear una nueva preconfiguración.

Criterios basados en el tiempo

Período de tiempo (T2): permite desencadenaciones durante el período de tiempo especificado. Si, por ejemplo, esto se configura en diez segundos y durante este período se generan diez invocaciones, solo la primera desencadenaría el evento.

Debe configurar la limitación con criterios basados en el tiempo para restringir la ejecución de la tarea a, como máximo, una vez cada 1 minuto (un ícono de candado indica la restricción):
- Tareas del servidor (incluida la generación de informes): todos los tipos de desencadenadores.
- Tareas del cliente: tipos de desencadenadores de **expresión CRON** y **programados**.

Si ha actualizado ESET PROTECT On-Prem desde la versión 8.x o 9.x, se aplicará 1 minuto automáticamente a todas las tareas existentes con el periodo de tiempo definido en menos de 1 minuto.
El periodo de tiempo mínimo de 15 minutos no se aplica a las notificaciones.

Cronograma (T1): permiten marcas solo dentro del período de tiempo definido. Haga clic en **Agregar período** y se mostrará la ventana emergente. Configure un **Rango de duración** en unidades de tiempo seleccionadas. Seleccione una opción de la lista de **Recurrencia** y complete los campos, que cambian según la recurrencia seleccionada. Además, puede definir la recurrencia en una forma de Expresión CRON. Haga clic en **Aceptar** para almacenar el rango. Puede agregar múltiples rangos de tiempo a la lista; se ordenarán cronológicamente.

Deben cumplirse todas las condiciones configuradas para que se desencadene la tarea.

Criterios estadísticos

Condición: las condiciones estadísticas se pueden combinar con:

- **Enviar notificación cuando se cumplan todos los criterios estadísticos** - **O** se use el operador lógico para evaluación
- **Enviar notificación cuando se cumple al menos un criterio estadístico** - **O** se use el operador lógico para evaluación

Cantidad de ocurrencias (S1): permite accionar solo cada marca X. Por ejemplo, si ingresa diez, solo se contará cada diez desencadenadores.

Cantidad de ocurrencias dentro de un período de tiempo

Cantidad de ocurrencias (S2): permite desencadenar solo dentro del período de tiempo definido. Esto definirá la frecuencia mínima de eventos para desencadenar la tarea. Por ejemplo, puede usar esta configuración para permitir la ejecución de la tarea si el evento se detecta 10 veces en una hora. Ejecutar el desencadenador hace que se reinicie el conteo.

Período de tiempo: define el período de tiempo para la opción descrita anteriormente.

Se encuentra disponible una tercera condición estadística para ciertos tipos de desencadenador. Consulte **Desencadenador** > **Tipo de desencadenador** > **Desencadenador de registro de evento**.

Criterios de registro de eventos

ESET PROTECT On-Prem evalúa estos criterios como criterios estadísticos terceros (S3). El operador de **aplicación de criterios estadísticos** (Y/O) se aplica para evaluar las tres condiciones estadísticas juntas. Recomendamos que use los criterios de registro de eventos junto a la tarea de **Generar informe**. Se necesitan los tres campos para que funcione el criterio. Se restablece el búfer de símbolos si se acciona el desencadenador y ya hay un símbolo en el búfer.

Condición: esto define qué eventos o conjunto de eventos desencadenarán la condición. Las opciones disponibles son:

- **Recibidos seguidos**: la cantidad especificada de eventos que deben ocurrir seguidos. Estos eventos deben ser únicos.
- **Recibidos desde la última ejecución del desencadenador**: la condición se desencadena cuando se alcanza la cantidad seleccionada de eventos únicos desde la última vez que se desencadenó la tarea.

Cantidad de ocurrencias: ingresar la cantidad de eventos únicos con los símbolos seleccionados para ejecutar la tarea.

Símbolo: en función del **tipo de registro**, que se configura en el menú **Desencadenador**, puede seleccionar el símbolo a buscar en el registro. Haga clic en **Seleccionar** para mostrar el menú. Puede eliminar el símbolo seleccionado haciendo clic en **Eliminar**.

> Cuando se utiliza con una tarea del servidor, se consideran todos los equipos. No es probable recibir una gran cantidad de símbolos distintivos en una fila. Use la configuración **Recibidos seguidos** solo para casos razonables. Un valor perdido (n/d) se considera como “no único” y por eso se restablece el búfer en este punto.

Propiedades adicionales

Como ya se indicó, no todos los eventos causarán que se accione el desencadenador. Las acciones a tomar para los eventos sin desencadenador pueden ser:

- Si se omite más de un evento, junte los últimos **N** eventos en uno (almacene datos de marcas suprimidas) [**N** <= 100]

- para **N** == 0, solo se procesa el último evento (**N** significa duración del historial, el último evento siempre se procesa)

- Se agrupan todos los eventos sin desencadenador (uniendo la última marca con **N** marcas de historial)

Si el desencadenador se activa muy seguido o si desea recibir menos notificaciones, tenga en cuenta las siguientes sugerencias:

- Si el usuario desea reaccionar solo en caso de que haya más sucesos (no uno solo), consulte la condición estadística S1

- Si el desencadenador se acciona solo cuando ocurre un clúster de eventos, siga la condición estadística S2

- Cuando deban ignorarse sucesos con valores no deseados, consulte la condición estadística S3

- Cuando se estén por ignorar aquellos sucesos fuera del horario relevante (por ejemplo, en horario laborable), consulte la condición temporal T1

- Para configurar el tiempo mínimo entre desencadenamientos, utilice la condición basada en tiempo T2

> Las condiciones también pueden combinarse para formar escenarios de límite más complejos. Consulte la sección ejemplos de límites para obtener más detalles.

Ejemplos de límite

Los ejemplos de límites explican cómo se combinan y evalúan las condiciones de límites (T1, T2, S1, S2, S3).

> "Marca" significa impulso desde el desencadenador. "T" representa los criterios basados en el tiempo, "S" representa los criterios estadísticos. "S3" representa los criterios de registro de eventos.

S1: Criterio para las ocurrencias (permitido cada 3 marcas)

Tiempo	00	01	02	03	04	05	06	Se modifica el desencadenador	07	08	09	10	11	12	13	14	15
Marcas	x	x	x	x	x	x	x		x	x		x	x		x		x
S1			1			1						1					1

S2: Criterio de ocurrencias dentro del tiempo (permitido si hay 3 marcas dentro de 4 segundos)

Tiempo	00	01	02	03	04	05	06	Se modifica el desencadenador	07	08	09	10	11	12	13
Marcas	x		x	x	x	x			x		x		x	x	x
S2				1										1	

S3: Criterio para los valores de símbolo único (se permite si hay 3 valores únicos seguidos)

Tiempo	00	01	02	03	04	05	06	Se modifica el desencadenador	07	08	09	10	11	12	13
Valor	A	B	B	C	D	G	H		J	K	n/d	L	M	N	N

Tiempo	00	01	02	03	04	05	06	Se modifica el desencadenador	07	08	09	10	11	12	13
S3					1									1	

S3: Criterio para los valores de símbolo único (se permite si hay 3 valores únicos desde la última marca)

Tiempo	00	01	02	03	04	05	06	07	Se modifica el desencadenador	08	09	10	11	12	13	14
Valor	A	B	B	C	D	G	H	I		J	K	n/d	L	M	N	N
S3				1			1						1			

T1: Permita una marca en ciertos rangos de tiempo (se permite todos los días a las 8:10, duración 60 segundos)

Tiempo	8:09:50	8:09:59	8:10:00	8:10:01	Se modifica el desencadenador	8:10:59	8:11:00	8:11:01
Marcas	x	x	x	x		x	x	x
T1			1	1		1		

El criterio no tiene estado, por lo que más modificaciones en el desencadenador no tienen efecto sobre los resultados.

T2: Permita una sola marca en un intervalo de tiempo (se permite como mucho cada 5 segundos)

Tiempo	00	01	02	03	04	05	06	Se modifica el desencadenador	07	08	09	10	11	12	13
Marcas	x		x	x	x	x			x		x		x	x	x
T2	1					1			1					1	

Combinación S1+S2

- S1: cada 5 marcas
- S2: tres marcas en cuatro segundos

Tiempo	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
Marcas	x	x	x	x	x		x	x	x			x		x	x		
S1															1		
S2			1				1								1		
Resultado			1				1								1		

El resultado aparece como: S1 (lógico o) S2

Combinación S1+T1

- S1: Se permite cada 3 marcas
- T1: Se permite todos los días desde las 8:08, duración 60 segundos

Tiempo	8:07:50	8:07:51	8:07:52	8:07:53	8:08:10	8:08:11	8:08:19	8:08:54	8:08:55	8:09:01
Marcas	x	x	x	x	x	x	x	x	x	x
S1			1			1			1	

Tiempo	8:07:50	8:07:51	8:07:52	8:07:53	8:08:10	8:08:11	8:08:19	8:08:54	8:08:55	8:09:01
T1					1	1	1	1	1	
Resultado						1			1	

El resultado aparece como: S1 (lógico y) T1

Combinación S2+T1

- S2: tres marcas en diez segundos
- T1: Se permite todos los días desde las 8:08, duración 60 segundos

Tiempo	8:07:50	8:07:51	8:07:52	8:07:53	8:08:10	8:08:11	8:08:19	8:08:54	8:08:55	8:09:01
Marcas	x	x	x	x	x	x	x	x	x	x
S2			1	1			1			1
T1					1	1	1	1	1	
Resultado							1			

El resultado aparece como: S2 (lógico y) T1.

Observe que el estado de S2 solo se restablece cuando el resultado general es 1.

Combinación S2+T2

- S2: tres marcas en diez segundos
- T2: Se permite una vez como mucho cada 20 segundos

Tiempo	00	01	02	03	04	05	06	07	...	16	17	18	19	20	21	22	23	24
Marcas	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x
S2			1			1	1	1				1	1	1	1	1		
T2	1	1	1													1		
Resultado			1													1		

El resultado aparece como: S2 (lógico y) T2.

Observe que el estado de S2 solo se restablece cuando el resultado general es 1.

Instaladores

En esta sección, se muestra cómo crear paquetes de instaladores del agente para implementar el agente ESET Management en equipos cliente. Los paquetes de instalación se guardan en la consola web de ESET PROTECT, y puede editarlos y descargarlos de nuevo cuando sea necesario.

Haga clic en **Instaladores** > **Crear instalador** y seleccione el sistema operativo.

Windows

- El paquete Descargar el instalador o utilizar Remote Deployment Tool de ESET Instalador de agente y producto de seguridad ESET permite opciones de configuración avanzada, como configuración de políticas para

el agente de ESET Management y productos ESET, nombre de host y puerto del servidor de ESET PROTECT, y la capacidad para seleccionar un grupo principal. Puede implementar el instalador de forma local o remota (con ESET Remote Deployment Tool).

- Implementar agente primero (instalador de scripts del agente) –Este tipo de implementación del Agente es útil cuando las opciones de implementación local y remota no son adecuadas para usted. Puede distribuir el instalador del script del agente por correo electrónico y dejar que el usuario lo instale. También puede ejecutar el instalador del script del agente desde un medio extraíble (una unidad de memoria USB, por ejemplo).

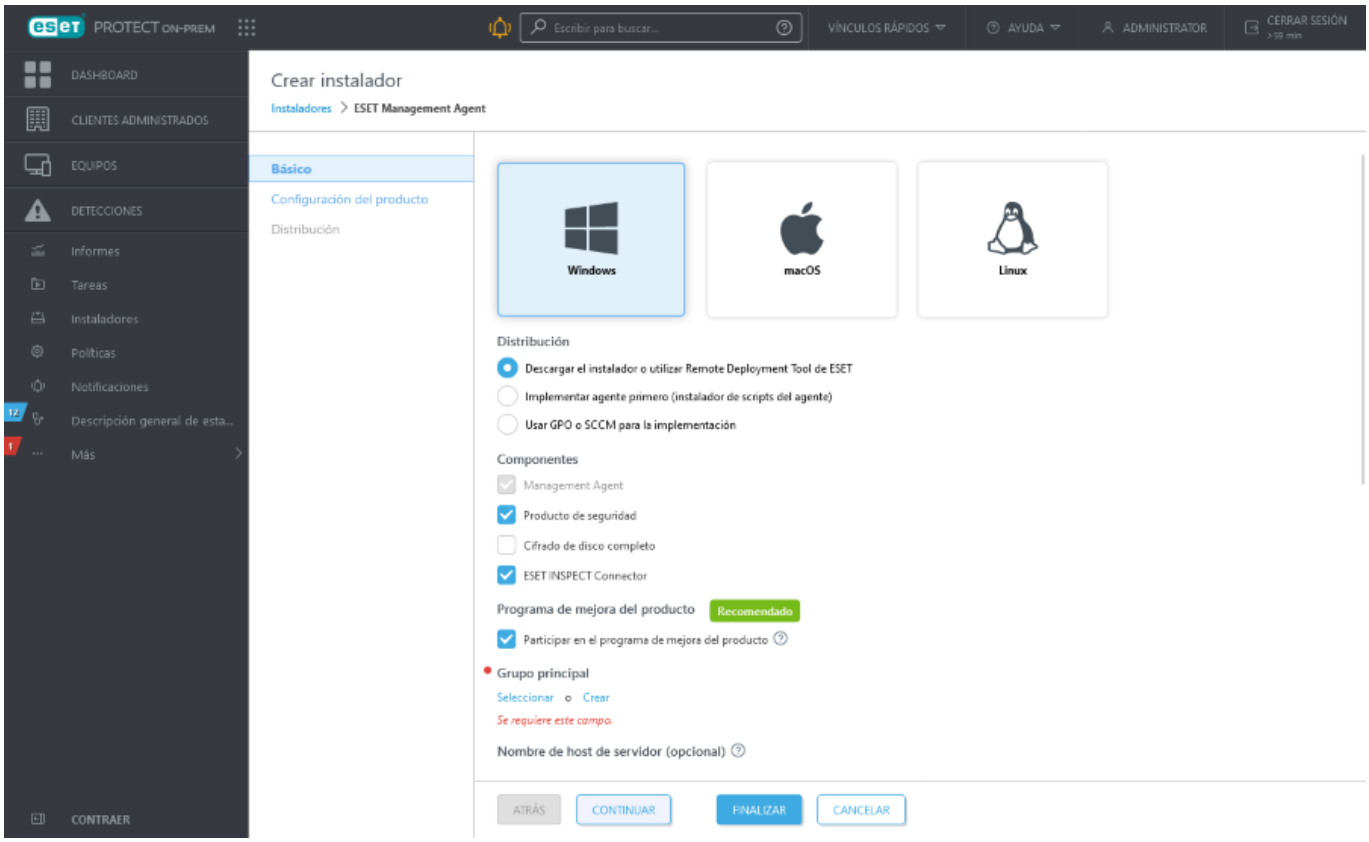
- Usar GPO o SCCM para la implementación –Utilice esta opción para la instalación masiva del agente ESET Management en equipos del cliente.

macOS

- El paquete Descargar o enviar el instalador Instalador de agente y producto de seguridad ESET permite opciones de configuración avanzada, como configuración de políticas para el agente de ESET Management y productos ESET, nombre de host y puerto del servidor de , y la capacidad para seleccionar un grupo principal.

Linux

- Implementar agente primero (instalador de scripts del agente) –Este tipo de implementación del Agente es útil cuando las opciones de implementación local y remota no son adecuadas para usted. Puede distribuir el instalador del script del agente por correo electrónico y dejar que el usuario lo instale. También puede ejecutar el instalador del script del agente desde un medio extraíble (una unidad de memoria USB, por ejemplo).



Instaladores y permisos

Un usuario puede crear o editar instaladores ubicados en los grupos donde el usuario cuenta con permisos de

Escritura para los **Grupos y equipos** e **Instaladores almacenados**.

Para descargar instaladores ya creados, el usuario debe tener permiso de **Uso** para **Grupos y equipos** e **Instaladores almacenados.**

- Asigne el permiso **Usar** a un usuario para las **Políticas** seleccionadas en **Avanzado** > **Configuración del instalador inicial** > **Tipo de configuración** al crear un instalador todo en uno, un instalador GPO o un script SCCM.
- Asigne el permiso **Usar** a un usuario para **Licencias** si se ha especificado la licencia para el grupo estático.
- La selección del grupo principal durante la creación del instalador no afecta a la ubicación del instalador. Después de crear el instalador, se coloca en el grupo de acceso del usuario actual. El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario.
- Tenga en cuenta que el usuario será capaz de trabajar con Certificados al crear instaladores. Asigne el permiso **Usar** a un usuario para **Certificados** con acceso al grupo estático que contiene los certificados. Si un usuario desea implementar un agente ESET Management, dicho usuario debe tener permisos de **Uso** para la autoridad de certificación que firma el certificado de servidor actual. Para obtener información sobre cómo dividir el acceso a Certificados y Autoridad de certificación, lea este ejemplo.

Grupo de pertenencia: el grupo de pertenencia se detecta automáticamente según el conjunto de permisos asignado del usuario activo en ese momento.

Situación de ejemplo:
La cuenta de usuario activa actualmente tiene el derecho de acceso de **Escritura** para la **tarea del cliente Instalación del software** y el **grupo de pertenencia** de la cuenta de usuario es "Department_1". Cuando el usuario cree una nueva **tarea del cliente Instalación del software**, se seleccionará automáticamente "Department_1" como **grupo de pertenencia** de la tarea del cliente.

Si el grupo de pertenencia seleccionado previamente no cumple con sus expectativas, podrá seleccionar el grupo de pertenencia de forma manual.

Permitir que los usuarios creen instaladores

Administrador quiere permitir al usuario *John* crear o editar nuevos instaladores en el *Grupo de John*. El *Administrador* tiene que seguir estos pasos:

1. Crear un nuevo Grupo estático llamado *Grupo de John*
2. Crear un nuevo Conjunto de permisos

a.Asignar un nombre al nuevo conjunto de permisos *Permisos de John: crear instaladores*
b.Agregar el grupo *Grupo de John* en la sección **Grupos estáticos**
c.En la sección **Funcionalidad**, seleccionar

- **Escritura** para **Instaladores almacenadas**
- **Uso** para **Certificados**
- **Escritura** para **Grupos y equipos**

d.Hacer clic en **Finalizar** para guardar el conjunto de permisos

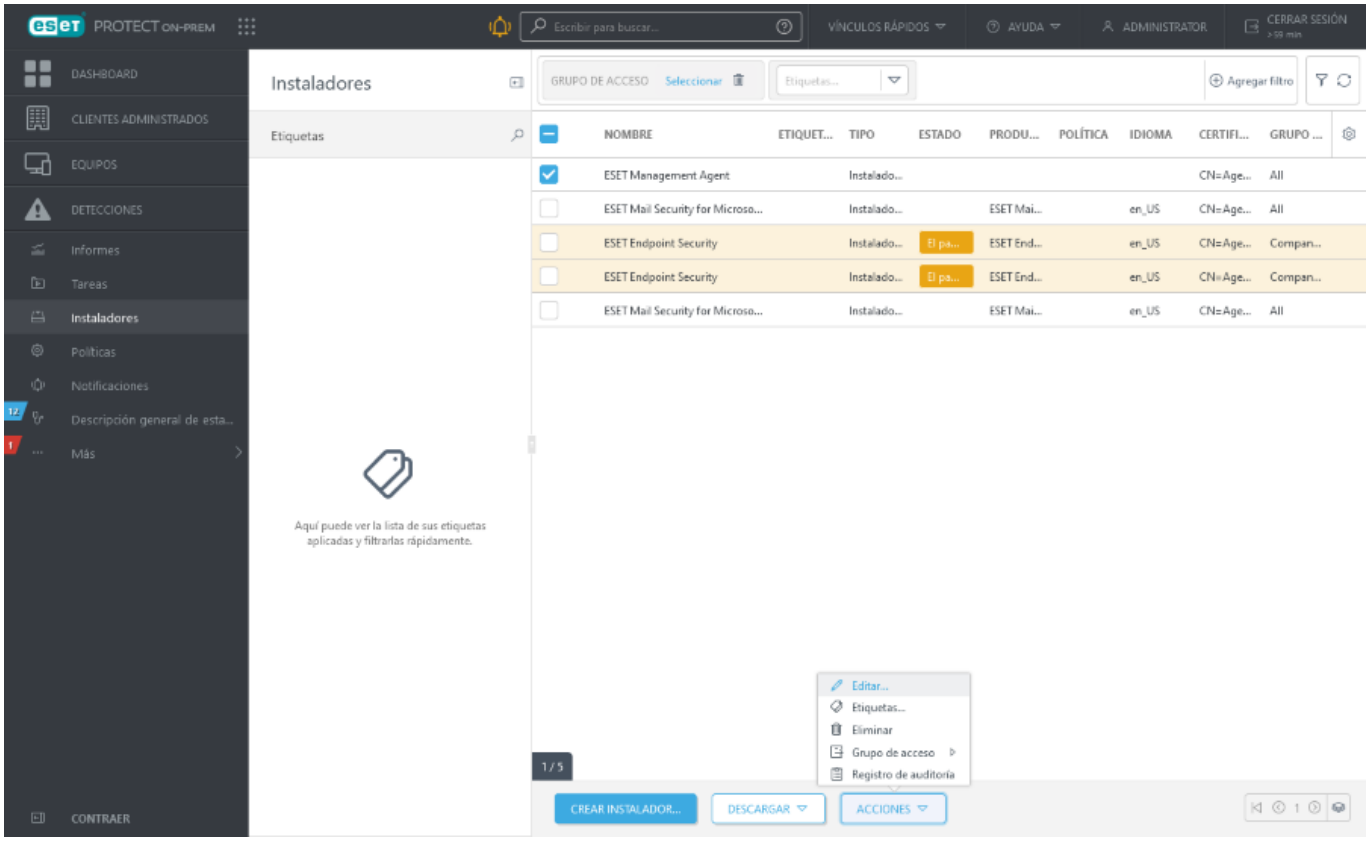
3. Crear un nuevo Conjunto de permisos

a.Asignar un nombre al nuevo conjunto de permisos *Permisos de John: certificados*
b.Agregar el grupo *Todos* en la sección **Grupos estáticos**
c.En la sección **Funcionalidad**, seleccione **Usar** para **Certificados**.
d.Hacer clic en **Finalizar** para guardar el conjunto de permisos

Estos permisos son los requisitos mínimos para uso de instalador completo (crear y editar).

4. Crear un nuevo usuario

a.Asigne el nombre *John* al nuevo usuario.
b.En la sección **Básico**, seleccionar *Grupo de John* como el grupo hogar
c.Establecer la contraseña para el usuario *John*
d.En la sección **Conjuntos de permisos**, seleccione *Permisos para John - Certificados* y *Permisos para John - Crear instaladores*
e.Hacer clic en **Finalizar** para guardar el usuario



Descargar instaladores desde el menú de instaladores

1.Haga clic en **Instaladores**.

2.Seleccionar la casilla de verificación junto al instaladores que desea descargar.

3.Haga clic en **Descargar** y elija el paquete de instalación correcto (según la cantidad de bits o el sistema operativo). Si hay disponible una versión posterior de un producto de ESET en el instalador (producto de seguridad de ESET, conector ESET Inspect o ESET Full Disk Encryption), aparecerá una ventana. Seleccione la casilla de verificación **Acepto el Acuerdo de licencia de usuario final y la Política de privacidad**, y haga clic en **Actualizar y descargar** para actualizar el instalador y descargarlo.

4.Puede encontrar el paquete de instalación en la carpeta donde su navegador web guarda los archivos descargados.

Editar instaladores desde el menú de instaladores

1.Haga clic en **Instaladores**.

2.Seleccionar la casilla de verificación junto al instaladores que desea editar.

3.Haga clic en **Acciones** > **Editar** para modificar el paquete instalador.

Personalización del diseño y de los filtros

Puede personalizar la vista de la pantalla de la consola web actual:

- Administre el panel lateral y la tabla principal.

- Agregar filtro y filtros preestablecidos. Puede usar etiquetas para filtrar los elementos mostrados.

Políticas

Las políticas se usan para insertar configuraciones específicas a los productos ESET que se ejecutan en equipos cliente. Esto le permite evitar la configuración del producto de ESET de cada cliente en forma manual. Puede aplicarse políticas directamente en equipos individuales y también en grupos (estáticos y dinámicos). Además, puede asignar políticas múltiples a un equipo o a un grupo.

Políticas y permisos

El usuario necesita tener permisos suficientes para crear y asignar políticas. Permisos necesarios para ciertas acciones de políticas:

- Para leer la lista de políticas y su configuración, un usuario necesita permisos de **Lectura**.
- Para asignar políticas a objetivos, un usuario necesita permisos de **Uso**.
- Para crear, modificar o editar políticas, un usuario necesita permisos de **Escritura**.

Consulte la lista de permisos para obtener más información sobre los derechos de acceso.

Hay un icono de bloqueo junto a políticas bloqueadas (no editables): políticas integradas específicas (por ejemplo, la política de actualización automática o las políticas de ESET LiveGuard) o políticas en las que el usuario tiene el permiso de **Lectura**, pero no de **Escritura**.

- Si el usuario *John* solo necesita leer las políticas creadas por él, se necesitan permisos de **Lectura** para las **Políticas**.
- Si el usuario *John* desea asignar ciertas políticas a equipos, necesita permisos de **Uso** para las **Políticas** y permisos de **Uso** para los **Grupos y equipos**.
- Para que *John* tenga acceso completo a las políticas, el *Administrador* debe establecer permisos de **Escritura** para las **Políticas**.

Aplicación de políticas

Las políticas se aplican en el orden en que se acomodan los Grupos estáticos. Esto no ocurre con los Grupos dinámicos, donde los más recientes se recorren primero. Esto le permite aplicar políticas con un mayor impacto en la parte superior del árbol del grupo y políticas más específicas definidas por subgrupos. Mediante indicadores, un usuario de ESET PROTECT On-Prem con acceso a los grupos ubicados en la parte más alta del árbol puede anular las políticas de grupos. El algoritmo se explica en detalle en Cómo se aplican las políticas a los clientes.

Reglas de eliminación de políticas

Cuando decida quitar una política aplicada, la configuración resultante de los equipos del cliente dependerá de la versión instalada del producto de seguridad de ESET en los equipos administrados.

- Al quitar una política o seleccionar el indicador **No se aplica**, la configuración vuelve automáticamente a los valores locales anteriores. Cuando un equipo deja un Grupo dinámico donde había una configuración de política vigente, estas configuraciones de políticas se quitarán del equipo. Este comportamiento se aplica a:

Productos de seguridad ESET Windows	versión 7 y posteriores
Productos de seguridad ESET macOS	versión 7 y posteriores
Productos de seguridad ESET Linux	versión 8.1 y posteriores

- Productos de seguridad de ESET más antiguos (que los mencionados anteriormente): La configuración no volverá automáticamente a la configuración original cuando se elimine la política. La configuración se mantendrá de acuerdo a la política más reciente aplicada a los clientes. Lo mismo ocurre cuando un equipo se convierte en miembro de un Grupo dinámico al que se le aplica cierta política que cambia las configuraciones del equipo. Estas configuraciones se mantienen, aún si el equipo deja de formar parte del grupo dinámico. En consecuencia, le recomendamos que genere una política con las configuraciones por defecto y la asigne al grupo raíz (**Todos**) para que la configuración vuelva a la predeterminada en dicha situación. De esta forma, cuando un equipo deja un Grupo dinámico que cambió su configuración, el equipo volverá a la configuración predeterminada.

Combinar políticas

Una política que se aplica a un cliente a menudo es el resultado de múltiples políticas que se combinan en una política final.

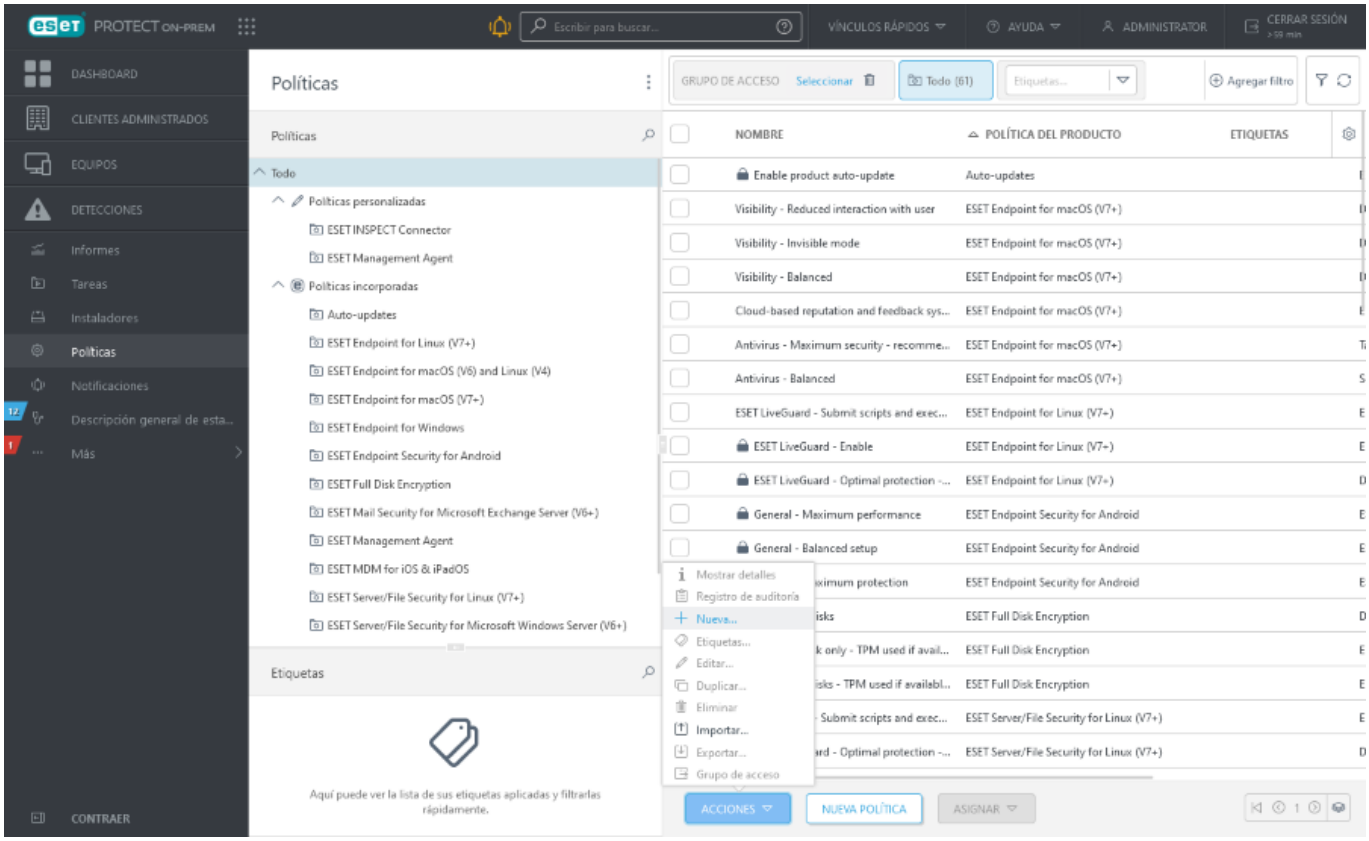
> Recomendamos que asigne políticas más genéricas (por ejemplo, el servidor de actualización) a los grupos que se ubiquen en la parte superior del árbol de grupo. Las políticas más específicas (por ejemplo, la configuración de control del dispositivo) se deben aplicar al grupo que se ubique en la parte inferior del árbol. Las políticas inferiores suelen reemplazar las configuraciones de las superiores cuando se combinan (a menos que se defina lo contrario con indicadores de políticas).

Asistente de políticas

Las políticas se agrupan/categorizan por producto ESET. Las **políticas incorporadas** incluyen políticas definidas previamente y las **políticas personalizadas** enumeran las categorías de todas las políticas que ha creado o modificado manualmente.

Use políticas para configurar su producto ESET del mismo modo en que lo haría desde la ventana de Configuración avanzada de la interfaz gráfica del usuario del producto. A diferencia de las políticas en Active Directory, las políticas de ESET PROTECT On-Prem no pueden contener ninguna cadena o serie de comandos.

Escriba para buscar un elemento en la Configuración avanzada (por ejemplo, HIPS). Se mostrarán todas las configuraciones de HIPS. Cuando haga clic en el icono en el ángulo superior derecho, se mostrará la pagina de ayuda En línea de la configuración particular.



Personalización del diseño y de los filtros

Puede personalizar la vista de la pantalla de la consola web actual:

- Administre el panel lateral y la tabla principal.
- Agregar filtro y filtros preestablecidos. Puede usar etiquetas para filtrar los elementos mostrados.

Creación de una política nueva

1.Haga clic en **Acciones** > **Nuevo**.

2.Ingrese la información básica acerca de la política, como el **Nombre** y la **Descripción** (opcional). Haga clic en **Seleccionar etiquetas** para asignar etiquetas.

3.Seleccione el producto correcto en la sección **Configuración**.

4.Use indicadores para agregar configuraciones que serán gestionadas por la política.

5.Especifica los clientes que recibirán esta política. Haga clic en **Asignar** para visualizar todos los Grupos estáticos y dinámicos y a sus miembros. Seleccione el equipo donde quiere aplicar la política y haga clic en **Aceptar**.

6.Revise la configuración de esta política y haga clic en **Finalizar**.

Indicadores

Al combinar políticas puede cambiar su comportamiento a través de indicadores de política. Los indicadores definen la manera en que una política manejará la configuración.

Para cada ajuste puede seleccionar uno de los siguientes indicadores:

No aplicar: todo ajuste con este indicador no se establece por la política. Debido a que la configuración no está forzada, las políticas posteriores pueden modificarla.

Aplicar: se le enviará al cliente una configuración con este indicador. Sin embargo, al combinar las políticas, puede ser anulada por una política posterior. Cuando la política se aplica a un equipo cliente y una configuración en particular tiene este indicador, esta configuración se modifica independientemente de lo configurado por el cliente localmente. Debido a que la configuración no está forzada, las políticas posteriores pueden modificarla.

Forzar: los ajustes con una configuración con el indicador de forzar tienen prioridad y no pueden anularse por una política posterior (incluso si esta política también tiene establecido el indicador de forzar). Esto garantiza que las políticas posteriores no modificarán la configuración durante una combinación.

Para que la navegación sea más fácil, se consideran todas las reglas. Se mostrará en forma automática la cantidad de reglas que haya definido en una sección en particular. Asimismo, verá un número junto a los nombres de la categoría en el árbol que se encuentra a la izquierda. Esto muestra la suma de las reglas en todas las secciones. De esta forma, puede ver rápidamente dónde y cómo se definen muchas configuraciones/reglas.

También puede usar las siguientes sugerencias para que la edición de políticas sea más simple:

- Use para establecer el indicador de **Aplicar** para todos los elementos de la sección actual
- Utilice el indicador **No aplicar** para quitar las reglas aplicadas a los elementos de la sección actual.

Ver también Reglas de eliminación de políticas.

Cómo puede un Administrador permitir que los usuarios vean todas las políticas

Administrador desea permitir al usuario *John* crear o editar políticas en su grupo hogar y permitirle a *John* ver las políticas creadas por *Administrador*. Las políticas creadas por *Administrator* incluyen indicadores de **Forzar**. El usuario *John* puede ver todas las políticas pero no puede editar las creadas por *Administrador*porque está establecido un permiso de **Lectura** para las **Políticas** con acceso al Grupo estático *Todos*. El usuario *John* puede crear o editar políticas en su grupo hogar *San Diego*.
El *Administrador* tiene que seguir estos pasos:
Crear ambiente
1.Crear un nuevo Grupo estático llamado *San Diego*.
2.Crear un nuevo conjunto de permisos llamado *Política - Todos John* con acceso al grupo estático *Todos* y permisos de **Lectura** para **Políticas**.
3.Crear un nuevo conjunto de permisos llamado *Política John* con acceso al grupo estático *San Diego*, con acceso a funcionalidad y permiso de **Escritura** para **Grupo y equipos** y **Políticas**. Este conjunto de permisos le permite al usuario *John* crear o editar políticas en su grupo hogar *San Diego*.
4.Cree un nuevo usuario *John* y, en la sección **Conjuntos de permisos**, seleccione *Política - Todo John* y *Política John*.
Crear políticas
5.Crear una nueva política *Todos - Habilitar Firewall*, expandir la sección **Configuración**, seleccionar **ESET Endpoint para Windows**, ir a **Protección de red** > **Firewall** > **Básico** y aplicar todas las configuraciones mediante un indicador **Forzar**. Expandir la sección **Asignar** y seleccionar el grupo estático *Todos*.
6.Crear una nueva política *Grupo John - Habilitar Firewall*, expandir la sección **Configuración**, seleccionar **ESET Endpoint para Windows**, ir a **Protección de red** > **Firewall** > **Básico** y aplicar las configuraciones mediante un indicador **Aplicar**. Expandir la sección **Asignar** y seleccionar el grupo estático *San Diego*.
Resultado
Se aplicarán primero las políticas creadas por el *administrador* porque están asignadas al grupo *Todo*. Los ajustes con el indicador **Forzar** tienen prioridad y no pueden ser sobrescritos por una política más reciente. Luego se aplicarán las políticas creadas por el usuario *John*.
Ir a **Más** > **Grupos** > **San Diego**, hacer clic en el equipo y seleccionar **Detalles**. En **Configuración** > **Políticas aplicadas** es el orden final de aplicación de políticas.

ORDEN...	POLÍTICA DEL ...	NOMBRE DE L...	DESCRIPCIÓN ...
1 (aplicado prime...	Common features	Enable produ...	Enable automatic...
2	ESET Endpoint fo...	Protection se...	This policy enabl...

La primera política la crea *Administrador* y la segunda creada por el usuario *John*.

Grupo de pertenencia: el grupo de pertenencia se detecta automáticamente según el conjunto de permisos asignado del usuario activo en ese momento.

Situación de ejemplo:
La cuenta de usuario activa actualmente tiene el derecho de acceso de **Escritura** para la **tarea del cliente Instalación del software** y el **grupo de pertenencia** de la cuenta de usuario es "Department_1". Cuando el usuario cree una nueva **tarea del cliente Instalación del software**, se seleccionará automáticamente "Department_1" como **grupo de pertenencia** de la tarea del cliente.

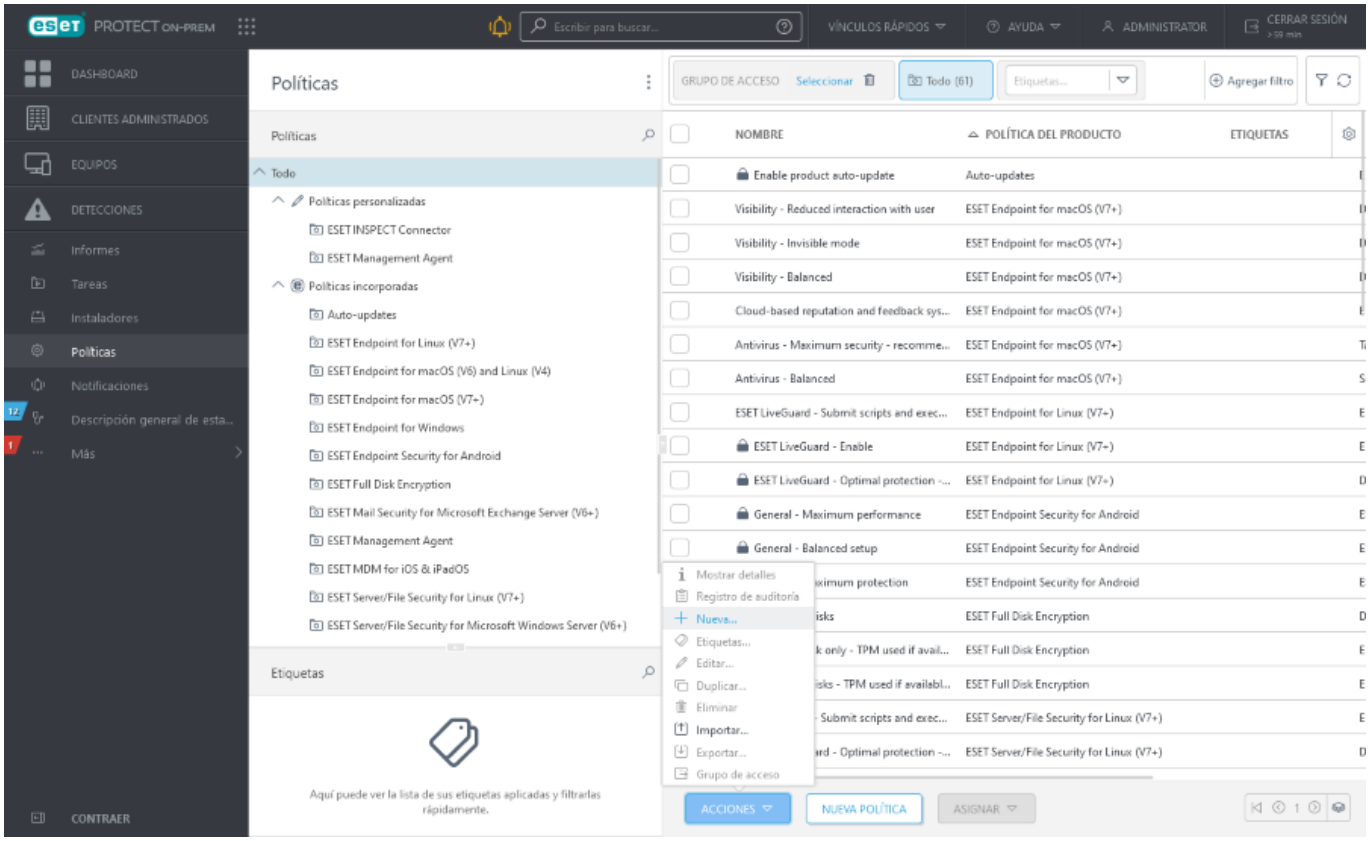
Si el grupo de pertenencia seleccionado previamente no cumple con sus expectativas, podrá seleccionar el grupo de pertenencia de forma manual.

Administrar políticas

Las políticas se agrupan/categorizan por producto ESET. Las **políticas incorporadas** incluyen políticas definidas previamente y las políticas personalizadas enumeran las categorías de todas las políticas que ha creado o modificado manualmente.

Acciones disponibles para las políticas:

Mostrar detalles	Mostrar detalles de la política.
Registro de auditoría	Ver el registro de auditoría del elemento seleccionado.
Nueva	Creación de una política nueva.
Etiquetas	Editar etiquetas (asignar, desasignar, crear, quitar).
Editar	Modificar una política existente.
Duplicar	Crear una nueva política con base en una política´ existente que ha seleccionado. La política duplicada necesita de un nuevo nombre.
Cambiar asignaciones	Asignación de una política a un grupo o a un cliente.
Eliminar	Eliminar una política. Ver también Reglas de eliminación de políticas.
Importar	Haga clic en **Políticas** > **Importar**, luego haga clic en **Seleccionar archivo** y busque el archivo que desea importar. Solo puede importar un archivo *.dat* que contenga las políticas exportadas de la Consola web de ESET PROTECT. No puede importar un archivo *.xml* que contenga las políticas exportadas del producto de seguridad de ESET. Las políticas importadas aparecerán en **Políticas personalizadas**.
Exportar	Seleccione las casillas de verificación junto a las políticas que desea exportar de la lista y haga clic en **Acciones** > **Exportar**. Se exportarán las políticas a un archivo *.dat*. Para exportar todas las políticas de la categoría seleccionada, marque la casilla de verificación del encabezado de la tabla.
Grupo de acceso > **Mover**	Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen derechos suficientes para el grupo de destino. Cambiar el grupo de acceso es útil cuando se resuelven problemas de acceso con otros usuarios. El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario.



Cómo se aplican las políticas a los clientes

Se le pueden asignar varias políticas tanto a los grupos como a los equipos. Es más, un equipo puede estar en un grupo profundamente anidado, de los cuales los padres tienen sus propias políticas.

Lo más importante para la aplicación de las políticas es su orden. Esto se deriva del orden de los grupos y del orden de las políticas asignadas al grupo.

Para ver todas las políticas aplicadas a un equipo seleccionado, consulte Políticas aplicadas en los detalles del equipo.

Siga los pasos a continuación para determinar la política activa en cualquier cliente:

1. Encuentre el orden de los grupos en los que reside el cliente
2. Reemplace grupos por políticas asignadas
3. Combine políticas para obtener los ajustes finales

Orden de grupos

Las políticas se pueden asignar a grupos, **y se aplican en un orden específico. Las reglas a continuación determinan el orden en que las políticas se aplican a los clientes**.

Regla 1: Los Grupos estáticos se recorren desde el Grupo estático raíz (**Todos**).

Regla 2: En cada nivel, los Grupos estáticos de ese nivel se recorren por primera vez en el orden en que aparecen en el árbol (esto también se denomina búsqueda “en amplitud”).

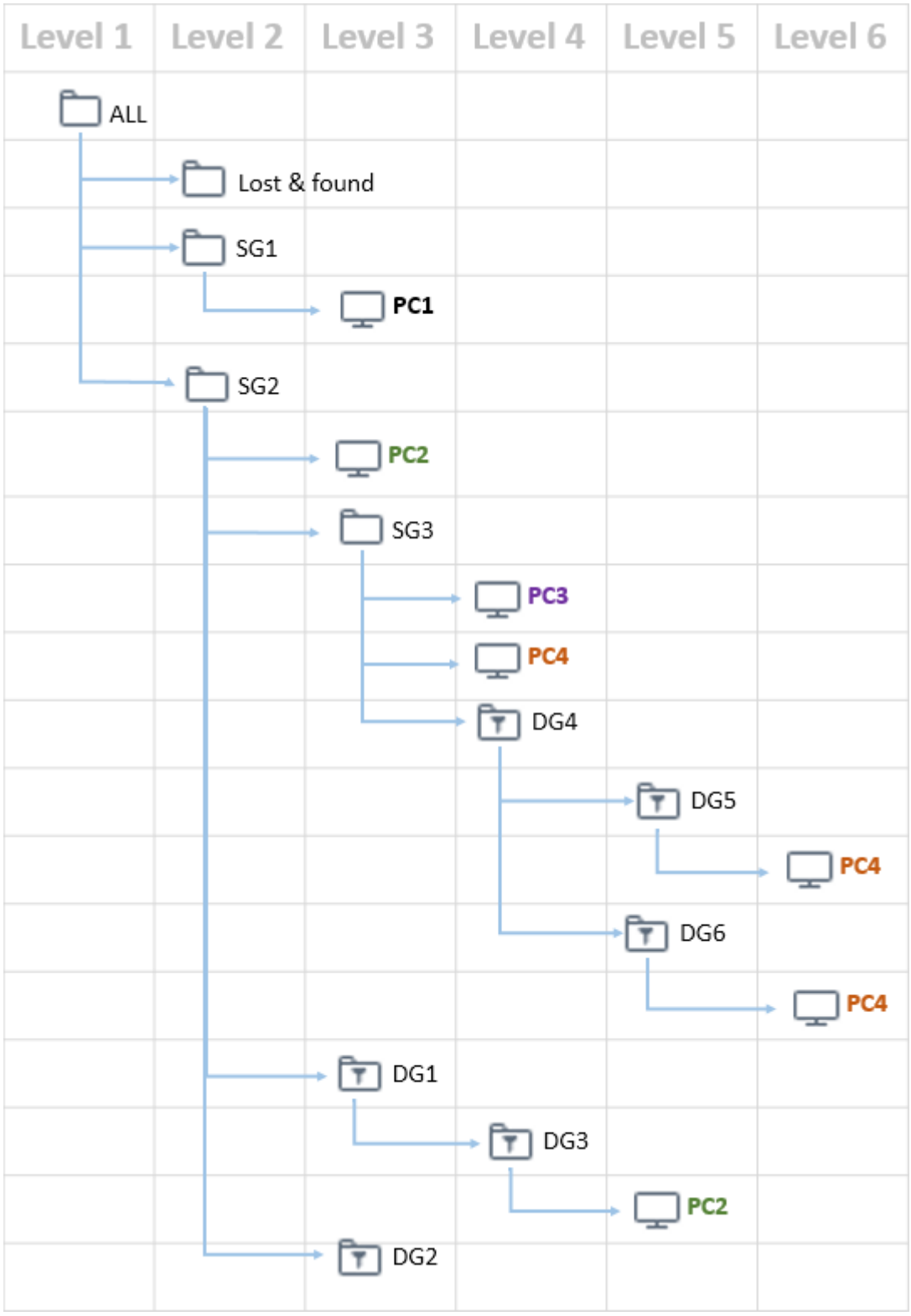
Regla 3: Después de que todos los Grupos estáticos en un cierto nivel están representados, se recorren los Grupos dinámicos.

Regla 4: En cada Grupo dinámico, todos los niños se recorren en el orden en que aparecen en la lista.

Regla 5: En cualquier nivel de un grupo dinámico, todo secundario se enumerará y será analizado en busca de sus secundarios. Cuando no hay más niños, los próximos Grupos dinámicos en el nivel primario se enumeran (esto también se denomina búsqueda “en profundidad”).

Regla 6: El recorrido termina en un equipo.

La política se aplica al equipo. Esto significa que el recorrido termina en el equipo en el que desea aplicar la política.



Al usar las reglas escritas anteriormente, el orden de aplicación de las políticas en equipos individuales será la siguiente:

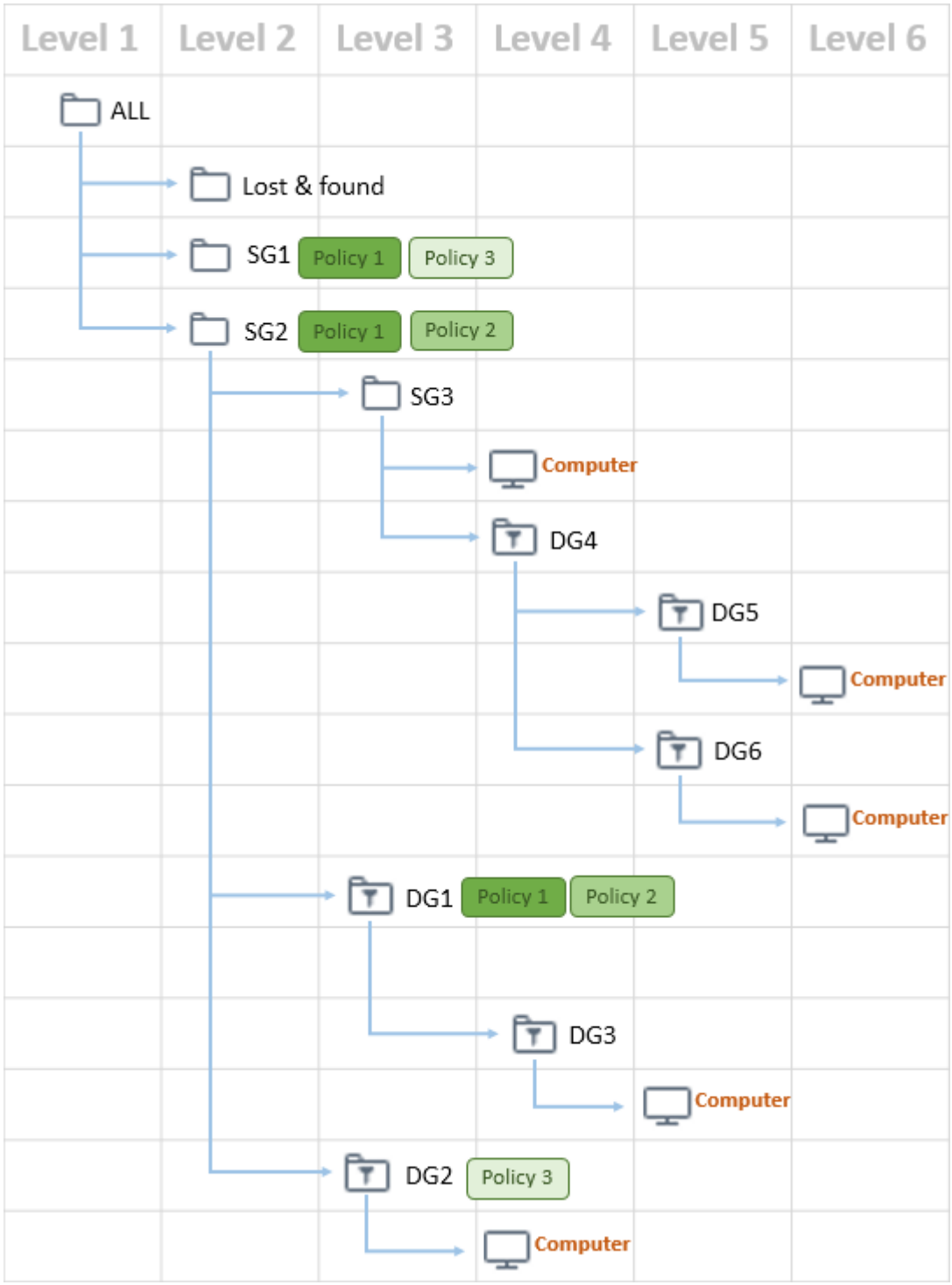
PC1:	PC2:	PC3:	PC4:
1.ALL 2.SG1 3.PC1	1.ALL 2.SG2 3.DG1 4.DG3 5.PC2	1.ALL 2.SG2 3.SG3 4.PC3	1.ALL 2.SG2 3.SG3 4.DG4 5.DG5 6.DG6 7.PC4

Enumeración de políticas

Una vez que se conoce el orden de los grupos, el siguiente paso es reemplazar cada grupo con las políticas que se les asignen. Las políticas se enumeran en el mismo orden en que se asignan a un grupo. Es posible editar la prioridad de las políticas de un grupo con más políticas asignadas. Cada política configura solo un producto (agente ESET Management, ESET Endpoint Security, etc.).

Un grupo sin una política se elimina de la lista.

Contamos con 3 políticas aplicadas tanto en grupos estáticos como dinámicos (vea la imagen abajo):



El orden en que se aplicarán políticas en el equipo

La siguiente lista muestra grupos y las políticas que se aplican sobre ellos:

1.Todo: eliminado, sin política aquí

2.SG 2 -> Política 1, Política 2

3.SG 3 -> eliminado por no tener ninguna política

4.DG 1 – Política 1, Política 2

5.DG 3 – eliminado, no hay políticas

6.DG 2 – Política 1, Política 3

7.DG 4 – eliminado, no hay políticas

8.DG 5 – eliminado, no hay políticas

9.DG 6 – eliminado, no hay políticas

10. Equipo: quitado, sin política

La lista final de políticas es:

1.Política 1

2.Política 2

3.Política 1

4.Política 2

5.Política 3

Combinar políticas

Cuando aplica una política a un producto de seguridad de ESET en el que ya se ha aplicado otra política, la configuración de la política que se superpone se combina. Las políticas se fusionaron una a una. Al fusionar políticas, la regla general es que la última política siempre reemplaza la configuración establecida por la anterior. Para cambiar este comportamiento, puede usar los indicadores de política (disponible en todas las configuraciones). Algunas configuraciones tienen otra regla (reemplazar/añadir/anteponer) que puede configurar.

Tenga en cuenta que la estructura de los grupos (su jerarquía) y la secuencia de las políticas determina cómo se combinan las políticas. La combinación de dos políticas cualesquiera puede tener distintos resultados diferentes según su orden.

Al crear políticas, verá que algunas configuraciones poseen reglas adicionales que puede configurar. Estas reglas le permiten colocar los mismos ajustes en varias políticas.

- **Sustituir**: la regla predeterminada que se usa al combinar políticas. Reemplaza la configuración establecida por la política anterior.

- **Añadir**: al aplicar la misma configuración en más de una política, puede añadir la configuración con esta regla. La configuración se colocará al final de la lista que se creó al combinar políticas.

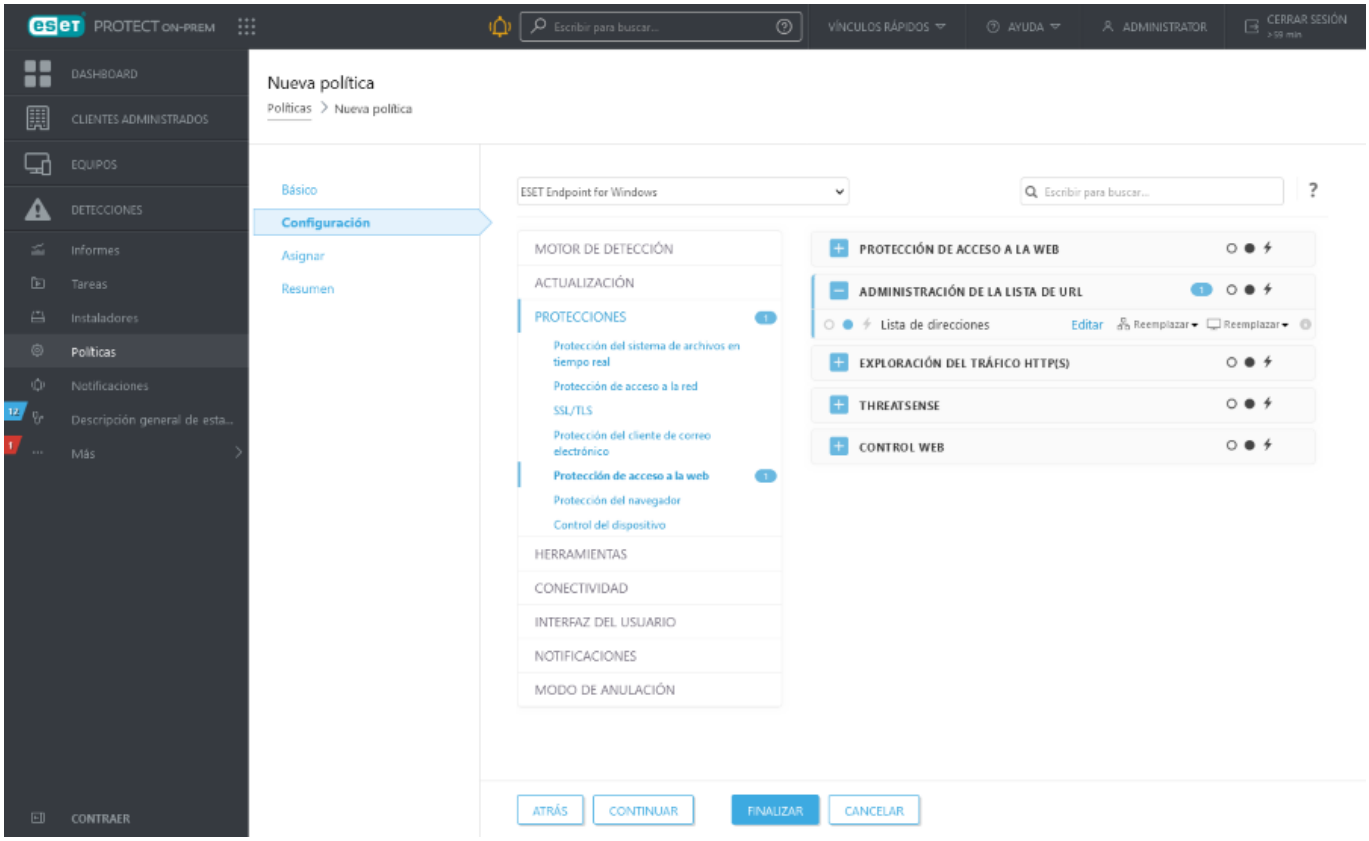
- **Anteponer**: al aplicar la misma configuración en más de una política, puede anteponer la configuración con esta regla. La configuración se colocará al inicio de la lista que se creó al combinar políticas.

Fusión de listas locales y remotas

Los últimos productos de seguridad de ESET (vea las versiones compatibles en la siguiente tabla) pueden fusionar las configuraciones locales con las políticas remotas de una nueva manera. Si la configuración es una lista (por ejemplo, una lista de sitios web) y la política remota entra en conflicto con una configuración local existente, la política remota la sobrescribe. Puede escoger cómo combinar listas locales y remotas. Puede seleccionar

diferentes reglas de fusión para:

- Configuración de fusión para políticas remotas.
- Fusión de políticas remotas y locales: configuraciones locales con la resultante política remota. Las opciones son las mismas mencionadas anteriormente: **Reemplazar**, **Añadir**, **Anteponer**.



Ver también Reglas de eliminación de políticas.

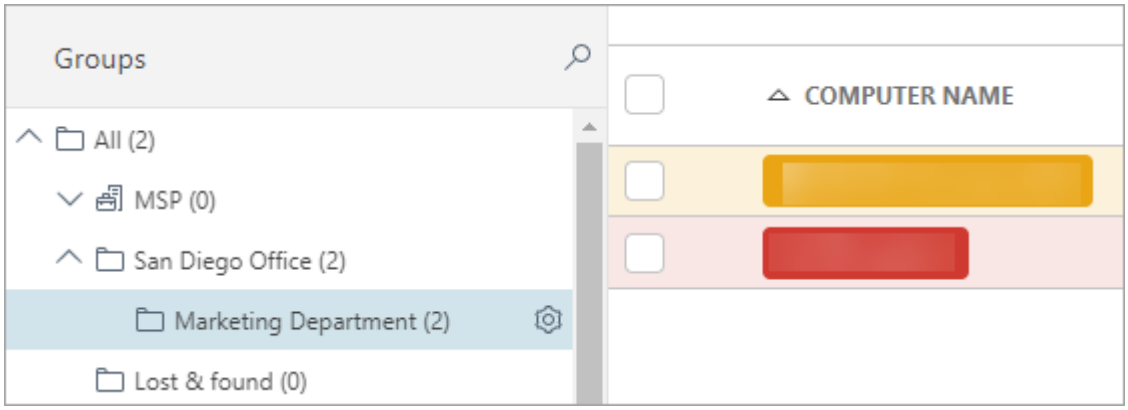
Ejemplo de escenario de políticas combinadas

Este ejemplo describe:

- Instrucciones sobre cómo aplicar configuraciones a productos de seguridad ESET Endpoint
- Cómo las políticas se combinan al aplicar indicadores y reglas

En situaciones donde el *Administrador* desea:

- Denegar acceso de la *Oficina en San Diego* a los sitios web *www.forbidden.uk*, *www.deny-access.com*, *www.forbidden-websites.uk* y *www.forbidden-website.com*
- Permitir que el *Departamento de Mercadeo* acceda a los sitios web *www.forbidden.uk*, *www.deny-access.com*



El *Administrador* tiene que seguir estos pasos:

1. Crear un nuevo grupo estático *Oficina en San Diego* y luego *Departamento de mercadeo* como un subgrupo del grupo estático *Oficina en San Diego*.

2. Ir a **Políticas** y crear un nueva política de la siguiente manera:

   i)Llamada *Oficina en San Diego*.

   ii)Expandir **Configuración** y seleccionar **ESET Endpoint para Windows**

   iii)Vaya a **Protecciones** > **Protección de acceso a la Web** > **Administración de listas de URL**

   iv)Hacer clic en el botón para **Aplicar** la política y editar la **Lista de direcciones** haciendo clic en**Editar**

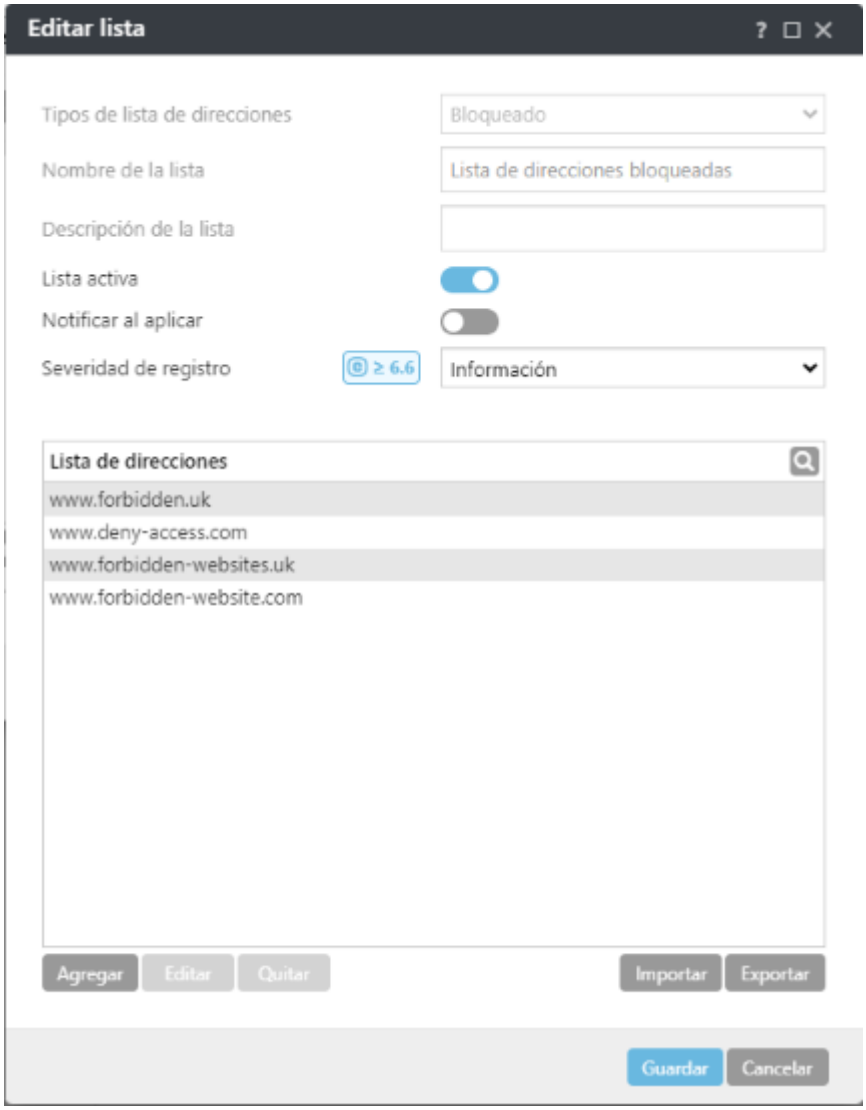
   v)Hacer clic en **Lista de direcciones bloqueadas** y seleccionar **Editar**.

   vi)Agregar las siguientes direcciones web: *www.forbidden.uk*, *www.deny-access.com*, *www.forbidden-websites.uk* y *www.forbidden-website.com*. Guardar la lista de direcciones bloqueadas y luego la lista de direcciones.

   vii) Expandir **Asignar** y asignar la política a *Oficina en San Diego* y su subgrupo *Departamento de Mercadeo*.

   viii) Haga clic en **Finalizar** para guardar la política.

Esta política se aplicará a la *Oficina en San Diego* y *Departamento de mercado* y bloqueará los sitios web como se muestra a continuación.

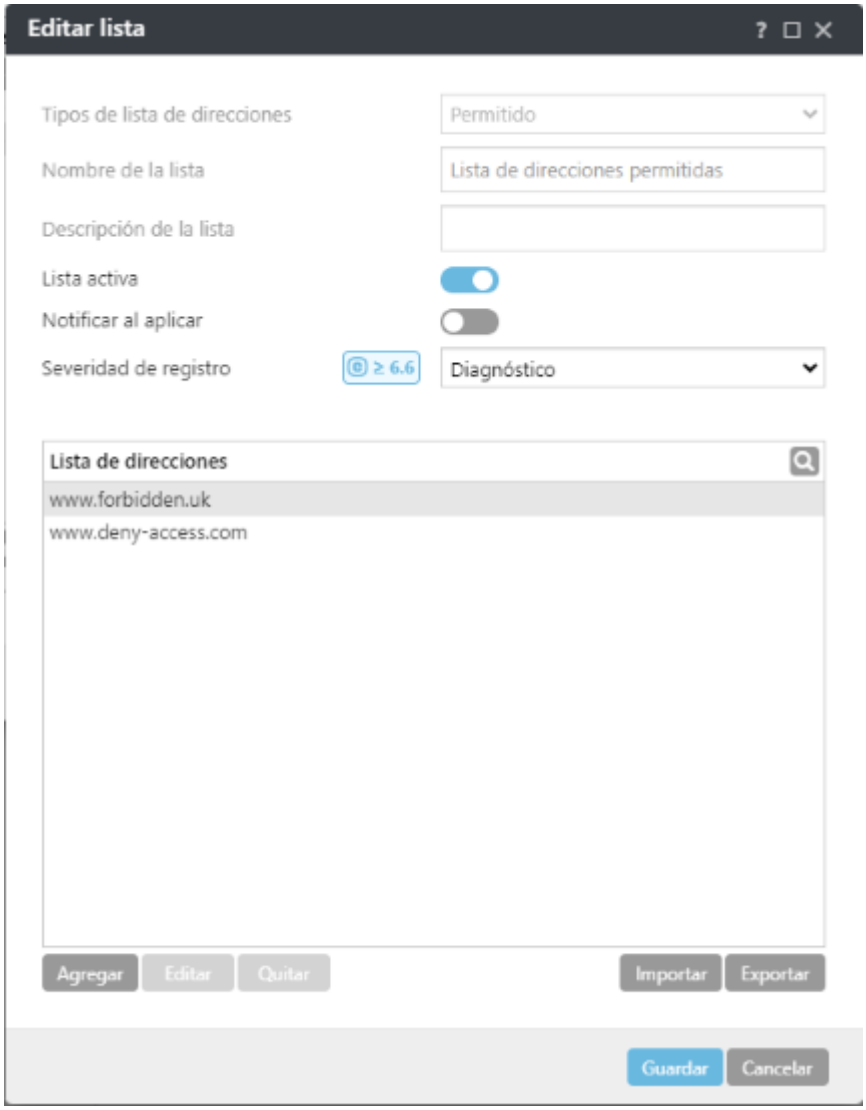


3. Ir a **Políticas** y crear una nueva política:

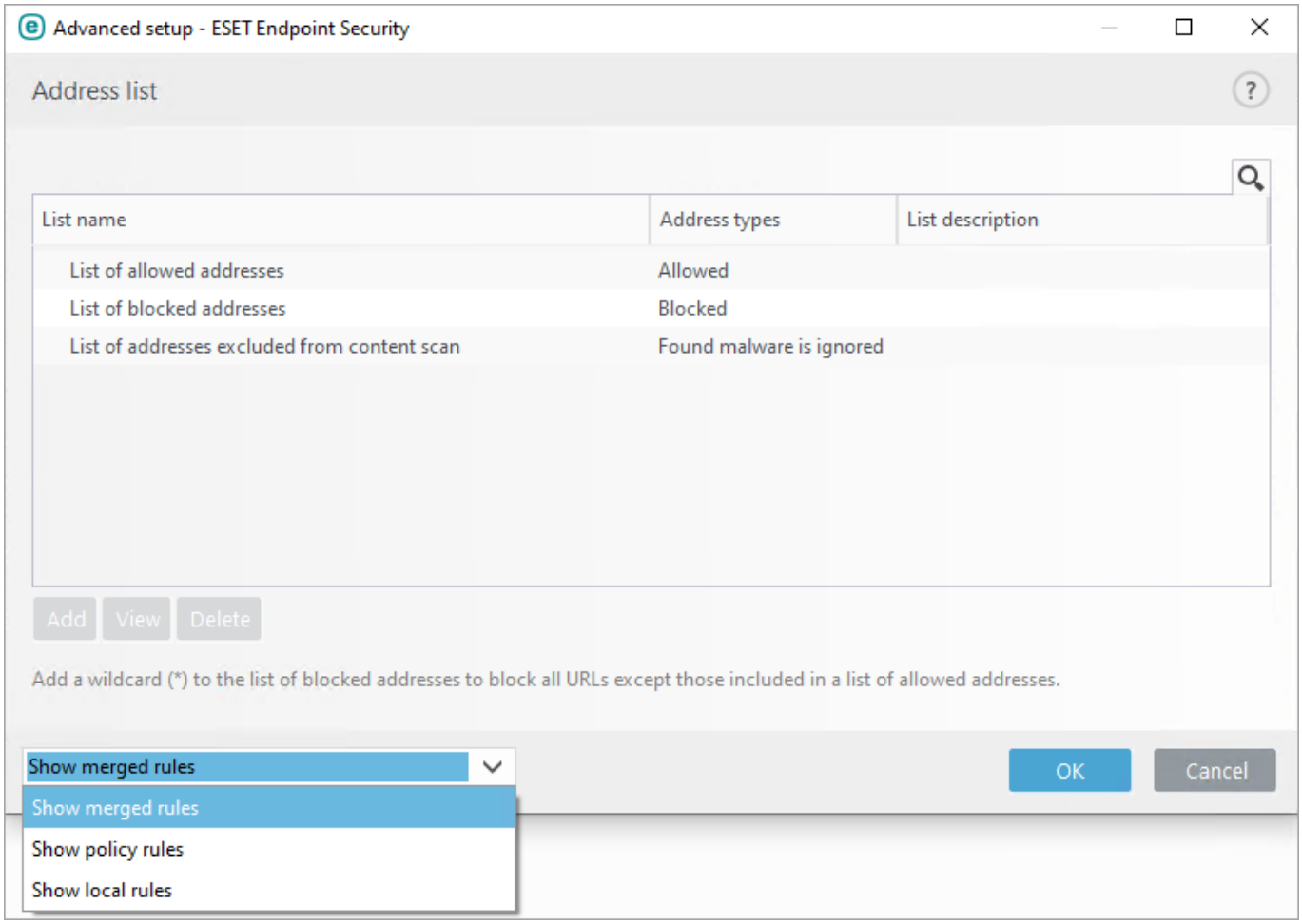
   i)Llamada *Departamento de mercadeo*.
   ii)Expandir **Configuración** y seleccionar **ESET Endpoint para Windows**
   iii)Vaya a **Protecciones** > **Protección de acceso a la Web** > **Administración de listas de URL**
   iv)Hacer clic en el botón para **Aplicar** la política, seleccionar Añadir regla y, luego, editar la **Lista de direcciones** haciendo clic en**Editar** Añadir regla hace que la lista de direcciones se colocará al final al combinar políticas.
   v)Hacer clic en **Lista de direcciones permitidas** y seleccionar **Editar**.
   vi)Agregar las siguientes direcciones web: *www.forbidden.uk*, *www.deny-access.com*. Guardar la lista de direcciones permitidas y, luego, la lista de direcciones.
   vii) Expandir **Asignar** y asignar la política al *Departamento de Mercadeo*

   viii) Haga clic en **Finalizar** para guardar la política.

Esta política se aplicará al *Departamento del mercadeo* y permitirá el acceso a los sitios web como se muestra a continuación.



4. La política final incluirá ambas políticas aplicada a la *Oficina en San Diego* y el *Departamento de mercadeo*. Abra **ESET Endpoint Security**, vaya a **Configuración** > **Configuración avanzada** > **Protecciones** > **Protección de acceso a la Web** > y expanda **Administración de listas de URL**. Se mostrará la configuración final del producto de terminales.



La configuración final incluye:

- Lista de direcciones de política de *Oficina en San Diego*
- Lista de direcciones de política de *Departamento de mercadeo*

Configuración de un producto de ESET PROTECT On-Prem

Puede usar políticas para configurar su producto ESET del mismo modo en que lo haría desde la ventana de configuración avanzada de la interfaz gráfica del usuario del producto. A diferencia de las políticas en Active Directory, las políticas de ESET PROTECT On-Prem no pueden contener ninguna cadena o serie de comandos.

Para productos ESET versión 6 y más nuevos, puede configurar ciertos estados para informar en el cliente o la consola web. Se puede configurar en una política para un producto v6 en **Interfaz de usuario** > **Elementos de interfaz de usuario** > **Estados**:

- **Mostrar**: se informa el estado en la interfaz gráfica del cliente
- **Enviar**: se informa el estado a ESET PROTECT On-Prem

Ejemplos de uso de política para configurar productos ESET:

- Configuración de políticas del agente ESET Management

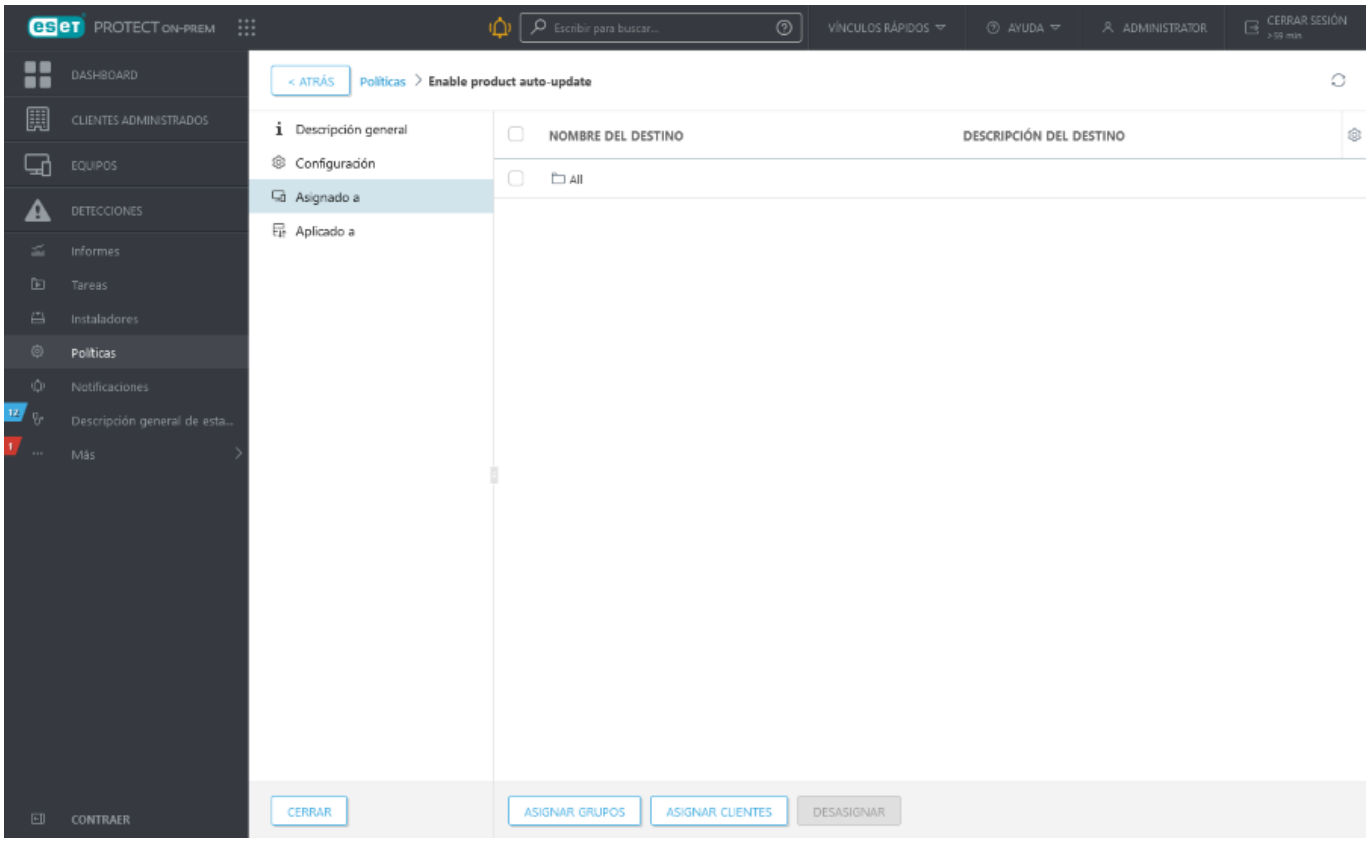
- Ajustes de política de ESET Rogue Detection Sensor
- Crear una política para iOS MDM - Cuenta de Exchange ActiveSync
- Crear una política para que MDC active APNS para la inscripción de iOS

Asignación de una política a un grupo

Después de crear una política, puede asignarla a un **Grupo estático** o **dinámico**. Hay dos formas de asignar una política:

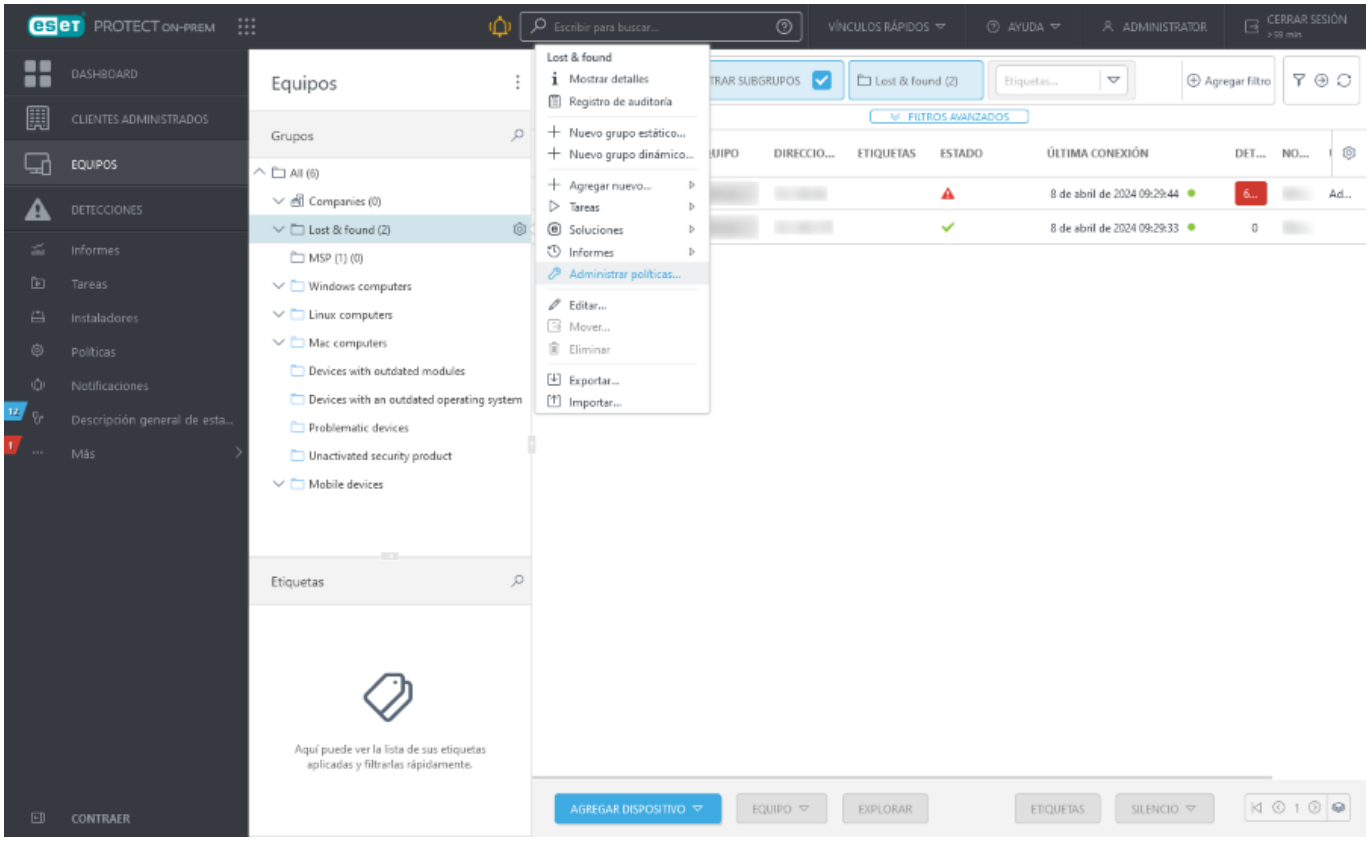
Método I.

En **Políticas**, seleccione una política y haga clic en **Acciones** > **Mostrar detalles** > **Asignado a** > **Asignar grupo(s)**. Seleccione un grupo estático o dinámico de la lista (puede seleccionar más grupos) y haga clic en **Aceptar**.



Método II.

1. Haga clic en **Equipos** y luego en el ícono del engranaje junto al nombre del grupo y seleccione **Administrar políticas**.



2. En la ventana de **Orden de aplicación de políticas** haga clic en **Agregar política**.

3. Seleccione la casilla de verificación junto a la política que desea asignar a este grupo y haga clic en **Aceptar**.

4. Haga clic en **Cerrar**.

Para ver qué políticas se asignaron a un grupo en particular, seleccione ese grupo y haga clic en la pestaña de **Políticas** para visualizar una lista de políticas asignadas al grupo.

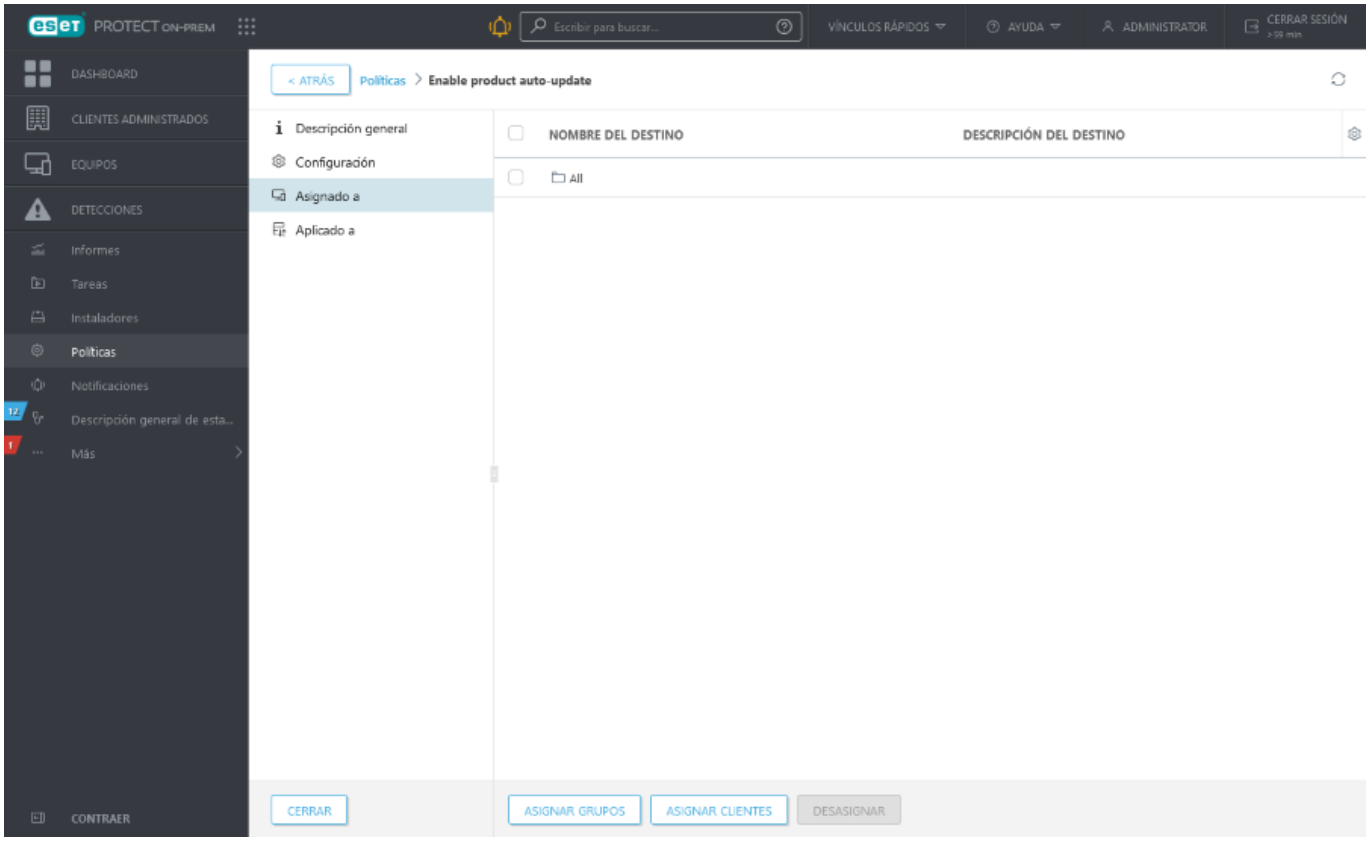
Para ver cuáles grupos están asignados a una política en particular, seleccione la política y haga clic en **Mostrar detalles** > **Aplicado a**.

Para obtener más información acerca de las políticas, consulte el capítulo Políticas.

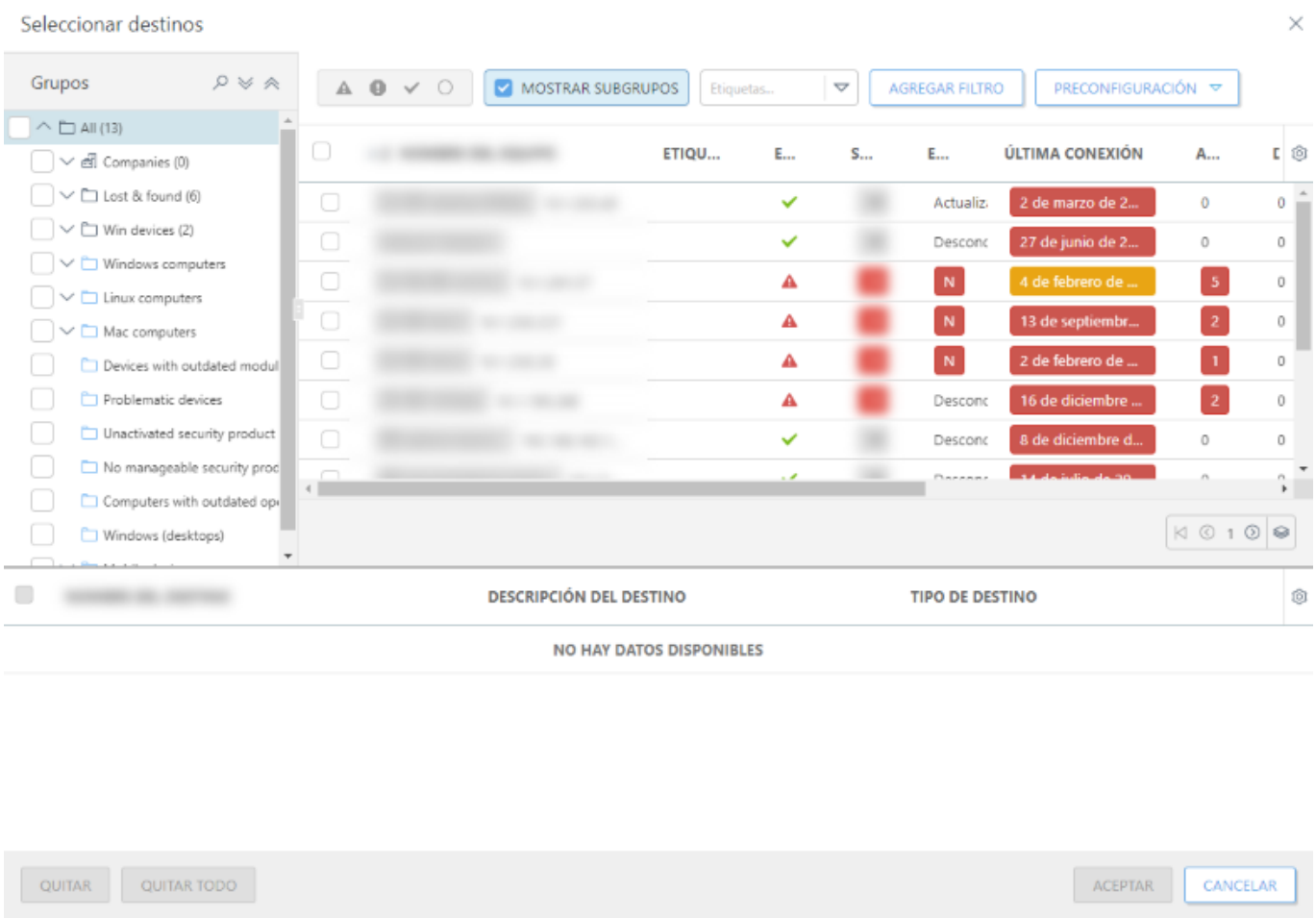
Asignar una política a un cliente

Para asignar una política a una estación de trabajo de cliente, haga clic en **Políticas**, seleccione una política y haga clic en **Acciones** > **Mostrar detalles** > **Asignado a** > **Asignar clientes**.

Para asignar todos los equipos de un grupo, asigne el grupo en lugar de los equipos individuales para evitar que la consola web se ralentice.
Si selecciona una gran cantidad de equipos, la consola web muestra una advertencia.



Seleccione los equipos cliente de destino y haga clic en **Aceptar**. Se asignará la política a todos los equipos que haya seleccionado.



Para ver cuáles clientes están designados a una política en particular, seleccione la política y haga clic en la primera pestaña **Designado a**.

Cómo utilizar el modo anulación

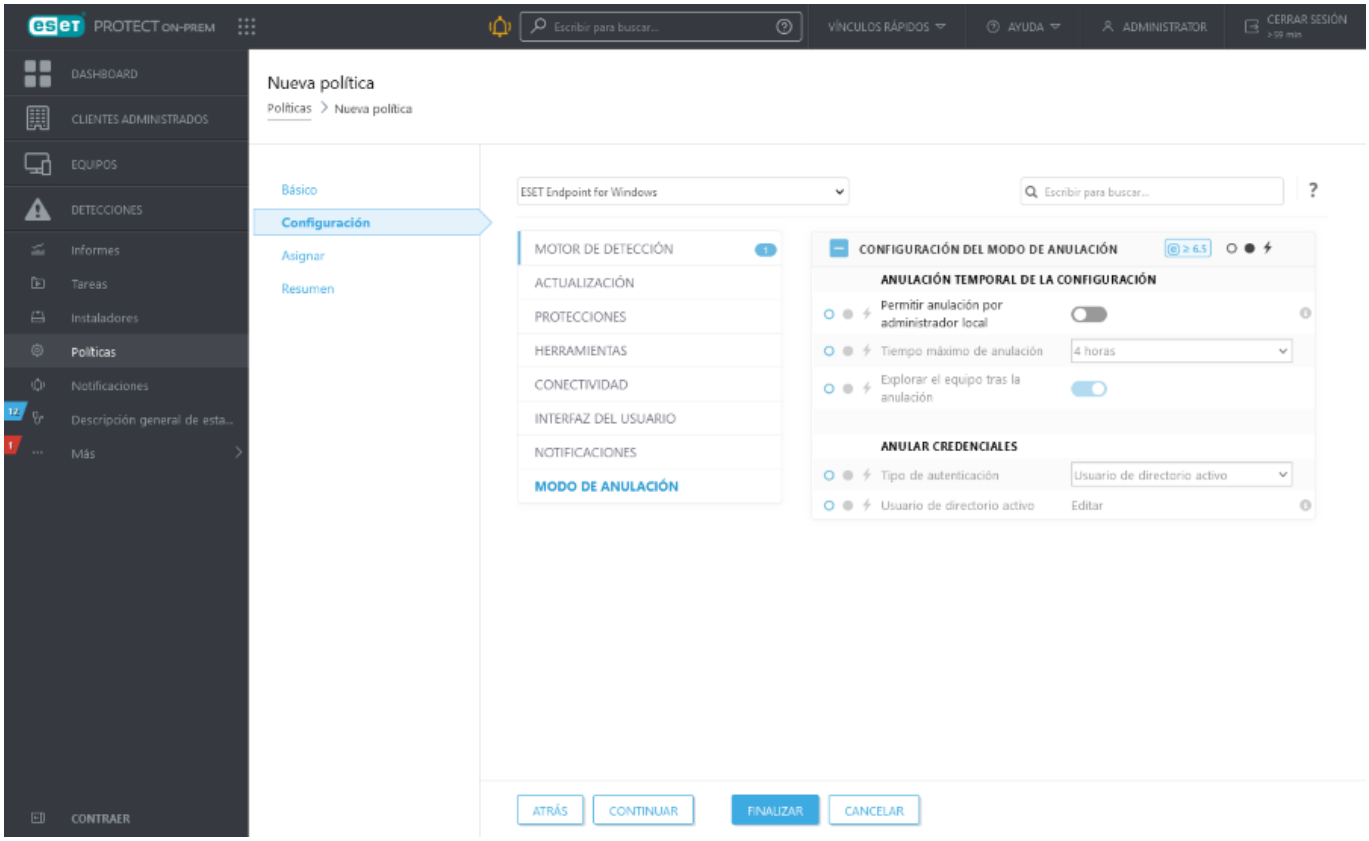
Los usuarios con los productos ESET para Endpoint para Windows instalado en sus equipos pueden utilizar la característica de anulación. Puede activar el modo de anulación solo de forma remota desde la consola web ESET PROTECT. El modo anulación le permite a los usuarios en el nivel cliente-computadora cambiar la configuración en el producto ESET instalado, incluso si hubiera una política aplicada sobre esta configuración. El modo Anulación puede habilitarse para usuarios AD o se puede proteger con contraseña. La función no puede habilitarse por más de cuatro horas de una sola vez.

Limitaciones del modo de anulación

- El modo Anulación no puede detenerse desde la consola web ESET PROTECT una vez que se habilita. La Anulación se deshabilita únicamente una vez que el período de anulación expire o una vez que el mismo cliente la apague.
- El usuario que usa el modo de anulación necesita tener también derechos de administración de Windows. De lo contrario, el usuario no podrá guardar los cambios realizados en la configuración del producto de ESET.
- La autenticación de grupo de Active Directory es compatible con los productos administrados seleccionados:
  - ESET Endpoint Security
  - ESET Server Security para Microsoft Windows Server (anteriormente ESET File Security para Microsoft Windows Server)
  - ESET Mail Security para IBM Domino
  - ESET Mail Security para Microsoft Exchange Server

Para establecer el **modo anulación**:

1. Navegue hasta **Políticas** > **Nueva política**.
2. En la sección **Básico**, ingrese un **Nombre** y una **Descripción** para esta política.
3. En la sección **Configuración**, seleccione **ESET Endpoint para Windows**.
4. Haga clic en **Modo anulación** y configure reglas para el modo anulación.
5. En la sección **Asignar**, seleccione el equipo o el grupo de equipos en los que se aplicará esta política.
6. Repase la configuración en el sección **Resumen** y haga clic en **Finalizar** para aplicar la política.



Si *John* tiene un problema con la configuración de su endpoint porque bloquea alguna funcionalidad importante o el acceso a la web en su máquina, el Administrador puede permitir que *John* anule la política existente de su endpoint y que corrija los ajustes manualmente en su máquina. Luego, es posible que ESET PROTECT On-Prem solicite estos ajustes para que el Administrador pueda crear una nueva política de ellos. Para hacerlo, siga los siguientes pasos:

1.Navegue hasta **Políticas** > **Nueva política**.

2.Complete los campos **Nombre** y **Descripción**. En la sección **Configuración**, seleccione **ESET Endpoint para Windows**.

3.Haga clic en **Modo anulación**, habilite el modo anulación durante una hora y seleccione *John* como usuario AD.

4.Asigne la política a la *computadora de John* y haga clic en **Finalizar** para guardar la política.

5.*John* tiene que habilitar el **Modo anulación** en este endpoint de ESET y cambie los ajustes manualmente en su máquina.

6.En la consola web ESET PROTECT, navegue a **Equipos**, seleccione el *equipo de John* y haga clic en **Mostrar detalles**.

7.En la sección **Configuración**, haga clic en **Solicitar configuración** para programar una tarea de cliente para obtener la configuración de cliente ASAP.

8.Tras un corto período, aparecerá la nueva configuración. Haga clic en el producto de los ajustes que desea guardar y luego haga clic en **Abrir configuración**.

9.Puede repasar los ajustes y luego hacer clic en **Convertir a política**.

10. Complete los campos **Nombre** y **Descripción**.

11. En la sección **Configuración**, usted puede modificar los ajustes, de ser necesario.

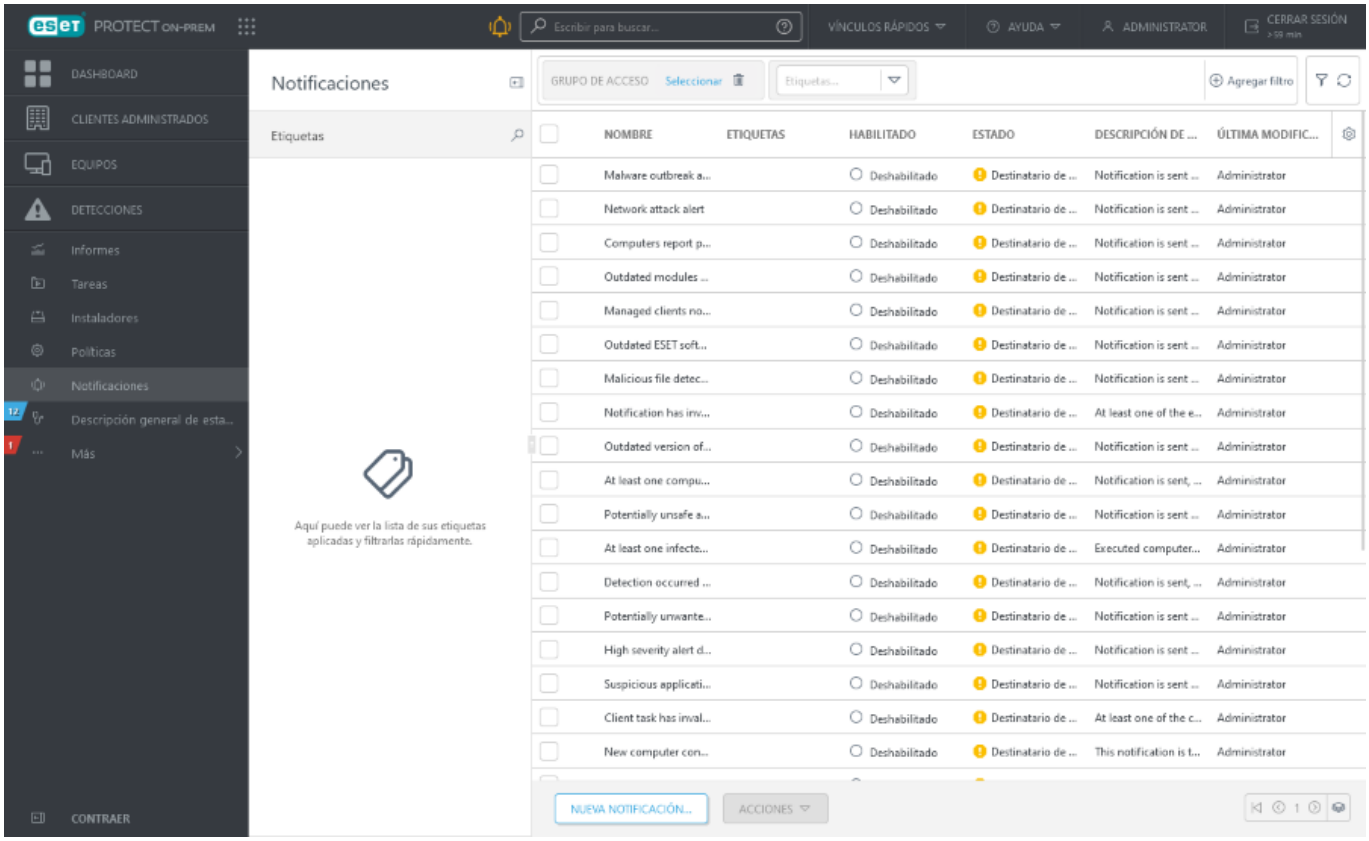
12. En la sección **Asignar**, usted puede asignar esta política para la *computadora de John* (u otras).

13. Haga clic en **Finalizar** para guardar los ajustes.

14. No olvide quitar la política de anulación una vez que ya no la necesite.

Notificaciones

Las notificaciones son esenciales para hacer un seguimiento del estado general de su red. Cuando se produzca un nuevo evento (según la configuración de notificaciones), se lo notificará mediante un método definido (ya sea una captura SNMP, un mensaje por correo electrónico o un envío al servidor syslog), y usted podrá responder como corresponda. Puede configurar notificaciones automáticas basadas en eventos específicos, como detecciones, puntos de conexión desactualizados y más. Para obtener más información acerca de una notificación específica y su desencadenador, consulte la descripción de notificaciones.



Para crear una nueva notificación, haga clic en **Nueva notificación** en la parte inferior de la página.

Seleccione una notificación existente y haga clic en **Acciones** para administrar la notificación.

Para agregar criterios de filtrado, haga clic en **Agregar filtro** y seleccione los elementos de la lista. Escriba las cadenas de búsqueda o seleccione los elementos del menú desplegable en los campos de filtrado y pulse **Intro**. Los filtros activos están resaltados en azul.

Notificaciones, usuarios y permisos

El uso de las Notificaciones se encuentra restringido por los permisos del usuario actual. Cada vez que se ejecuta la notificación, existe un usuario ejecutor cuyos permisos se tienen en cuenta. El usuario ejecutar es siempre el último que editó la lista de notificaciones. Un usuario solo puede ver las notificaciones dentro de un grupo para el que tiene permisos de **Lectura**.

Para que una notificación funcione bien, es necesario que el usuario ejecutor cuente con los permisos suficientes para todos los objetos a los que se refiere (dispositivos, grupos, plantillas). Generalmente, se necesitan permisos de **Lectura** y **Uso**. Si el usuario no cuenta con estos permisos, o si los pierde, la notificación fallará. Las notificaciones fallidas se resaltan y desencadenarán un correo electrónico para informar al usuario.

Crear notificación: el usuario debe contar con permisos de **Escritura** para las notificaciones en su grupo hogar Una nueva notificación se crea en el grupo hogar del usuario.

Modificar notificación: el usuario debe contar con permisos de **Escritura** para las notificaciones en un grupo donde se ubica la notificación

Quitar notificación: el usuario debe contar con permisos de **Escritura** para las notificaciones en un grupo donde se ubica la notificación

John, cuyo **Grupo hogar** es *Grupo de John*, desea eliminar (o modificar) la *Notificación 1*. La notificación fue creada originalmente por *Larry*, por lo que automáticamente se encuentra en el grupo hogar de Larry, *Grupo de Larry*. Se deben cumplir las siguientes condiciones para que *John* pueda eliminar (o modificar) la *Notificación 1* :

- *John* debe tener un conjunto de permisos con permisos de **Escritura** para **notificaciones**
- El conjunto de permisos debe contener al *Grupo de Larry* en **Grupos estáticos**

Grupo de pertenencia: el grupo de pertenencia se detecta automáticamente según el conjunto de permisos asignado del usuario activo en ese momento.

Situación de ejemplo:
La cuenta de usuario activa actualmente tiene el derecho de acceso de **Escritura** para la **tarea del cliente Instalación del software** y el **grupo de pertenencia** de la cuenta de usuario es "Department_1". Cuando el usuario cree una nueva **tarea del cliente Instalación del software**, se seleccionará automáticamente "Department_1" como **grupo de pertenencia** de la tarea del cliente.

Si el grupo de pertenencia seleccionado previamente no cumple con sus expectativas, podrá seleccionar el grupo de pertenencia de forma manual.

Clonación y VDI

Existen tres notificaciones preparadas para notificar al usuario acerca de eventos relacionados con clonaciones, o el usuario puede crear una notificación nueva personalizada.

Personalización del diseño y de los filtros

Puede personalizar la vista de la pantalla de la consola web actual:

- Administre el panel lateral y la tabla principal.
- Agregar filtro y filtros preestablecidos. Puede usar etiquetas para filtrar los elementos mostrados.

Administrar notificaciones

Las notificaciones se administran en la sección **Notificaciones**. Puede realizar las siguientes acciones:

- Haga clic en **Nueva notificación** para crear una nueva notificación.
- Haga clic en una notificación existente y seleccione una acción desde el menú desplegable:

Mostrar detalles	Mostrar detalles de la notificación, incluidas la configuración y los ajustes de distribución. Haga clic en **Ver vista previa del mensaje** para ver la vista previa de la notificación.
Registro de auditoría	Ver el registro de auditoría del elemento seleccionado.
Etiquetas	Editar etiquetas (asignar, desasignar, crear, quitar).
Deshabilitar / Habilitar	Cambie el estado de una notificación. La notificación deshabilitada no se evalúa. Todas las configuraciones están configuradas como **Desactivadas** de forma predeterminada.
Editar	Configure los ajustes y la distribución de la notificación.
Duplicar	Crea una notificación duplicada en su grupo hogar.
Eliminar	Elimina la notificación.
Grupo de acceso > **Mover**	Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen derechos suficientes para el grupo de destino. Cambiar el grupo de acceso es útil cuando se resuelven problemas de acceso con otros usuarios. El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario.

Notificación nueva

Básica

Ingrese un **Nombre** y una **Descripción** para que sea más fácil filtrar su notificación entre diferentes notificaciones.

Si está editando una notificación activada y desea desactivarla, haga clic en el conmutador y su estado cambiará a **Desactivada** .

Configuración

Evento – Hay tres tipos básicos de eventos que pueden desencadenar una notificación. Cada tipo de evento proporciona opciones diferentes en la sección **Configuración**. Seleccione uno de los siguientes tipos de eventos:

- Eventos en equipos administrados o grupos
- Cambios de estado del servidor
- Cambios en el grupo dinámico

Configuración avanzada: Umbral

El límite le permite configurar reglas avanzadas que determinan cuándo se desencadena una notificación. Consulte Límites para obtener más información.

Distribución

Configure los ajustes de distribución para notificaciones. Configure su servidor SMTP, si desea enviar notificaciones por correo electrónico.

Eventos en equipos administrados o grupos

Esta opción se usa para las notificaciones que no están asociadas con un grupo dinámico, sino con eventos de sistema filtrados en el registro de eventos. Seleccione un tipo de registro con el que se basará la notificación y un operador lógico para los filtros.

Categoría: elija entre las siguientes categorías de evento:

- **Detección de firewall**
- **Detección de antivirus**
- **Exploración**
- **HIPS**
- **ESET Inspect alertas**
- **Archivo bloqueado**
- **Equipo conectado primero**
- **Identidad del equipo recuperada**
- **Pregunta de clonación del equipo creada**
- **Se encontró un nuevo cliente de MSP**

De acuerdo con la categoría seleccionada, hay una lista de eventos disponibles en **Configuración** > **Filtrar por**. Los valores en filtros se comparan directamente con los eventos enviados por los clientes. No hay una lista definitiva de valores disponibles.

Grupos estáticos supervisados: haga clic en **Seleccionar** o en **Crear nuevo grupo** y seleccione los grupos estáticos para limitar los dispositivos supervisados de los que desea recibir notificaciones. Si no selecciona ningún grupo estático, recibirá notificaciones para todos los dispositivos a los que tenga acceso.

Omitir dispositivos silenciados: si marca esta casilla de verificación, no recibirá notificaciones de equipos sin sonido (los equipos sin sonido se excluirán de las notificaciones).

Configuración

En **Configuración**, seleccione un **Operador** y los valores por el filtro (**Filtrar por**). Solo se puede seleccionar un

operador y se evaluarán todos los valores juntos usando ese operador. Haga clic en **Agregar filtro** para agregar un nuevo valor al filtro.

El contenido predeterminado del mensaje tiene un propósito informativo; no se puede personalizar. Puede personalizar el mensaje entregado a través de una notificación en la sección Distribución.

Cambios de estado del servidor

Esta opción le notifica los cambios de estado del objeto. El intervalo de notificación depende de la **categoría** seleccionada. Puede seleccionar una de sus configuraciones existentes o configurar sus propios parámetros.

Cargar las configuraciones preestablecidas: Haga clic en Seleccionar para escoger una de las configuraciones preexistentes, o déjela en blanco. Haga clic en Borrar para borrar la sección Configuraciones.

Categoría - Seleccione una categoría de objetos. Según la categoría seleccionada, los objetos se muestran en la sección de Configuraciones a continuación.

Grupos estáticos supervisados: en las categorías en las que la notificación se refiere a un cliente (Clientes administrados, Software instalado), puede hacer clic en **Seleccionar** o **Crear nuevo grupo** y seleccionar los grupos estáticos para limitar los dispositivos supervisados sobre los que desea recibir una notificación. Si no selecciona ningún grupo estático, recibirá notificaciones para todos los dispositivos a los que tenga acceso.

Configuración

Seleccione un **Operador** y los valores para el filtro (**Filtrar por**). Solo se puede seleccionar un operador y se evaluarán todos los valores juntos usando ese operador. Haga clic en **Agregar filtro** para agregar un nuevo valor para el filtro. Si selecciona más filtros, se evalúa la ejecución de una notificación con *Y* operador (la notificación únicamente se envía si todos los campos del filtro se evalúan como *verdadero*).

> Algunos filtros pueden causar que la notificación se presente con mucha frecuencia. Se recomienda usar Limitación para agregar las notificaciones.

Lista de valores de filtros disponibles

Categoría	Valor	Comentario
Certificados CA	Intervalo de tiempo relativo (Autoridad certificadora válida hasta, Certificado de pares válido hasta)	Seleccione un intervalo de tiempo relativo.
Certificados de pares	Intervalo de tiempo relativo (Autoridad certificadora válida hasta, Certificado de pares válido hasta)	Seleccione un intervalo de tiempo relativo.
Clientes administrados	Intervalo de tiempo relativo (última onexión)	Seleccione un intervalo de tiempo que debe supervisarse para la **Última conexión**.
	Porcentaje de equipos sin conexión	Un valor entre 0 y 100. Solo puede usarse en combinación con el filtro de **Intervalo de tiempo relativo**.
Licencias	Intervalo relativo de tiempo (fecha de vencimiento de la licencia)	Seleccione un intervalo de tiempo que monitorear para la expiración de una licencia.
	Porcentaje de uso de licencia	Un valor entre 0 y 100 calculado según las **Unidades** de licencia que se usaron para la activación. En el caso de los productos ESET Mail Security, el uso de licencias se calcula en función de las **Subunidades** que se usan para la activación.
	Tipo de usuario de licencia	Seleccione **Empresa**, **Cliente MSP** o **Sitio**.
Tareas de clientes	Tarea	Seleccione tareas para la validez del filtro. Si no selecciona nada, se considera todas.
	La tarea es válida	Seleccione **Si** / **No**. Si selecciona **No**, la notificación se desencadena cuando por lo menos una tarea de la selección (filtro **Tarea**) no sea válida.
Tareas del servidor	Cuenta (falló)	Número de fallas de tareas seleccionadas.
	Último estado	Último estado informado de tareas seleccionadas.
	Tarea	Seleccionar tareas para este filtro. Si no selecciona nada, se considera todas.
	La tarea es válida	Seleccione **Si** / **No**. Si selecciona **No**, la notificación se desencadena cuando por lo menos una tarea de la selección (filtro **Tarea**) no sea válida.
	Intervalo de tiempo relativo (hora de ocurrencia)	Seleccione un intervalo de tiempo para monitorear.
Software instalado	Nombre de la aplicación	Nombre completo de la aplicación. Si se monitorea más aplicaciones, use el operador **en** y agregue más campos.
	Proveedor de la aplicación	Nombre completo del proveedor. Si se monitorea más proveedores, use el operador **en** y agregue más campos.
	Estado de comprobación de la versión	Si se selecciona **Versión desactualizada**, la notificación se desencadena cuando por lo menos una aplicación está desactualizada.
Pares de red	Par	Si tiene más servidores ESET PROTECT en su red, seleccione uno de ellos.

Categoría	Valor	Comentario
	Estado del servidor	Si el servidor de ESET PROTECT está sobrecargado con registros de escritura, cambia su estado: • **Normal**: respuesta inmediata del servidor. • **Limitada**: el servidor responde al agente una vez por hora • **Sobrecargado**: el servidor no responde a los agentes
Notificaciones	Notificación	Seleccione la notificación para este filtro. Si no selecciona nada, se considera todas.
	La notificación está habilitada	Seleccione **Si** / **No**. Si selecciona **No**, la notificación se desencadena cuando por lo menos una notificación de la selección (filtro **Notificación**) esté deshabilitada.
	La notificación es válida	Seleccione **Si** / **No**. Si selecciona **No**, la notificación se desencadena cuando por lo menos una notificación de la selección (filtro **Notificación**) no sea válida.

El contenido predeterminado del mensaje tiene un propósito informativo; no se puede personalizar. Puede personalizar el mensaje entregado a través de una notificación en la sección Distribución.

Cambios en el grupo dinámico

La notificación se enviará cuando se cumpla la condición. Solo puede seleccionar una condición para monitorear para un grupo dinámico dado.

Grupo dinámico: seleccione un grupo dinámico para evaluar.

Configuración - Condiciones

Seleccione el tipo de condición que desencadenará una notificación.

- **Notificar cada vez que el grupo dinámico contiene cambios** – Habilite esta opción para recibir una notificación en caso de que se agreguen, quiten o modifiquen miembros del grupo seleccionado.

> ESET PROTECT On-Prem comprueba el estado del grupo dinámico una vez cada 20 minutos.
> Por ejemplo, si la primera comprobación ocurre a las 10:00, las demás se llevarán a cabo a las 10:20, 10:40, 11:00. Si el contenido del Grupo dinámico cambia a las 10:05, y luego regresa al estado inicial a las 10:13, durante la siguiente comprobación, realizada a las 10:20, ESET PROTECT On-Prem no reconoce el cambio previo y no notifica al respecto.

- **Notificar cuando el tamaño del grupo supere un número específico**: seleccione el operador de tamaño del grupo y el umbral para la notificación:
  - **Más que**: envía una notificación cuando el tamaño del grupo es superior al límite.
  - **Más que**: envía una notificación cuando el tamaño del grupo es inferior al límite.
- **Notificar cuando el crecimiento del grupo supere una velocidad específica**: define un umbral y un periodo de tiempo que desencadenarán una notificación. Puede definir un número de clientes, o un porcentaje de clientes (miembros del grupo de dinámico). Defina el período de tiempo (en minutos, horas o días) para la comparación con el nuevo estado. Por ejemplo, hace siete días, la cantidad de clientes con productos de seguridad obsoletos era de 10 y el límite estaba definido en 20. Si la cantidad de clientes con productos de seguridad obsoletos llega a 30, se le notificará.
- **Notificar cuando el número de clientes del grupo dinámico cambie en comparación con otro grupo**: si el número de clientes de un grupo dinámico cambia de acuerdo con un grupo comparado (ya sea estático o dinámico), se enviará una notificación. Umbral - Define un umbral que activará el envío de una notificación.

> Solo puede asignar una notificación a un grupo dinámico donde tenga permisos suficientes. Para ver un grupo dinámico, debe **leer** el permiso para su grupo estático principal.

Distribución

Tiene que elegir un medio de distribución como mínimo.

Enviar captura SNMP

Envía capturas del SNMP. La captura SNMP notifica al Servidor mediante un mensaje SNMP no solicitado. Para más información, vea cómo configurar un servicio de captura SNMP.

Enviar correo electrónico

Envía un mensaje de correo electrónico basado en la configuración de su correo electrónico. De forma predeterminada, el correo electrónico de la notificación está en formato HTML y hay un logotipo de ESET PROTECT On-Prem en el encabezado. Puede elegir un logotipo personalizado y diferentes posiciones del logotipo según la configuración de personalización (**logotipo con fondo claro**).

Si está seleccionado **Enviar correo electrónico**, introduzca al menos un destino para el correo electrónico.

- **Dirección de correo electrónico**: introduzca la dirección de correo electrónico de los destinatarios de los mensajes de notificación.
- Haga clic en + agregue un nuevo campo de dirección.
- Para agregar varios usuarios a la vez, haga clic en **Más** > **Agregar usuarios** (agregar la dirección del usuario desde los Usuarios del equipo) o en **Más** > **Importar CSV** o **Pegar desde el portapapeles** (Importar una lista personalizada de las direcciones desde un archivo CSV estructurado con delimitadores).
- **Más** > **Pegar del portapapeles**: importe una lista personalizada de direcciones separadas con delimitadores personalizados. Esta característica funciona de manera similar a la importación de CSV.

Enviar Syslog

Puede usar a ESET PROTECT On-Prem para enviar notificaciones y mensajes de eventos a su servidor Syslog. Además, exportar los registros de un producto de ESET del cliente y enviarlos al servidor Syslog. **Severidad de Syslog**: elija el nivel de gravedad del menú desplegable. Las notificaciones aparecerán luego con la severidad seleccionada en el servidor Syslog.

Campos básicos en la distribución

- **Vista previa del mensaje**: una vista previa del mensaje que aparece en la notificación y contiene los ajustes configurados en formato de texto. Puede personalizar tanto el contenido como el asunto del mensaje y usar variables que se convertirán en valores reales cuando se genere la notificación. Esto es opcional, pero se recomienda filtrar mejor.
  - **Asunto**: asunto de un mensaje de notificación; haga clic en el ícono de edición para editar el contenido; un asunto preciso puede mejorar la clasificación y el filtrado del mensaje
  - **Contenido**: haga clic en el icono de edición para editar el contenido; después de editar el contenido, puede hacer clic en el icono de restablecimiento para restablecer el contenido predeterminado del

mensaje

Para **eventos o gestionar equipos o grupos**, puede agregar variables al **Asunto** y al **Contenido** para incluir información específica en la notificación. Haga clic en **Agregar variable** o comience a escribir $ para mostrar la lista de variables.

- **General**

  o**Localización**: idioma del mensaje predeterminado; el contenido del mensaje no se traduce

  o**Zona horaria**: establece la zona horaria para la variable `${timestamp}` de **Hora de ocurrencia**, que se puede usar en el mensaje personalizado.

Si el evento ocurre a las 3:00 de la hora local, la hora local es UTC+2, la zona horaria seleccionada es UTC+4, la hora indicada en la notificación sería 5:00.

Haga clic en **Finalizar** para crear uno nuevo notificación basada en la plantilla que está editando.

Cómo configurar un servicio de captura del SNMP

Para recibir mensajes SNMP correctamente, el servicio de captura de SNMP debe estar configurado. Siga los pasos de configuración que figuran a continuación según corresponda para su sistema operativo:

WINDOWS

Requisitos previos

- El servicio del **Protocolo de administración de redes simples** (SNMP) debe instalarse en el equipo en el que está instalado el servidor ESET PROTECT, así como también donde se instalará el software de captura del SNMP.
- Ambos equipos (anteriores) deben estar en la misma subred.
- El servidor del SNMP debe estar configurado en el equipo del servidor ESET PROTECT.

Configuración del servicio del SNMP (servidor ESET PROTECT)

1.PPresione tecla de Windows + R para abrir un cuadro de diálogo, escriba Services.msc en el campo **Abrir** y presione **Intro**. Busque SNMP Service.

2.Abra la pestaña **Capturas**, escriba **público** en el campo de **Nombre de comunidad** y haga clic en **Agregar a lista**.

3.Haga clic en **Agregar**, escriba el **Nombre de host y la dirección IP o IPX** del equipo en el que está instalado el software de captura del SNMP en el campo adecuado y haga clic en **Agregar**.

4.Proceda a la pestaña **Seguridad**. Haga clic en **Agregar** para mostrar la ventana de **Configuración de servicio del SNMP**. Escriba **público** en el campo **Nombre de comunidad** y haga clic en **Agregar**. Los

derechos se configurarán como **SOLO LECTURA**, esto es correcto.

5.Asegúrese de que la opción **Aceptar paquetes del SNMP de cualquier host** esté seleccionada y haga clic en **Aceptar** para confirmar. El servicio del SNMP no está configurado.

Configuración del software de captura del SNMP (Cliente)

1.Asegúrese de que el servicio del SNMP esté instalado en el equipo cliente.

2.Instale una aplicación receptora de captura.

3.Configure la aplicación receptora de capturas para recibir capturas del SNMP desde el servidor ESET PROTECT (esto puede incluir la dirección IP del servidor ESET PROTECT y la configuración del puerto).

4.Asegúrese de que el firewall en los equipos cliente permita la comunicación de red para la comunicación del SNMP establecida en el paso anterior.

5.La aplicación receptora de capturas ahora le permite recibir mensajes del servidor ESET PROTECT.

SNMP Trap no es compatible con el dispositivo virtual ESET PROTECT.

LINUX

1. Instale el paquete snmpd al ejecutar alguno de los siguientes comandos:
`apt-get install snmpd snmp`(Distribuciones Debian y Ubuntu)
`yum install net-snmp` (distribuciones Red Hat, CentOS)

2. Abra el archivo */etc/default/snmpd* y edite los siguientes atributos:

```
#SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid'
```

Agregar # deshabilitará esta línea por completo.

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid -
c /etc/snmp/snmpd.conf'
```

Agregue esta línea al archivo.

```
TRAPDRUN=yes
```

Cambie el atributo trapdrun a yes.

3. Cree una copia de seguridad del archivo snmpd.conf original. El archivo se editará más adelante.

```
mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.original
```

4. Cree un archivo snmpd.conf nuevo y agregue estas líneas:

```
rocommunity public
syslocation "Testing ESET PROTECT On-Prem"
syscontact admin@PROTECT.com
```

5. Abra el archivo */etc/snmp/snmptrapd.conf* y agregue la siguiente línea al final del archivo:

```
authCommunity log,execute,net public
```

6. Escriba el siguiente comando para iniciar los servicios de administración del SNMP y para crear un registro de las capturas entrantes:

```
/etc/init.d/snmpd restart
```

o

```
service snmpd restart
```

7. Para verificar si la captura funciona y captura los mensajes, ejecute el siguiente comando:

```
tail -f /var/log/syslog | grep -i TRAP
```

Información general de estado

El servidor ESET PROTECT realiza verificaciones de diagnósticos periódicas. Use la **Información general de estado** para ver las estadísticas de uso y el estado general de ESET PROTECT On-Prem. También puede ayudarlo con la configuración inicial de ESET PROTECT On-Prem. Haga clic en **Información general de estado** para ver la información de estado detallada de ESET PROTECT On-Prem.

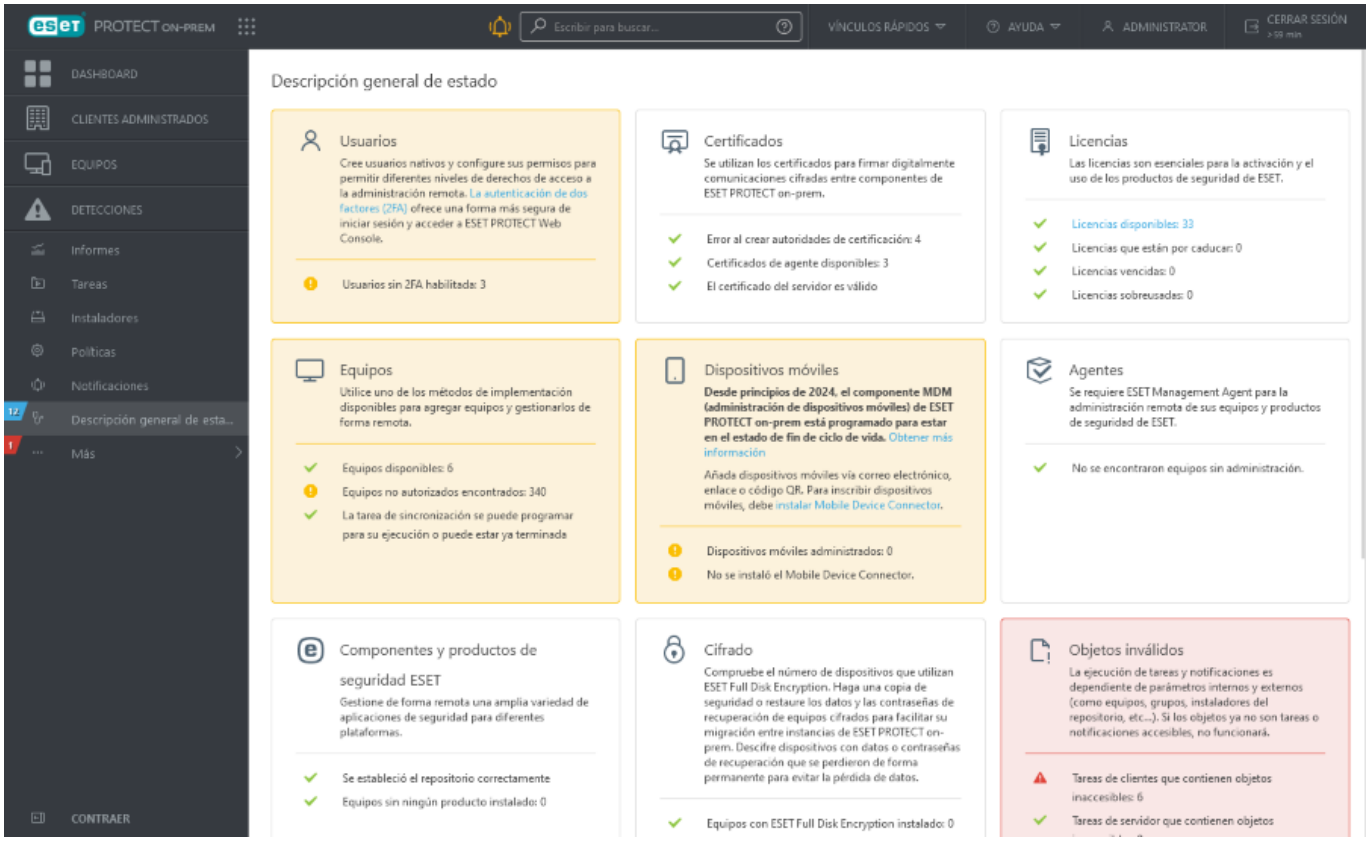
Haga clic en un mosaico de sección para mostrar una barra de tareas a la derecha con acciones. Cada mosaico de sección puede tener uno de varios colores, según el estado de gravedad de los elementos incluidos:

Color	Ícono	Significado del ícono	Descripción
Verde		Aceptar	Todos los elementos de la sección no tienen problemas.
Amarillo		Advertencia	Al menos un elemento de la sección tiene una advertencia.
Rojo		Error	Al menos un elemento de la sección tiene un error.
Gris		Contenido no disponible	El contenido no está disponible debido a derechos de acceso insuficientes del usuario de la consola web ESET PROTECT. El administrador necesita establecer permisos adicionales para el usuario o usted debe iniciar sesión como otro usuario con derechos de acceso adecuados.
Azul		Información	Existe una cuestión relacionada al equipo(s) conectado(s) (vea la descripción de la sección **Cuestiones** abajo).

La **Información general de estado** contiene las siguientes secciones:

Usuarios	Puede crear diferentes usuarios y configurar sus permisos para permitir diferentes niveles de administración en ESET PROTECT On-Prem. La cuenta predeterminada del administrador de ESET PROTECT On-Prem se creó durante la instalación. No recomendamos usar la cuenta predeterminada del Administrador de ESET PROTECT On-Prem como una cuenta de usuario normal. Haga clic en **Ver usuarios**, cree una nueva cuenta de usuario nativo con autenticación de dos factores y úsela como la cuenta predeterminada en ESET PROTECT On-Prem.
Certificados	Si desea usar certificados diferentes a los predeterminados proporcionados por ESET PROTECT On-Prem, puede crear las Autoridades de certificación y los Certificados de pares para componentes individuales de ESET PROTECT que permitan la comunicación con el servidor ESET PROTECT.
Licencias	ESET PROTECT On-Prem usa el sistema de generación de licencias de ESET. Seleccione el método que desea usar para agregar la(s) licencia(s) que se usará(n) al activar los componentes de ESET PROTECT y productos de seguridad ESET en equipos clientes.

Equipos	• **Agregar equipo**: agregue equipos en su red a la estructura de ESET PROTECT On-Prem. Puede Agregar equipos y dispositivos móviles en forma manual o importar una lista de dispositivos. • **Agregar equipos Rogue**: importa equipos detectados automáticamente usando el ESET RD Sensor. • **Nueva tarea de sincronización**: ejecuta la Sincronización de grupos estáticos con Active Directory, LDAP, VMware, etc.
Dispositivos móviles	⚠ El componente de conector/administración de dispositivos móviles (MDM/MDC) de ESET PROTECT (solo on-prem) llega al fin de ciclo de vida en enero de 2024. Leer más. Le recomendamos migrar a Cloud MDM. • **Descargar**: si MDC no está instalado, puede descargar el instalador de Mobile Device Connector desde la web de ESET. • **Agregar dispositivos móviles**: inscriba dispositivos móviles por correo electrónico, enlace o código QR o como propietario del dispositivo.
Agentes	• **Nueva política**: crea una nueva política para que el agente ESET Management cambie el intervalo de conexión. • **Instalar agente**: hay varias maneras de instalar el agente ESET Management en los equipos cliente en su red.
Componentes y productos de seguridad ESET	• **Nueva política**: puede crear una nueva política para cambiar la configuración del producto de seguridad ESET instalado en los equipos cliente. • **Configurar repositorio**: cambia la Configuración del ESET PROTECT servidor. • **Instalar software**: con el agente ESET Management implementado, puede instalar el software directamente desde el repositorio ESET o especificar la ubicación de un paquete de instalación (URL o una carpeta compartida).
Cifrado	Si administra dispositivos cifrados con ESET Full Disk Encryption, utilice estas opciones para evitar perder los datos de recuperación: • **Exportar**: exporta los datos de recuperación de ESET Full Disk Encryption actuales antes de migrar los equipos administrados cifrados. • **Importar**: importa los datos de recuperación de ESET Full Disk Encryption tras migrar los equipos administrados cifrados a una nueva instancia de ESET PROTECT On-Prem.
Objetos inválidos	Contiene la lista de tareas del cliente y el servidor, desencadenadores, notificaciones o instaladores que hacen referencia a objetos no válidos o inalcanzables. Haga clic en cualquiera de los campos de resultado para ver un menú con la lista de objetos seleccionada.
Servicios externos	ESET PROTECT On-Prem puede configurarse para conectarse a servicios externos para proporcionar funcionalidad completa. • **Configurar repositorio**: el repositorio contiene archivos de instalación para otros productos de seguridad ESET que puede instalar mediante la tarea de instalación. El repositorio se configura en Más > Ajustes. Si fuera necesario, puede crear un repositorio fuera de línea. • **Configurar actualizaciones**: las actualizaciones son necesarias para que ESET PROTECT On-Prem se mantenga actualizado. Las actualizaciones están disponibles solo si ESET PROTECT On-Prem importó la licencia de un producto comercial que no expiró. Puede cambiar la configuración de actualización en **Más** > Ajustes. • **Configurar SMTP**: configura ESET PROTECT On-Prem para usar su servidor SMTP existente que permite enviar mensajes de correo electrónico, por ejemplo, Notificaciones, Mensajes de correo electrónico de inscripción de dispositivos móviles, Informes, etc.
Cuestiones	Cuando se detecta un dispositivo clonado o cambio de hardware en un dispositivo cliente, se lista una cuestión. Lea más sobre resolver equipos clonados.
Estado de MSP	Si importa una cuenta MSP, hay un mosaico con los estados de MSP disponibles.



Más

La sección **Más** es el componente de configuración avanzada de ESET PROTECT On-Prem. Esta sección contiene herramientas que el administrador puede usar para administrar las soluciones de seguridad del cliente, así como la Configuración ESET PROTECT On-Prem. Puede usar estas herramientas para configurar su entorno de red, de tal manera que no requiera mucho mantenimiento.

La sección **Más** contiene los siguientes elementos:

Detecciones oArchivos enviados oExclusión oCuarentena
Equipos oUsuarios de equipos oPlantillas de grupos dinámicos
Licencias oAdministración de licencias
Derechos de acceso oUsuarios oConjuntos de permisos
Certificados oCertificados de pares oAutoridades de certificación
Auditoría de actividad oRegistro de auditoría

Admin
o[Configuración]

Archivos enviados

ESET LiveGuard Advanced es un servicio que provee protección avanzada de detecciones nunca antes vistas. El usuario de ESET PROTECT On-Prem puede enviar archivos para analizar como malware en un ambiente en la nube y recibir un informe acerca del comportamiento de la muestra. Consulte la Guía para el usuario de ESET LiveGuard Advanced para instrucciones paso a paso. Puede enviar un archivo de forma remota directamente desde la consola web de ESET PROTECT bajo **Detecciones** > haga clic en un elemento de la categoría > **Archivos bloqueados** > **Enviar el archivo a ESET LiveGuard**.

La ventana **Archivos enviados** provee una lista de todos los archivos enviados a los servidores de ESET. Esto incluye los archivos que se envían en forma automática a ESET LiveGrid® desde equipos cliente (en caso de que ESET LiveGrid® esté habilitado en su producto de seguridad ESET) y los archivos que se envían a ESET LiveGuard Advanced en forma manual desde la consola web de ESET PROTECT.

Ventana archivos enviados

Puede ver la lista de archivos enviados y la información relacionada con esos archivos, como el usuario que envió el archivo y la fecha de envío. Haga clic en un archivo enviado y seleccione una acción desde el menú desplegable:

Mostrar detalles	Haga clic para ver la pestaña **último envío**.
Ver comportamiento	Ver el informe del análisis de comportamiento para una muestra dada. Esta opción solo está disponible para los archivos enviados a ESET LiveGuard Advanced.
Exportar informe	Descargue el informe de análisis de comportamiento para una muestra determinada. Esta opción solo está disponible para los archivos enviados a ESET LiveGuard Advanced.
Crear exclusión	Seleccione uno o más archivos y haga clic en **Crear exclusión** para agregar una exclusión de detección para los archivos seleccionados en una política existente.

Ventana de detalles del archivo

La ventana de detalles del archivo contiene una lista de detalles del archivo para el archivo seleccionado. Si se envía un archivo varias veces, se muestra los detalles del último envío.

Estado	Resultado del análisis de malware. **Desconocido**: el archivo no fue analizado. **Desinfectar**: ninguno de los motores de detección evaluó el archivo como malware. **Sospechoso**, **Altamente sospechoso**: el archivo muestra un comportamiento sospechoso pero puede no ser malware. **Malicioso**: el archivo muestra un comportamiento peligroso.
Estado	Estado del análisis. El estado **Reanalizando** significa que el resultado está disponible, pero puede cambiar con más análisis.
Último procesamiento en	Un archivo puede enviarse para análisis varias veces, desde más equipos. Esta es la hora del último análisis.

Enviado en	La hora del envío.
Comportamientos	Haga clic en Ver comportamiento para ver el análisis o en ESET LiveGuard Advanced **Exportar informe** para descargar el informe. Esto solo es válido si el equipo que envió el archivo tiene una licencia ESET LiveGuard Advanced activa.
Equipo	El nombre del equipo desde el que se envió en archivo.
Usuario	Usuario del equipo que envió el archivo.
Motivo	El motivo por el que se envió el archivo.
Enviado a	Parte de la nube de ESET que recibió el archivo. No todos los archivos enviados se analizan en busca de malware.
Hash	Hash SHA 1 del archivo enviado.
Tamaño	Tamaño del archivo enviado.
Categoría	Categoría del archivo. Es posible que la categoría no siga la extensión del archivo.

Para obtener más información acerca de los informes de comportamiento de ESET LiveGuard Advanced, ver la Documentación.

Personalización del diseño y de los filtros

Puede personalizar la vista de la pantalla de la consola web actual:

- Administre el panel lateral y la tabla principal.
- Agregar filtro y filtros preestablecidos. Puede usar etiquetas para filtrar los elementos mostrados.

Exclusión

En esta sección, puede ver una lista de todas las exclusiones creadas para detecciones de reglas IDS de **Antivirus** y **Firewall**. Esta nueva sección incluye todas las exclusiones, incrementa su visibilidad y simplifica su administración.

Haga clic en una exclusión o seleccione más exclusiones, y haga clic en el botón **Detección** para administrar las exclusiones:

- **Cambiar asignación** : cambia los equipos de destino en los que se aplicará la exclusión.
- **Mostrar equipos afectados**: muestra los equipos con exclusión aplicada.
- **Registro de auditoría**: muestre el Registro de auditoría para la exclusión seleccionada.
- **Quitar**: quita la exclusión.
- **Grupo de acceso** > **Mover** – Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen derechos suficientes para el grupo de destino. Cambiar el grupo de acceso es útil cuando se resuelven problemas de acceso con otros usuarios. El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario.

Si la acción de detección o firewall excluida vuelve a aparecer en los equipos administrados, la columna **Recuento de coincidencias** muestra la cantidad de veces que se aplicó la exclusión.

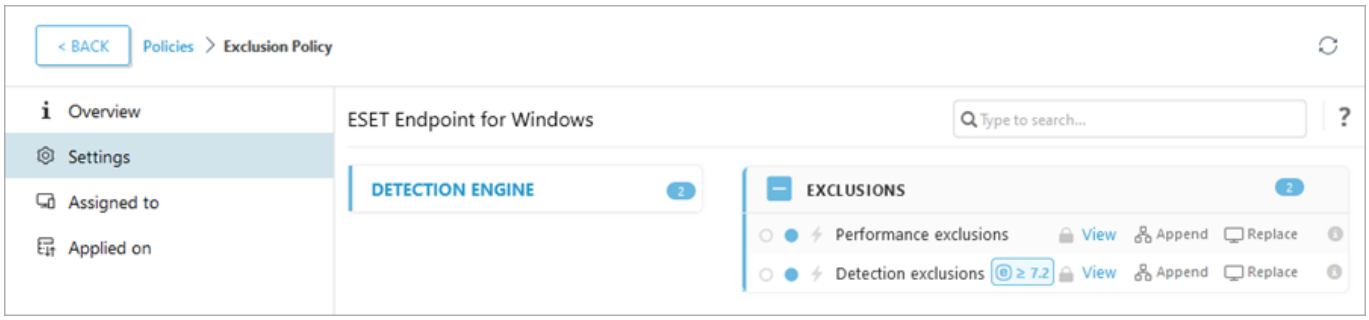
Migrar exclusiones desde una política

En ESET PROTECT On-Prem, no puede crear exclusiones de detección de antivirus por medio de una política. En caso de que sus políticas anteriormente contuviesen exclusiones, siga los pasos que se mencionan abajo para migrar las exclusiones de las políticas a la lista **Exclusiones** en ESET PROTECT On-Prem:

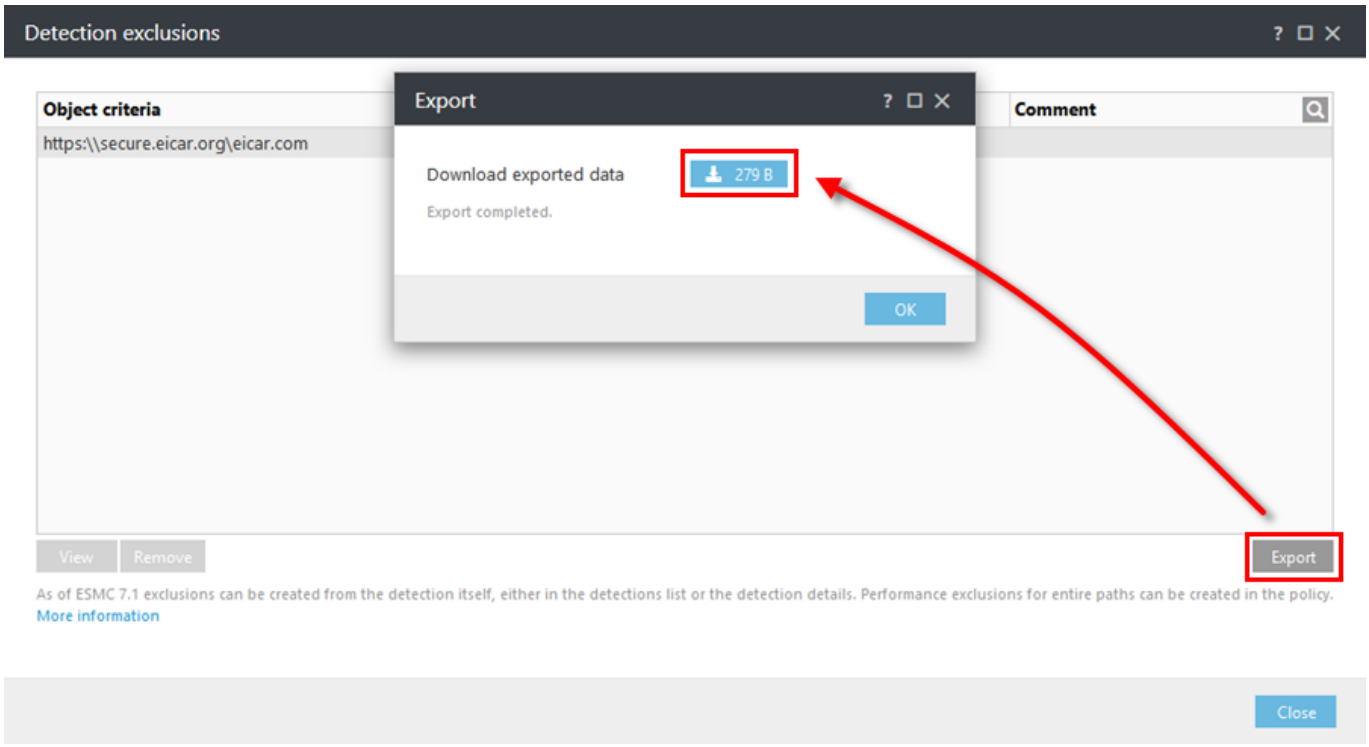
1. Vaya a **Políticas** y haga clic en la política que contenga las exclusiones, y seleccione **Mostrar detalles**.

2. Haga clic en **Configuración** > **Motor de detección**.

3. Haga clic en **Ver** junto a **Exclusiones de la detección**.

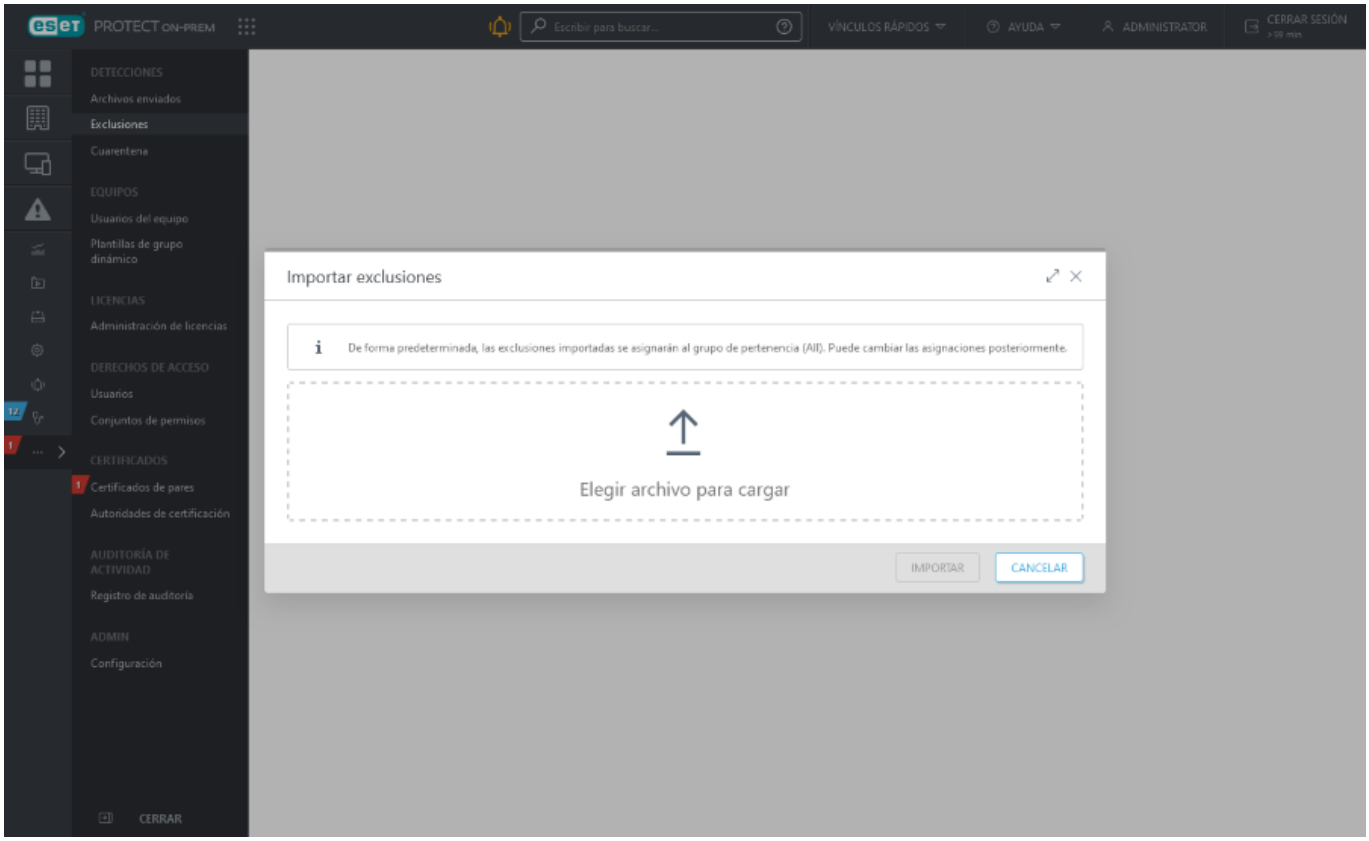


4. Haga clic en el botón **Exportar** y, luego, en el botón junto a **Descargar datos exportados**, y guarde el archivo *export.txt*. Haga clic en **OK**.



5. En la consola web de ESET PROTECT, vaya a **Más** > **Exclusiones**.

6. Haga clic en el botón **Importar** para importar exclusiones de detección de un archivo. Haga clic en **Elegir archivo para cargar** y vaya al archivo *export.txt*, o bien, arrastre y suelte el archivo.



7. Haga clic en el botón **Importar** para importar las exclusiones de detección. Las exclusiones de detección importadas se mostrarán en la lista de exclusiones.

Limitaciones de la asignación de exclusiones

- No se conservan las asignaciones de la exclusión original. Las exclusiones de detección importadas se asignan de manera predeterminada a los equipos de su grupo hogar. Para cambiar la asignación de la exclusión, haga clic en la exclusión y seleccione **Cambiar asignación**.
- Puede asignar exclusiones (para detecciones de **Antivirus** y reglas IDS del **Firewall**) únicamente a equipos con productos de seguridad ESET compatibles instalados. No se aplicarán las exclusiones a productos de seguridad ESET no compatibles y se procederá a ignorarlas.

Personalización del diseño y de los filtros

Puede personalizar la vista de la pantalla de la consola web actual:

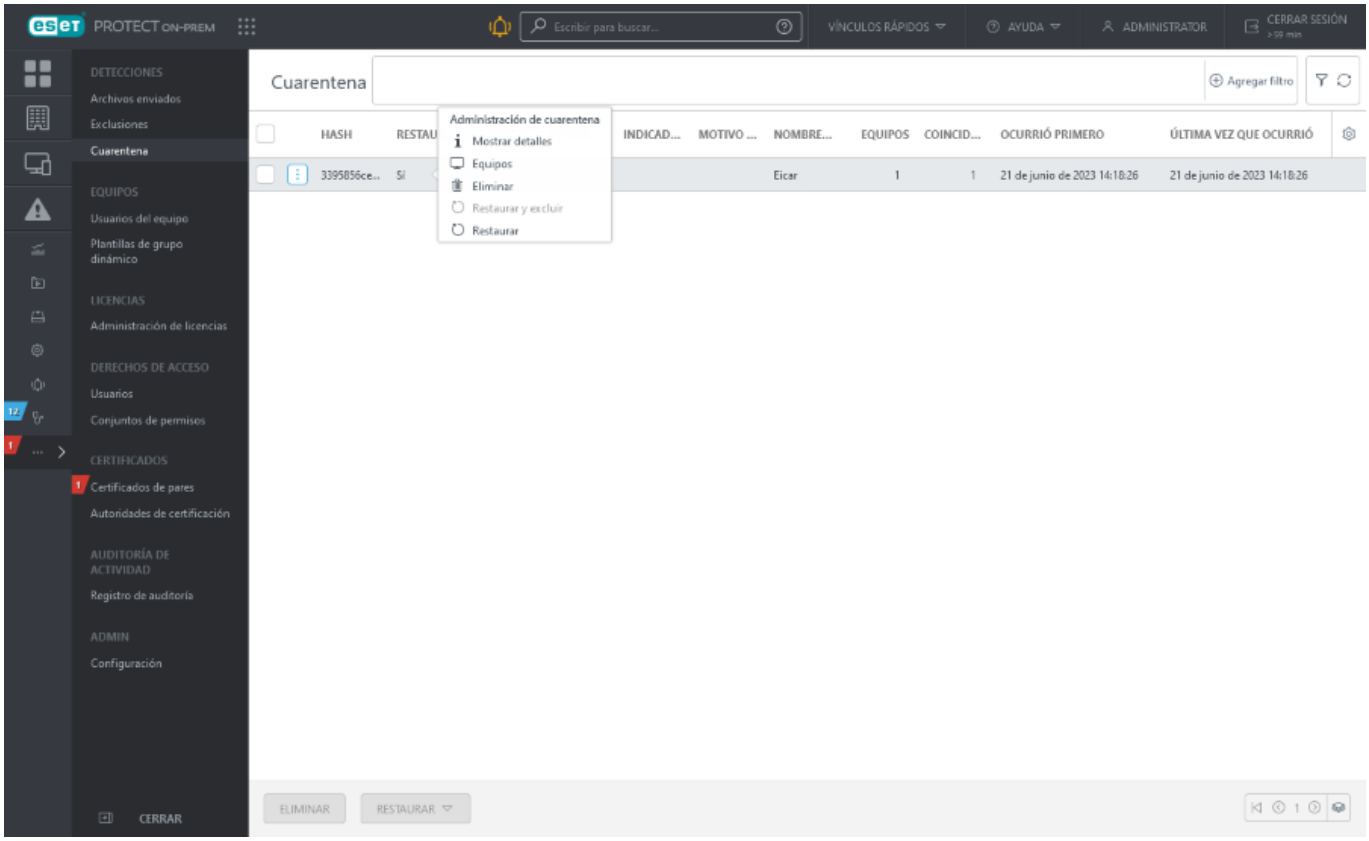
- Administre el panel lateral y la tabla principal.
- Agregar filtro y filtros preestablecidos. Puede usar etiquetas para filtrar los elementos mostrados.

Cuarentena

Esta sección muestra todos los archivos puestos en cuarentena en dispositivos del cliente. Los archivos deben ponerse en cuarentena cuando no se pueden limpiar, cuando no es seguro o recomendable eliminarlos o en caso de que un producto ESET los esté detectado erróneamente.

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

- Detecciones que no pueden eliminarse
- Detecciones que son sospechosas por su comportamiento, pero no se detectan como malware, por ejemplo, las PUA.



Puede **eliminar** el archivo en cuarentena o **restaurarlo** a su ubicación anterior. Puede utilizar **Restaurar y excluir** el archivo en cuarentena para evitar que el producto de ESET vuelva a informar el archivo.

Puede usar varios filtros para filtrar la lista de archivos en cuarentena.

Hay dos formas de ingresar a **cuarentena**:

1. **Más** > **Cuarentena**.

2. **Detalles del equipo** > **Detecciones y cuarentena** > **Pestaña cuarentena**.

Si hace clic en un elemento en la sección **Cuarentena** abrirá el menú **Administración de cuarentena**.

Mostrar detalles: muestra el dispositivo fuente, nombre y tipo de detección, nombre de objeto con ruta completa, hash, tamaño, etc.

Equipos: abre la sección **Equipos** con dispositivo filtrados conectados al archivo en cuarentena.

Eliminar: elimina el archivo de la cuarentena y el dispositivo afectado.

Restaurar: restaura el archivo a su ubicación original.

Restaurar y excluir: restaura el archivo a su ubicación original y excluirlo de los análisis.

Cargar: abre la tarea cargar archivo en cuarentena. Esta acción se encuentra disponible luego de hacer clic en **Mostrar detalles**.

> La función **Cargar** se recomienda solo para usuarios experimentados. Si desea investigar más el archivo en cuarentena, puede **Cargarlo** al directorio compartido.

Personalización del diseño y de los filtros

Puede personalizar la vista de la pantalla de la consola web actual:

- Administre el panel lateral y la tabla principal.
- Agregar filtro y filtros preestablecidos. Puede usar etiquetas para filtrar los elementos mostrados.

Usuarios de equipos

La sección Usuarios de equipos le permite administrar usuarios y grupos de usuarios. Puede emparejar un usuario con un dispositivo para sincronizar algunas configuraciones específicas de este. Se recomienda sincronizar primero los usuarios con Active Directory. Una vez creado un nuevo equipo, puede emparejar el equipo con un usuario específico. Luego, podrá buscar al usuario para ver los detalles de los equipos que se le asignaron y su actividad.

También puede administrar Usuarios y Grupos de usuarios para lograr la Administración de dispositivos móviles iOS mediante el uso de políticas asignadas a dispositivos iOS. Podrá modificar o añadir Atributos personalizados a los usuarios.

> Los **Usuarios del equipo** son diferentes a los usuarios de la Consola web de **ESET PROTECT**. Para administrar usuarios de la Consola web de ESET PROTECT y conjuntos de permisos, vaya a **Más** > **Usuarios**..

- Los usuarios resaltados no tienen ningún dispositivo asignado. Haga clic en el usuario, seleccione Editar y haga clic en **Equipos asignados** para ver los detalles del usuario. Haga clic en **Agregar equipos** para asignar dispositivos a este usuario.

- También puede agregar o eliminar **Usuarios asignados** desde Detalles de equipos. Cuando esté en **Equipos**, seleccione un dispositivo y haga clic en **Mostrar detalles**. Es posible asignar al usuario a más de un dispositivo. También puede usar **Asignar usuario** para asignar un usuario directamente al dispositivo seleccionado. Si hay un dispositivo asignado a un usuario, puede hacer clic en el nombre del dispositivo para ver los detalles sobre ese dispositivo.

- Puede arrastrar y soltar usuarios y grupos de usuarios. Seleccione el usuario (o grupo), mantenga presionado el botón del mouse y muévalo a otro grupo.

Acciones de la administración de usuarios.

Seleccione un usuario para abrir un menú desplegable donde pueda ejecutar acciones. Consulte la Leyenda del icono para obtener detalles de las acciones.

Mostrar detalles: el menú muestra información como la **dirección de correo electrónico**, la **oficina o ubicación**, y los **equipos asignados**. El usuario puede tener más de un dispositivo asignado. Podrá cambiar el **Nombre de usuario**, la **Descripción** o el **Grupo principal**. Puede usar los **atributos personalizados** al crear políticas de administración de dispositivos móviles para iOS.

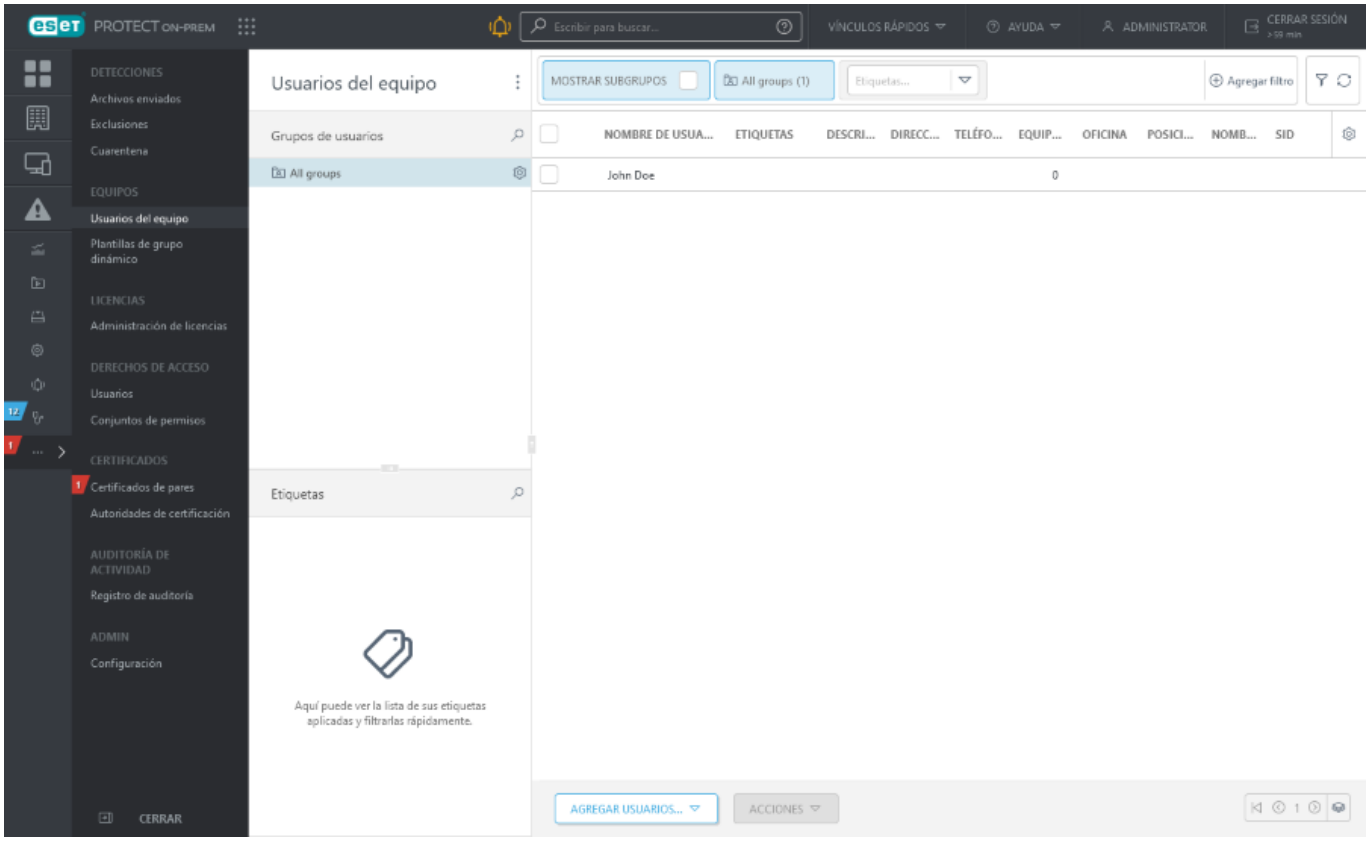
Personalización del diseño y de los filtros

Puede personalizar la vista de la pantalla de la consola web actual:

- Administre el panel lateral y la tabla principal.
- Agregar filtro y filtros preestablecidos. Puede usar etiquetas para filtrar los elementos mostrados.

Agregar nuevos usuarios

1. Haga clic en **Usuarios de equipos** > **Agregar usuarios** para agregar usuarios. Use esta opción para agregar usuarios que no se encontraron o que no se agregaron automáticamente durante la sincronización de usuarios.



2. Ingrese el nombre del usuario que desea agregar en el campo **Nombre de usuario**. Haga clic en + **Agregar** para agregar usuarios adicionales. Si desea agregar múltiples usuarios a la vez, haga clic en Importar CSVpara cargar un archivo *.csv* que contiene un listado de usuarios a agregar. Haga clic en **Copiar y pegar** para importar

una lista personalizada de direcciones separadas con delimitadores personalizados (esta característica funciona de manera similar a una importación CSV). Opcionalmente, puede ingresar una **Descripción** de los usuarios para una identificación más fácil.

3. Puede seleccionar un **Grupo principal** existente, o bien, crear uno nuevo.

4. Haga clic en **Seleccionar etiquetas** para asignar etiquetas.

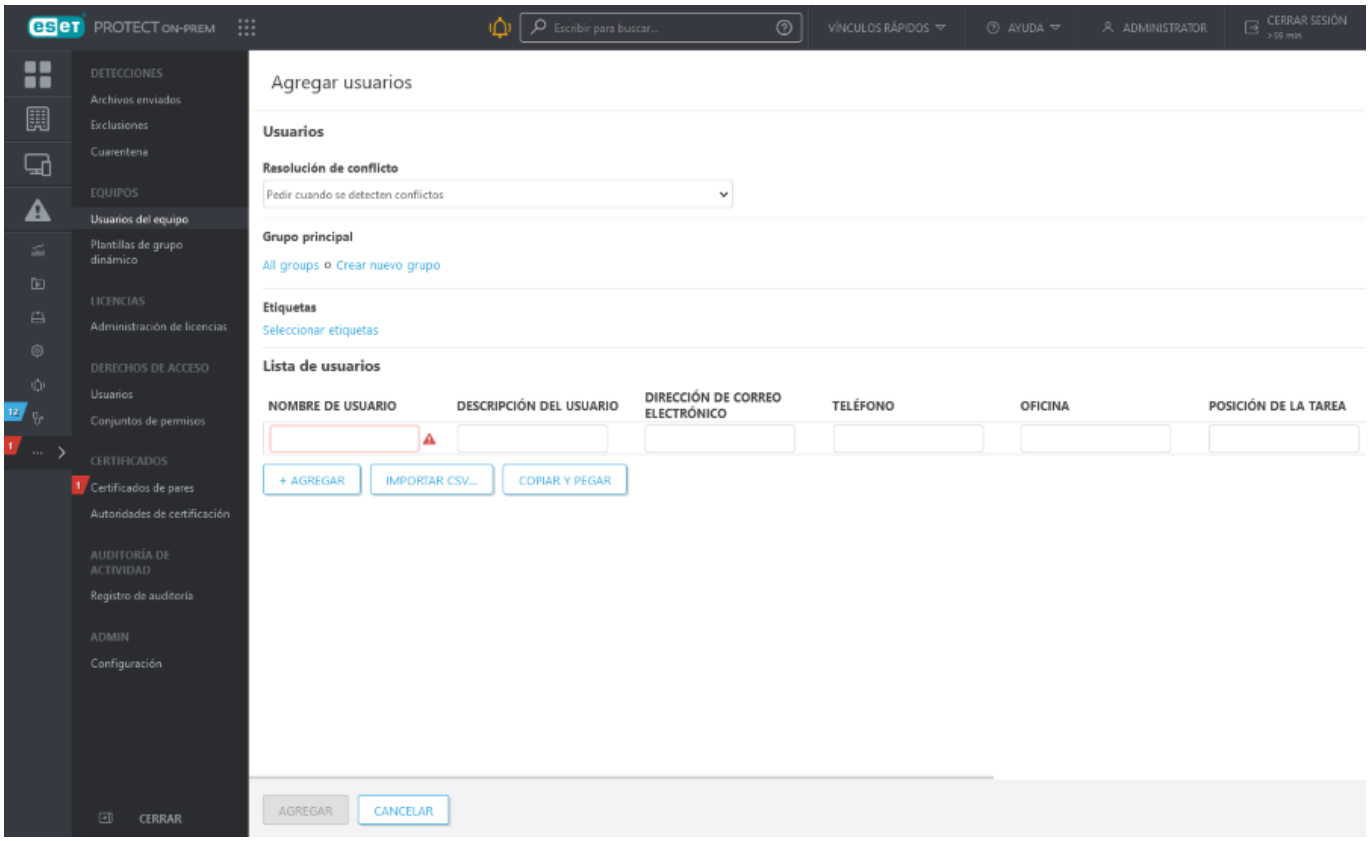
5. Use el menú desplegable de **Resolución de conflictos** para seleccionar la acción a realizar si el usuario agregado ya se encuentra en ESET PROTECT On-Prem:

- **Preguntar cuando se detectan conflictos**: cuando se detecta un conflicto, el programa le solicitará que seleccione una acción (vea las siguientes opciones).

- **Omitir usuarios con conflictos**: no se agregarán usuarios con el mismo nombre. Esto también asegura que los atributos personalizados de usuarios existentes en ESET PROTECT On-Prem se mantengan (no serán sobrescritos con los datos de Active Directory).

- **Sobrescribir usuarios con conflictos**: los usuarios existentes en ESET PROTECT On-Prem se sobrescribirán por los usuarios de Active Directory. Si dos usuarios tienen el mismo SID, el usuario existente en ESET PROTECT On-Prem se elimina de su ubicación anterior (incluso si el usuario se encontraba en un grupo diferente).

6. Haga clic en **Agregar** cuando haya finalizado con los cambios. Los usuarios aparecerán en el grupo principal que haya especificado.



Editar usuarios

Puede modificar los detalles de un usuario como la información **Básica** y los **Equipos asignados**.

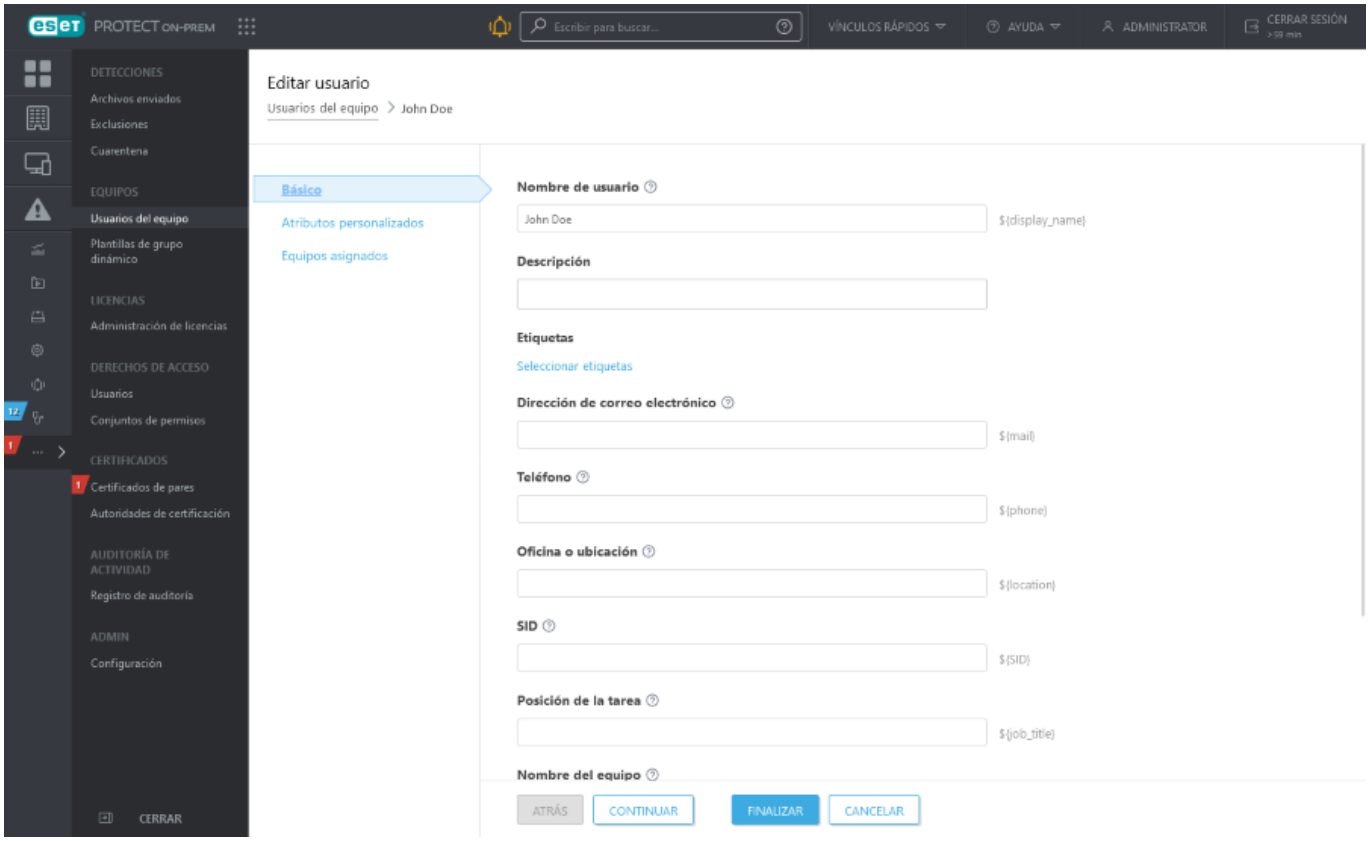
> Al realizar una tarea de Sincronización de usuario para los usuarios que poseen atributos personalizados definidos, configure**Manejo de colisión de creación de usuarios** a **Omitir**. Si no lo hace, los datos del usuario serán reemplazados por los datos de Active Directory.

Básica

Si ha usado una tarea de Sincronización de usuarios para crear el usuario y algunos campos están en blanco, podrá especificarlos de forma manual cuando sea necesario.

Aquí puede editar los detalles del usuario, como por ejemplo:

- **Nombre de usuario** y **descripción**: para fines informativos únicamente.
- **Etiquetas** –Editar etiquetas (asignar, desasignar, crear, quitar).
- **Dirección de correo electrónico**: se puede usar como dirección de destinatario para el envío de notificaciones.
- **Teléfono** y **Oficina o ubicación**: para fines informativos únicamente.
- **SID**: se lo puede asociar con varias funciones de ESET PROTECT On-Prem que requieren esta información de AD (por ejemplo, modo de Anulación de la política de Endpoint).



Atributos personalizados

Puede editar atributos personalizados existentes o añadir nuevos atributos. Para agregar nuevos atributos, haga clic en **Agregar nuevos** y seleccione una de las categorías:

- **Cuentas de Wi-Fi**: los perfiles pueden usarse para enviar la configuración wifi corporativa directamente a los dispositivos gestionados.

- **Cuentas de VPN**: puede configurar una VPN junto con las credenciales, certificados, y otra información necesaria para hacer que la VPN sea fácilmente accesible para los usuarios.

- **Cuentas de correo electrónico**: Esta opción se usa con cualquier cuenta de correo electrónico que usa especificaciones IMAP o POP3. Si usa un servidor de Exchange, use la configuración de Exchange ActiveSync que se muestra a continuación.

- **Cuentas Exchange**: si su empresa usa Microsoft Exchange, podrá crear aquí todos los ajustes para reducir al mínimo el tiempo de configuración para que sus usuarios acceden al correo electrónico, calendario y contactos.

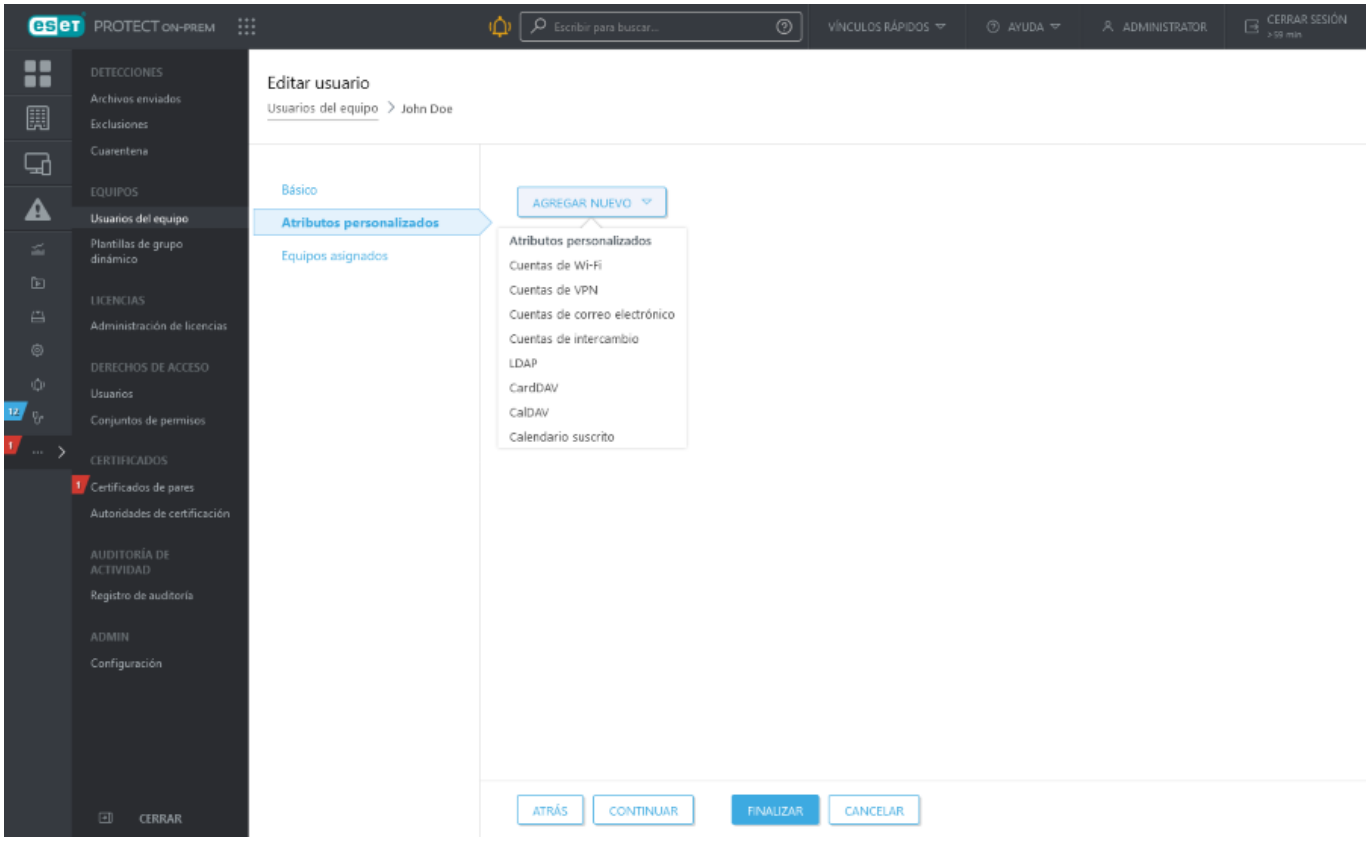
- **LDAP (Administración del alias)**: Esta opción es especialmente útil si su empresa usa LDAP para los contactos. Puede asignar los campos de contacto a los campos de contacto iOS correspondientes.

- **CalDAV**: Este contiene los ajustes para cualquier calendario que use las especificaciones CalDAV.

- **CardDAV**: para los contacto que se sincronizan a través de la especificación CardDAV; la información para la sincronización se puede establecer aquí.

- **Calendario suscrito**: si se configuran calendarios CalDAV, aquí es donde podrá definir el acceso de sólo lectura a los calendarios de los demás.

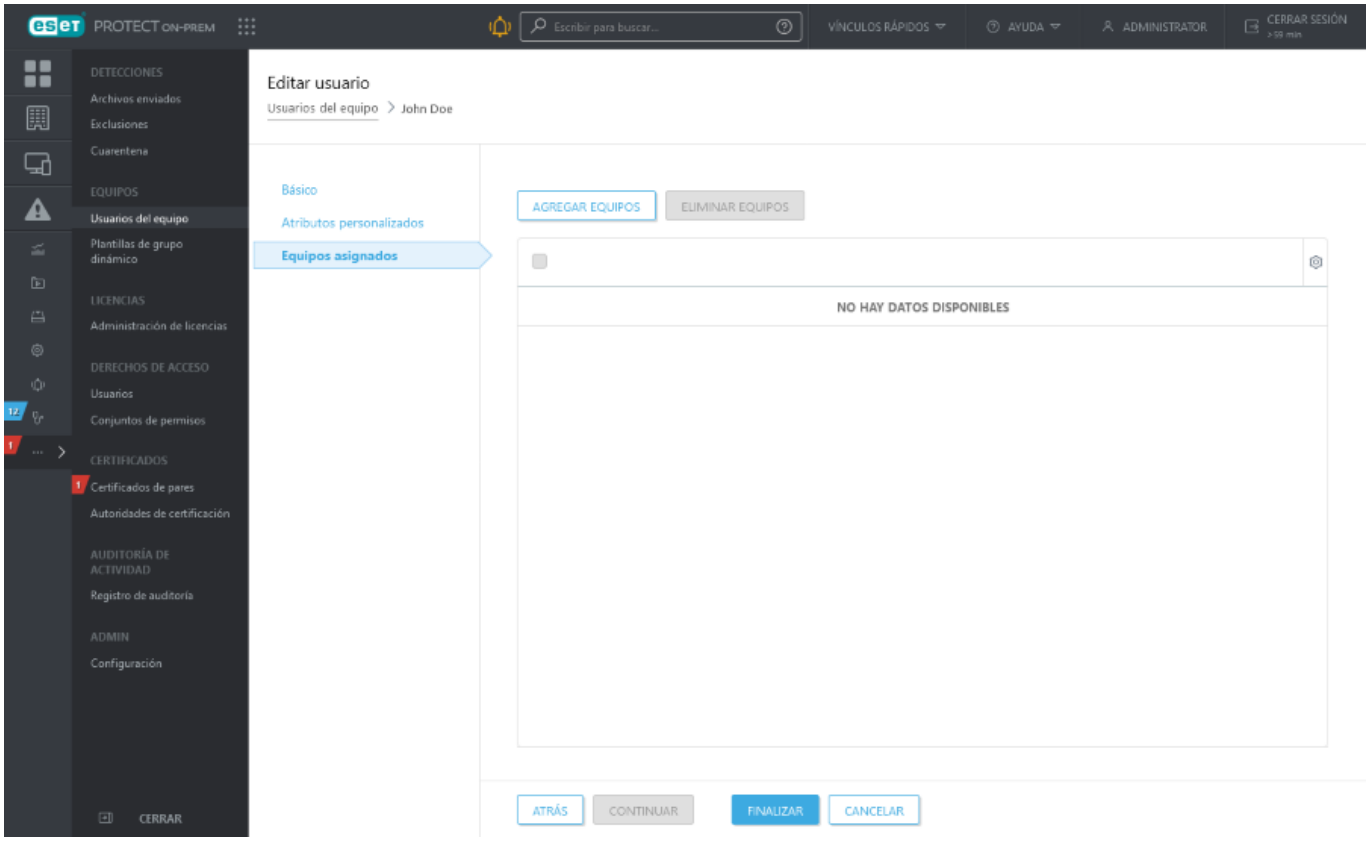
Algunos de los campos se convertirán en un atributo que luego podrá usar como una variable (marcador) al crear una política para dispositivos móviles iOS. Por ejemplo, Inicio de sesión `${exchange_login/exchange}` o Dirección de correo electrónico `${exchange_email/exchange}`.



Equipos asignados

Aquí puede seleccionar dispositivos individuales. Para ello, haga clic en **Agregar equipos -** se listarán todos los grupos estáticos y dinámicos con sus miembros. Use las casillas de verificación para realizar su selección y haga clic en **Aceptar**.

Un usuario solo puede asignarse a 200 equipos como máximo en una operación.

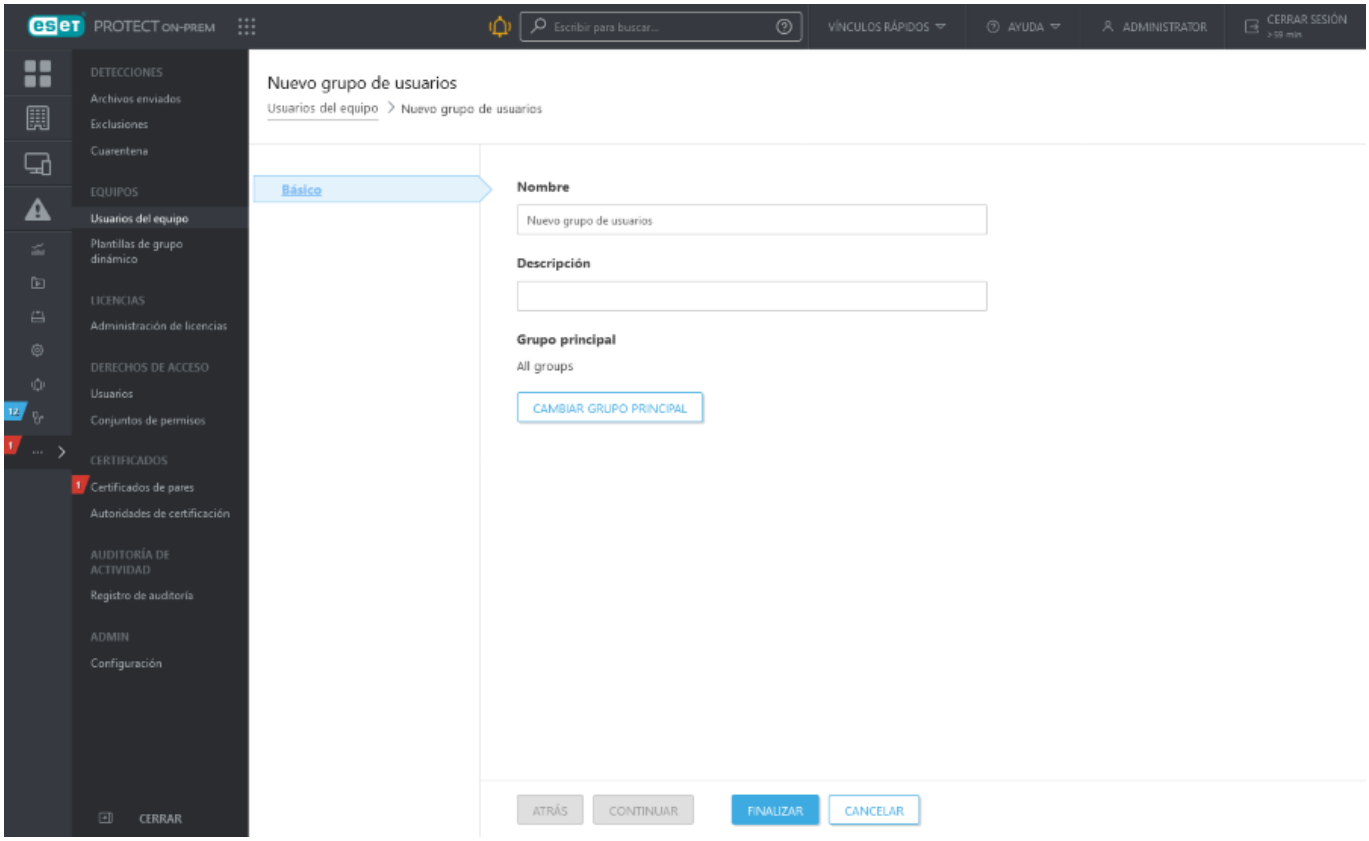


Crear nuevo grupo de usuarios

Haga clic en **Usuarios del equipo** > ⚙ y seleccione + **Nuevo grupo de usuarios**

Básica

Ingrese un **Nombre y Descripción** (opcional) para el nuevo Grupo de usuarios. En forma predeterminada, el grupo principal es el grupo que seleccionó cuando comenzó a crear el nuevo Grupo de usuarios. Si desea cambiar el grupo principal, haga clic en **Cambiar grupo principal** y seleccione un grupo principal del árbol. Haga clic en **Finalizar** para crear el nuevo Grupo de usuarios.



También puede asignar permisos específicos para este Grupo de usuarios dentro de Derechos de acceso mediante Grupos de permisos (consulte la sección **Grupos de usuarios**). De esta manera, puede especificar qué consola específica de ESET PROTECT Web Console los usuarios pueden administrar con qué grupos de usuarios específicos. Incluso, puede restringir el acceso de dichos usuarios a otras funciones de ESET PROTECT On-Prem usando las políticas, si así lo desea. Estos usuarios, en consecuencia, solo administrarán los Grupos de usuarios.

Plantillas de grupos dinámicos

Las plantillas de Grupos dinámicos establecen los criterios que los equipos deben cumplir para ser colocados en un Grupo dinámico. Cuando el cliente cumple con estas reglas, el cliente se moverá automáticamente al Grupo dinámico.

Una plantilla es un objeto estático en un grupo estático. Los usuarios deben contar con los permisos adecuados para acceder a las plantillas. Un usuario necesita de permisos de acceso para poder trabajar con plantillas de grupo dinámico. Todas las plantillas predefinidas se encuentran en el grupo estático **Todos** y, por defecto, se encuentran disponibles solo para el administrador. Los otros usuarios necesitan permisos adicionales asignados. Como resultado, es posible que los usuarios no puedan ver ni usar plantillas predeterminadas. Las plantillas se pueden mover a un grupo donde los usuarios tengan permisos.
Para duplicar una plantilla, el usuario debe contar con permisos de **Uso** (para plantillas de grupo dinámico) para el grupo donde se encuentra la plantilla fuente y de **Escribir** para el grupo hogar del usuario (donde se almacenará el duplicado). Consulte el ejemplo de duplicación de objetos.

- Crear plantilla nueva de grupo dinámico
- Reglas para la plantilla de un Grupo dinámico
- Plantilla de grupo dinámico: ejemplos

Administrar plantillas de Grupos dinámicos

Las plantillas se pueden administrar desde **Más** > **Plantillas de grupos dinámicos**.

Nueva plantilla	Haga clic para crear una Nueva plantilla en su grupo hogar.
Mostrar detalles	Consulte el resumen de información sobre la plantilla seleccionada.
Registro de auditoría	Ver el registro de auditoría del elemento seleccionado.
Etiquetas	Editar etiquetas (asignar, desasignar, crear, quitar).
Editar	Edita la plantilla seleccionada. Haga clic en **Guardar como** si desea mantener su plantilla existente y crear una nueva basada en la plantilla que está editando. Cuando se le solicite, especifique el nombre de la nueva plantilla.
Duplicar	Crea plantillas de un grupo dinámico nuevo en función de la plantilla seleccionada. Será necesario que la tarea duplicada tenga otro nombre. La plantilla duplicada se almacenará en su grupo hogar.
Eliminar	Elimina la plantilla permanentemente.
Importar	Importar plantillas de grupo dinámico desde un archivo. Durante la importación, se comprueba la estructura del archivo para asegurarse de que el archivo no esté corrupto.
Exportar	Exporte las plantillas del grupo dinámico seleccionado a un archivo con fines de creación de copias de seguridad o migración. No recomendamos hacer ediciones en el archivo, ya que es posible que los datos queden inutilizables.
Grupo de acceso > **Mover**	Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen derechos suficientes para el grupo de destino. Cambiar el grupo de acceso es útil cuando se resuelven problemas de acceso con otros usuarios. El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario.

Personalización del diseño y de los filtros

Puede personalizar la vista de la pantalla de la consola web actual:

- Administre el panel lateral y la tabla principal.
- Agregar filtro y filtros preestablecidos. Puede usar etiquetas para filtrar los elementos mostrados.

Nueva plantilla de grupo dinámico

Haga clic en **Nueva plantilla** en **Más** > **Plantillas de grupos dinámicos**

Básica

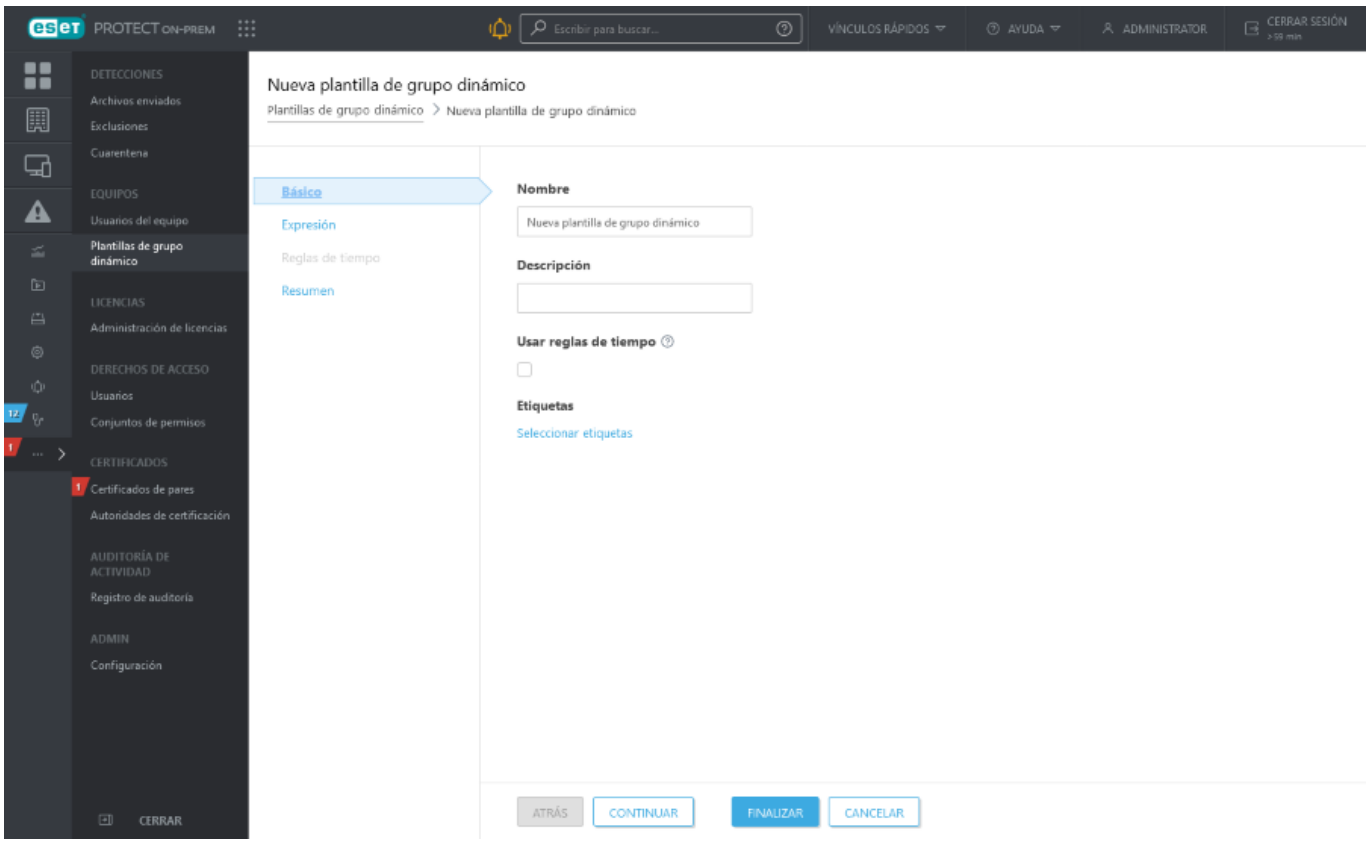
Ingrese un **Nombre** y una **Descripción** para la plantilla nueva del Grupo dinámico.

Seleccione **Usar reglas de tiempo** para habilitar **Reglas de tiempo** y configure un tiempo específico durante el cual se habilita la coincidencia dinámica de grupos.

Haga clic en **Seleccionar etiquetas** para asignar etiquetas.

Expresión

Consulte nuestros ejemplos con instrucciones paso a paso ilustradas para ver muestras sobre cómo usar Grupos dinámicos en su red.



Reglas de tiempo

Establezca una franja horaria para la nueva plantilla de grupo dinámico. Haga clic en el botón **Actualizar**. Haga clic en el campo de hora y seleccione **Hora de inicio** y **Hora de finalización** en el menú desplegable. Seleccione la frecuencia (Todos los días, Día laborable, Fin de semana) o el día de la semana y la hora. El tiempo seleccionado debe ser superior a 1 minuto e inferior a 24 horas. Después de configurar la **Hora de inicio** y la **Hora de finalización**, la columna **Duración** muestra la duración de la hora configurada. Puede agregar más franjas horarias.

Resumen

Revise los ajustes configurados y haga clic en **Finalizar** para crear la plantilla. Esta nueva plantilla se agregará a la lista de plantillas y puede usarse luego para crear un Grupo dinámico nuevo.

Reglas para la plantilla de un grupo dinámico

Cuando configure reglas para una plantilla de Grupo dinámico puede usar diferentes operadores para condiciones diferentes para alcanzar su escenario deseado.

Los siguientes capítulos explican las reglas y las operaciones utilizadas en las plantillas de grupo dinámico:

- Operaciones

- Reglas y conectores lógicos
- Plantilla de evaluación de reglas
- Cómo crear una automatización en ESET PROTECT On-Prem
- Plantillas de grupos dinámicos
- Casos de uso: crear una plantilla de Grupo dinámico específica

Operaciones

Si especifica múltiples roles (condiciones), debe seleccionar qué operación debe usarse para combinar las reglas. Según el resultado, un equipo cliente se agregará o no a un Grupo dinámico que usa esta Plantilla.

- La **operación** seleccionada funciona no solo al combinar más reglas, sino también cuando hay una sola regla.
- No puede combinar operaciones. Solo una operación se usa por cada plantilla de grupo dinámico y aplica a todas sus reglas.

AND (todas las condiciones deben ser verdaderas)	Verifica si todas las condiciones se evalúan positivamente; el equipo debe cumplir con todos los parámetros requeridos.
OR (al menos una condición debe ser verdadera)	Verifica si al menos una de las condiciones se evalúa positivamente; el equipo debe cumplir con al menos uno de los parámetros requeridos.
NAND (Al menos una condición debe ser falsa)	Verifica si una de las condiciones no se evalúa positivamente; el equipo no debe cumplir con al menos uno de los parámetros requeridos.
NOR (todas las condiciones deben ser falsas)	Verifica si todas las condiciones no se evalúan positivamente; el equipo no debe cumplir con algunos de los parámetros requeridos.

Reglas y conectores lógicos

Una regla cuenta con un elemento, un conector lógico (operador lógico) y un valor definido.

Al hacer clic en **+ Agregar regla**, se abre una ventana con una lista de elementos divididos en categorías. Por ejemplo:

Software instalado > **Nombre de aplicación**

Adaptadores de red > **Dirección MAC**

Edición del SO > **Nombre del SO**

Puede explorar la lista de todas las reglas disponibles en este artículo de la base de conocimiento de ESET.

Para crear una regla, seleccione un elemento, seleccione un operador lógico y especifique un valor. La regla se evaluará según el valor que ha especificado y el operador lógico usado.

Los tipos de valores aceptables incluyen número(s), cadena(s), enum(es), dirección(es) IP, máscaras de producto e identificaciones de equipos. Cada tipo de valor cuenta con diferentes operadores lógicos asociados con él mismo y la consola web ESET PROTECT mostrará automáticamente solo los compatibles.

• **“= (igual)”:** el valor del símbolo y la plantilla deben ser iguales. Las cadenas se comparan sin distinguir entre mayúsculas y minúsculas.

• **“> (mayor que)”:** el valor del símbolo debe ser mayor que el valor de la plantilla. También se puede usar para crear una comparación de rangos para símbolos de direcciones IP.

• **“≥ (mayor o igual)”:** el valor del símbolo debe ser mayor o igual que el valor de la plantilla. También se puede usar para crear una comparación de rangos para símbolos de direcciones IP.

• **“< (menor que)”:** el valor del símbolo debe ser menor que el valor de la plantilla. También se puede usar para crear una comparación de rangos para símbolos de direcciones IP.

• **“≤ (menor o igual)”:** el valor del símbolo debe ser menor o igual que el valor de la plantilla. También se puede usar para crear una comparación de rangos para símbolos de direcciones IP.

• **“contiene”:** el valor del sistema contiene el valor de la plantilla. En el caso de cadenas, busca una subcadena. La búsqueda se realiza sin distinguir entre mayúsculas y minúsculas.

• **“tiene prefijo”:** el valor del símbolo tiene el mismo prefijo que el valor de la plantilla. Las cadenas se comparan sin distinguir entre mayúsculas y minúsculas. Configura los primeros caracteres de la cadena buscada, por ejemplo, en “Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319”, el prefijo significa “Micros” o “Micr” o “Microsof”, etc.

• **“tiene postfijo”:** el valor del símbolo tiene el mismo postfix que el valor de la plantilla. Las cadenas se comparan sin distinguir entre mayúsculas y minúsculas. Configura los primeros caracteres de la cadena buscada, por ejemplo, en “Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319”, el postfijo es “319” o “0.30319”, etc.

• **“tiene máscara”:** el valor del símbolo debe ser igual a una máscara definida en la plantilla. El formateo de máscara permite cualquier carácter los símbolos especiales “*” - cero, uno o más caracteres y “?” exactamente un carácter, por ej.: "6.2.*" o "6.2.2033.?".

• **“regex”:** el valor del símbolo debe ser igual que la expresión normal (regex) de una plantilla. El regex debe estar escrito en el formato **Perl**.

Una expresión regular, *regex* o *regexp* es una secuencia de caracteres que define un patrón de búsqueda. Por ejemplo, *gray|grey* y *gr(a|e)y* son patrones equivalentes que coinciden con estas dos palabras: “*gray*”, “*grey*”.

• **“es uno de”:** el valor del símbolo debe ser igual a cualquier valor de una lista en una plantilla. Para agregar un elemento, haga clic en **+ Agregar**. Cada línea en un nuevo elemento en la lista. Las cadenas se comparan sin distinguir entre mayúsculas y minúsculas.

• **“es uno de (máscara de cadena)”:** el valor del símbolo debe ser igual a cualquier valor de una máscara en una plantilla. Las cadenas se comparan con la función de distinguir entre mayúsculas y minúsculas. Ejemplos: *endpoint-pc*, *Endpoint-PC*.

• **“tiene valor”**

Las reglas de tiempo permiten seleccionar la casilla **Medida del tiempo transcurrido** para crear una plantilla de grupo dinámico en función del tiempo transcurrido desde un suceso específico. El equipo administrado debe ejecutar el agente de ESET Management 10.0 y versiones posteriores.

Operadores negativos:

Los operadores negativos se deben usar con cuidado porque, en caso de registros de línea múltiples como "aplicación instalada", todas las líneas se prueban contra estas condiciones. Consulte los ejemplos incluidos (Evaluación de reglas de plantilla y Plantilla de grupo dinámico: ejemplos) para ver cómo los operadores negativos o las operaciones negativas se deben usar para obtener los resultados deseados.

- **"≠ (no igual)":** el valor del símbolo y la plantilla no deben ser iguales. Las cadenas se comparan sin distinguir entre mayúsculas y minúsculas.
- **"no contiene":** el valor del símbolo no contiene el valor de la plantilla. La búsqueda se realiza sin distinguir entre mayúsculas y minúsculas.
- **"no tiene prefijo":** el valor del símbolo no tiene el mismo prefijo que el valor de la plantilla. Las cadenas se comparan sin distinguir entre mayúsculas y minúsculas.
- **"no tiene postfix":** el valor del símbolo no tiene el mismo postfijo que el valor de la plantilla. Las cadenas se comparan sin distinguir entre mayúsculas y minúsculas.
- **"no tiene máscara":** el valor del símbolo no debe ser igual a una máscara definida en la plantilla.
- **"no regex":** el valor del símbolo no debe ser igual que la expresión normal (regex) de una plantilla. El regex debe estar escrito en el formato **Perl**. La operación negativa se brinda como ayuda para negar expresiones regulares sin reescritura.
- **"no es uno de":** el valor del símbolo no debe ser igual a cualquier valor de la lista en una plantilla. Las cadenas se comparan sin distinguir entre mayúsculas y minúsculas.
- **"no es uno de (máscara de cadena)":** el valor del símbolo no debe ser igual a cualquier valor de una máscara en una plantilla.
- **"no tiene valor"**

Plantilla de evaluación de reglas

La plantilla de evaluación de reglas se maneja a través del agente ESET Management, no del servidor ESET PROTECT (solo los resultados se envían al servidor ESET PROTECT). El proceso de evaluación se realiza según las reglas configuradas en la plantilla. A continuación, podrá encontrar algunos ejemplos de plantillas del proceso de evaluación de reglas.

Necesita distinguir entre prueba de existencia (algo que no existe en absoluto con ese valor) y prueba de diferencia (algo que existe pero tiene un valor diferente). Aquí, hay algunas reglas básicas para hacer esta distinción:

- Para verificar la existencia: Operación sin negativa (**AND**, **OR**) y operador sin negativa (=, >, <, **contiene**,...).
- Para verificar la existencia de un valor diferente: La operación **AND** los operadores incluidos una negación, como mínimo (=, >, <, **contiene**, **no contiene**,...).
- Para verificar la no existencia de un valor: Operaciones sin negativa (**NAND**, **NOR**) y operadores sin negativa (=, >, <, **contiene**,...).

Para comprobar la presencia de una lista de elementos (por ejemplo, una lista específica de aplicaciones instaladas en un equipo), debe crear una plantilla individual de Grupo dinámico para cada uno de los elementos de la lista y asignar la plantilla a otro Grupo dinámico. Cada uno de los Grupos dinámicos es un subgrupo del otro. Los equipos que poseen la lista de elementos forman parte del último subgrupo.

El Estado es un conjunto de información diversa. Algunas fuentes proporcionan más de un estado dimensional por máquina (por ejemplo, del sistema operativo, el tamaño de memoria RAM, etc.), otras proporcionan información sobre el estado multidimensional (por ejemplo, la dirección IP, las aplicaciones instaladas, etc.).

A continuación se muestra una representación visual del estado de un cliente:

Adaptadores de red - Dirección IP	Adaptadores de red - Dirección MAC	Nombre del sistema operativo	Versión de sistema operativo	Cantidad de RAM del equipo en MB	Aplicaciones instaladas
192.168.1.2	4A-64-3F-10-FC-75	Windows 11 Enterprise	10.0.22621	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				Lector de PDF
124.256.25.25	52-FB-E5-74-35-73				Aplicaciones Office
					Pronóstico del Tiempo

El Estado está hecho de grupos de información. Un grupo de datos proporciona siempre información coherente organizada en filas. El número de filas por grupo puede variar.

Las condiciones se evalúan por grupo y por fila: si hay más condiciones con respecto a las columnas de un grupo, solo se considerarán los valores dentro de la misma fila.

Ejemplo 1:

Para este ejemplo considere las siguientes condiciones:

```
Adaptadores de red.Dirección IP = 10.1.1.11 Y Adaptadores de red. Dirección MAC = 4A
-64-3F-10-FC-75
```

Esta regla no coincide con ningún equipo, ya que no hay ninguna fila en donde ambas condiciones son válidas.

Adaptadores de red - Dirección IP	Adaptadores de red - Dirección MAC	Nombre del sistema operativo	Versión de sistema operativo	Cantidad de RAM del equipo en MB	Aplicaciones instaladas
192.168.1.2	4A-64-3F-10-FC-75	Windows 11 Enterprise	10.0.22621	2048	ESET Endpoint Security

Adaptadores de red - Dirección IP	Adaptadores de red - Dirección MAC	Nombre del sistema operativo	Versión de sistema operativo	Cantidad de RAM del equipo en MB	Aplicaciones instaladas
10.1.1.11	2B-E8-73-BE-81-C7				Lector de PDF
124.256.25.25	52-FB-E5-74-35-73				Aplicaciones Office
					Pronóstico del Tiempo

Ejemplo 2:

Para este ejemplo considere las siguientes condiciones:

```
Adaptadores de red.Dirección IP = 192.168.1.2 y Adaptadores de red.Dirección MAC = 4A-64-3F-10-FC-75
```

Esta vez, las dos condiciones corresponden con celdas dentro de la misma fila y, por lo tanto, la regla en su conjunto se evalúa como VERDADERA. El equipo está seleccionado.

Adaptadores de red - Dirección IP	Adaptadores de red - Dirección MAC	Nombre del sistema operativo	Versión de sistema operativo	Cantidad de RAM del equipo en MB	Aplicaciones instaladas
192.168.1.2	4A-64-3F-10-FC-75	Windows 11 Enterprise	10.0.22621	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				Lector de PDF
124.256.25.25	52-FB-E5-74-35-73				Aplicaciones Office
					Pronóstico del Tiempo

Ejemplo 3:

Para las condiciones con el operador O (al menos una condición debe ser VERDADERA), como por ejemplo:

```
Adaptadores de red.Dirección IP = 10.1.1.11 O Adaptadores de red.Dirección MAC = 4A-64-3F-10-FC-75
```

La regla es VERDADERA en dos filas, ya que solo una de las condiciones se tiene que cumplir. El equipo está seleccionado.

Adaptadores de red - Dirección IP	Adaptadores de red - Dirección MAC	Nombre del sistema operativo	Versión de sistema operativo	Cantidad de RAM del equipo en MB	Aplicaciones instaladas
192.168.1.2	4A-64-3F-10-FC-75	Windows 11 Enterprise	10.0.22621	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				Lector de PDF
124.256.25.25	52-FB-E5-74-35-73				Aplicaciones Office

Adaptadores de red - Dirección IP	Adaptadores de red - Dirección MAC	Nombre del sistema operativo	Versión de sistema operativo	Cantidad de RAM del equipo en MB	Aplicaciones instaladas
					Pronóstico del Tiempo

Plantilla de grupo dinámico: ejemplos

Encontrará plantillas útiles predefinidas de grupos dinámicos en **Más** > **Plantillas de grupos dinámicos**.

Las plantillas de muestra de grupos dinámicos y los ejemplos de uso en esta guía muestran algunas de las formas en que puede usar los grupos dinámicos para administrar su red:

Un Grupo dinámico que detecta si se instalo un producto de seguridad
Un Grupo dinámico que detecta si se instaló una versión específica de un software
Un Grupo dinámico que detecta si no se instaló una versión específica de un software
Un Grupo dinámico que detecta si no se instaló una versión específica de un software pero existe otra versión
Un Grupo dinámico que detecta si un equipo se encuentra en una subred específica
Un Grupo dinámico que detecta versiones de productos de seguridad del servidor instaladas pero no activadas
Cómo implementar automáticamente productos ESET en nuevos equipos Windows de escritorios conectados
Aplicar las políticas basadas en la ubicación

Consulte también nuestros **artículos de la base de conocimiento** con ejemplos de plantillas de grupos dinámicos y su uso:

Ejemplos útiles de plantillas de grupos dinámicos en ESET PROTECT On-Prem: ejemplos de cómo puede usar los detalles del Inventario de hardware para crear reglas para un grupo dinámico que contenga los dispositivos que cumplen con los criterios de hardware seleccionados.
Configure ESET PROTECT On-Prem para implementar automáticamente productos de puntos de conexión de ESET para equipos desprotegidos
Configure puntos de conexión para usar diferentes ajustes de actualización según la red a la que estén conectados con ESET PROTECT On-Prem
Cree un nuevo certificado para que las nuevas estaciones de trabajo se unan automáticamente a un grupo dinámico en ESET PROTECT On-Prem

Es posible que los artículos de la base de conocimiento no estén disponibles en su idioma.

Existen, por supuesto, muchos otros objetivos que se pueden lograr a través de plantillas de grupos dinámicos con una combinación de reglas. Las posibilidades son prácticamente ilimitadas.

Grupo dinámico: se instaló un producto de seguridad

Este Grupo dinámico se puede usar para ejecutar una tarea inmediatamente luego de instalar el producto de seguridad de ESET en un equipo: activación, exploración personalizada, etc.

Puede crear una **Nueva plantilla** en **Más** > **Plantillas de grupo dinámico** y crear un nuevo grupo dinámico con plantilla.

Básica

Ingrese un **Nombre** y una **Descripción** para la plantilla nueva del Grupo dinámico.

Seleccione **Usar reglas de tiempo** para habilitar **Reglas de tiempo** y configure un tiempo específico durante el cual se habilita la coincidencia dinámica de grupos.

Expresión

1.Seleccione un operador lógico en el menú Operación: **AND** (Todas las condiciones deben ser verdaderas).

2.Haga clic en **+ Agregar regla** y seleccione una condición. Seleccione **Equipo** > **Máscara de productos administrados** > **en** > **Protegido por ESET: Escritorio**. También puede seleccionar diferentes productos de ESET.

Reglas de tiempo

Establezca una franja horaria para la nueva plantilla de grupo dinámico. Haga clic en el botón **Actualizar**. Haga clic en el campo de hora y seleccione **Hora de inicio** y **Hora de finalización** en el menú desplegable. Seleccione la frecuencia (Todos los días, Día laborable, Fin de semana) o el día de la semana y la hora. El tiempo seleccionado debe ser superior a 1 minuto e inferior a 24 horas. Después de configurar la **Hora de inicio** y la **Hora de finalización**, la columna **Duración** muestra la duración de la hora configurada. Puede agregar más franjas horarias.

Resumen

Revise los ajustes configurados y haga clic en **Finalizar** para crear la plantilla. Esta nueva plantilla se agregará a la lista de plantillas y puede usarse luego para crear un Grupo dinámico nuevo.

Grupo dinámico: se instaló una versión de software específica

Este Grupo dinámico se puede usar para detectar software de seguridad de ESET instalado en un equipo. Luego podrá ejecutar, por ejemplo, una tarea de actualización o ejecutar un comando personalizado en dichos equipos. Se pueden usar operadores diferentes como **“contiene”** o **“tiene el prefijo”**.

Puede crear una **Nueva plantilla** en **Más** > **Plantillas de grupo dinámico** y crear un nuevo grupo dinámico con plantilla.

Básica

Ingrese un **Nombre** y una **Descripción** para la plantilla nueva del Grupo dinámico.

Seleccione **Usar reglas de tiempo** para habilitar **Reglas de tiempo** y configure un tiempo específico durante el cual se habilita la coincidencia dinámica de grupos.

Expresión

1.Seleccione un operador lógico en el menú Operación: **AND** (Todas las condiciones deben ser verdaderas).

2.Haga clic en **+ Agregar regla** y seleccione una condición:

- **Software instalado** > **Nombre de aplicación** > **= (igual)** > *ESET Endpoint Security*
- **Software instalado** > **Versión de aplicación** > = **(igual)** > *6.2.2033.0*

Reglas de tiempo

Establezca una franja horaria para la nueva plantilla de grupo dinámico. Haga clic en el botón **Actualizar**. Haga clic en el campo de hora y seleccione **Hora de inicio** y **Hora de finalización** en el menú desplegable. Seleccione la frecuencia (Todos los días, Día laborable, Fin de semana) o el día de la semana y la hora. El tiempo seleccionado debe ser superior a 1 minuto e inferior a 24 horas. Después de configurar la **Hora de inicio** y la **Hora de finalización**, la columna **Duración** muestra la duración de la hora configurada. Puede agregar más franjas horarias.

Resumen

Revise los ajustes configurados y haga clic en **Finalizar** para crear la plantilla. Esta nueva plantilla se agregará a la lista de plantillas y puede usarse luego para crear un Grupo dinámico nuevo.

Grupo dinámico: no se instaló una versión específica de un software

Este Grupo dinámico se puede usar para detectar software de seguridad de ESET faltante en un equipo. La configuración de este ejemplo incluirá a las máquinas que no contienen el software en lo absoluto o a las máquinas con diferentes versiones a la especificada.

Este grupo es útil porque usted podrá ejecutar una tarea de instalación de software en dichos equipos para instalar o actualizar. Se pueden usar operadores diferentes como **“contiene”** o **“tiene el prefijo”**.

Haga clic en **Nueva plantilla** en **Más** > **Plantillas de grupos dinámicos**

Básica

Ingrese un **Nombre** y una **Descripción** para la plantilla nueva del Grupo dinámico.

Seleccione **Usar reglas de tiempo** para habilitar **Reglas de tiempo** y configure un tiempo específico durante el cual se habilita la coincidencia dinámica de grupos.

Expresión

1.Seleccione un operador lógico en el menú Operación: **NAND** (Al menos una condición debe ser falsa).

2.Haga clic en **+ Agregar regla** y seleccione una condición:

- **Software instalado** > **Nombre de aplicación** > **= (igual)** > *ESET Endpoint Security*
- **Software instalado** > **Versión de aplicación** > = **(igual)** > *6.2.2033.0*

Reglas de tiempo

Establezca una franja horaria para la nueva plantilla de grupo dinámico. Haga clic en el botón **Actualizar**. Haga clic en el campo de hora y seleccione **Hora de inicio** y **Hora de finalización** en el menú desplegable. Seleccione la frecuencia (Todos los días, Día laborable, Fin de semana) o el día de la semana y la hora. El tiempo seleccionado debe ser superior a 1 minuto e inferior a 24 horas. Después de configurar la **Hora de inicio** y la **Hora de finalización**, la columna **Duración** muestra la duración de la hora configurada. Puede agregar más franjas horarias.

Resumen

Revise los ajustes configurados y haga clic en **Finalizar** para crear la plantilla. Esta nueva plantilla se agregará a la lista de plantillas y puede usarse luego para crear un Grupo dinámico nuevo.

Grupo dinámico: no se instaló una versión específica de un software pero existe otra versión

El Grupo dinámico se puede usar para detectar un software que está instalado pero cuenta con una versión diferente a la que solicita. Este grupo es útil porque usted podrá ejecutar tareas de actualización en aquellas máquinas donde falta la versión requerida. Se pueden usar distintos operadores, pero asegúrese de que la prueba de versión se realice con un operador negativo.

Haga clic en **Nueva plantilla** en **Más** > **Plantillas de grupos dinámicos**

Básica

Ingrese un **Nombre** y una **Descripción** para la plantilla nueva del Grupo dinámico.

Seleccione **Usar reglas de tiempo** para habilitar **Reglas de tiempo** y configure un tiempo específico durante el cual se habilita la coincidencia dinámica de grupos.

Expresión

1.Seleccione un operador lógico en el menú Operación: **AND** (Todas las condiciones deben ser verdaderas).

2.Haga clic en **+ Agregar regla** y seleccione una condición:

- **Software instalado** > **Nombre de aplicación** > **= (igual)** > *ESET Endpoint Security*

- **Software instalado** > **Versión de aplicación** > **≠ (no es igual)** > *“6.2.2033.0”*

Reglas de tiempo

Establezca una franja horaria para la nueva plantilla de grupo dinámico. Haga clic en el botón **Actualizar**. Haga clic en el campo de hora y seleccione **Hora de inicio** y **Hora de finalización** en el menú desplegable. Seleccione la frecuencia (Todos los días, Día laborable, Fin de semana) o el día de la semana y la hora. El tiempo seleccionado debe ser superior a 1 minuto e inferior a 24 horas. Después de configurar la **Hora de inicio** y la **Hora de finalización**, la columna **Duración** muestra la duración de la hora configurada. Puede agregar más franjas horarias.

Resumen

Revise los ajustes configurados y haga clic en **Finalizar** para crear la plantilla. Esta nueva plantilla se agregará a la lista de plantillas y puede usarse luego para crear un Grupo dinámico nuevo.

Grupo dinámico: un equipo se encuentra en una subred específica

Este grupo dinámico se puede usar para detectar una subred específica. Luego, puede usarse para aplicar políticas personalizadas para la actualización o el control web. Puede especificar diferentes rangos.

Haga clic en **Nueva plantilla** en **Más** > **Plantillas de grupos dinámicos**

Básica

Ingrese un **Nombre** y una **Descripción** para la plantilla nueva del Grupo dinámico.

Seleccione **Usar reglas de tiempo** para habilitar **Reglas de tiempo** y configure un tiempo específico durante el cual se habilita la coincidencia dinámica de grupos.

Expresión

1.Seleccione un operador lógico en el menú Operación: **AND** (Todas las condiciones deben ser verdaderas).

2.Haga clic en **+ Agregar regla** y seleccione una condición:

- **Direcciones IP de la red** > **Dirección IP del adaptador** > **≥ (mayor o igual)** > *10.1.100.1*
- **Direcciones IP de la red** > **Dirección IP del adaptador** > **≤ (menor o igual)** > *10.1.100.254*
- **Direcciones IP de la red** > **Máscara de subred del adaptador** > **= (igual)** > *255.255.255.0*

Reglas de tiempo

Establezca una franja horaria para la nueva plantilla de grupo dinámico. Haga clic en el botón **Actualizar**. Haga clic en el campo de hora y seleccione **Hora de inicio** y **Hora de finalización** en el menú desplegable. Seleccione la frecuencia (Todos los días, Día laborable, Fin de semana) o el día de la semana y la hora. El tiempo seleccionado debe ser superior a 1 minuto e inferior a 24 horas. Después de configurar la **Hora de inicio** y la **Hora de**

finalización, la columna **Duración** muestra la duración de la hora configurada. Puede agregar más franjas horarias.

Resumen

Revise los ajustes configurados y haga clic en **Finalizar** para crear la plantilla. Esta nueva plantilla se agregará a la lista de plantillas y puede usarse luego para crear un Grupo dinámico nuevo.

Grupo dinámico: producto de seguridad del servidor instalado pero no activado

Este Grupo dinámico puede usarse para detectar productos de servidor inactivos. Una vez detectados estos productos, puede asignar una Tarea de cliente a este grupo para activar los equipos del cliente con la licencia adecuada. En este ejemplo, solo se especifica ESET Mail Security para Microsoft Exchange Server, pero puede especificar varios productos.

Haga clic en **Nueva plantilla** en **Más** > **Plantillas de grupos dinámicos**

Básica

Ingrese un **Nombre** y una **Descripción** para la plantilla nueva del Grupo dinámico.

Seleccione **Usar reglas de tiempo** para habilitar **Reglas de tiempo** y configure un tiempo específico durante el cual se habilita la coincidencia dinámica de grupos.

Expresión

1. Seleccione un operador lógico en el menú Operación: **AND** (Todas las condiciones deben ser verdaderas).
2. Haga clic en **+ Agregar regla** y seleccione una condición:
   - **Equipo** > **Máscara de productos administrados** > **es uno de** > **Protegido por ESET: Servidor de correo**
   - **Problemas de funcionalidad/protección** > **Fuente** > **= (igual)** > **Producto de seguridad**
   - **Problemas de funcionalidad/protección** > **Problema** > = **(igual)** > **Producto no activado**

Reglas de tiempo

Establezca una franja horaria para la nueva plantilla de grupo dinámico. Haga clic en el botón **Actualizar**. Haga clic en el campo de hora y seleccione **Hora de inicio** y **Hora de finalización** en el menú desplegable. Seleccione la frecuencia (Todos los días, Día laborable, Fin de semana) o el día de la semana y la hora. El tiempo seleccionado debe ser superior a 1 minuto e inferior a 24 horas. Después de configurar la **Hora de inicio** y la **Hora de finalización**, la columna **Duración** muestra la duración de la hora configurada. Puede agregar más franjas horarias.

Resumen

Revise los ajustes configurados y haga clic en **Finalizar** para crear la plantilla. Esta nueva plantilla se agregará a la lista de plantillas y puede usarse luego para crear un Grupo dinámico nuevo.

Cómo automatizar ESET PROTECT On-Prem

Al utilizar técnicas, como en el siguiente ejemplo, puede automatizar diferentes acciones, desde actualizaciones de productos y SO, escaneados y activaciones automáticas de nuevos productos agregados con licencias preseleccionadas, hasta resolver incidentes sofisticados.

Cómo implementar automáticamente productos ESET en nuevos equipos Windows de escritorios conectados

⚠ Este ejemplo debe solo realizarse en cliente sin software de seguridad de terceros o de ESET del segmento para el hogar (por ej., ESET Smart Security). No se recomienda instalar productos ESET en clientes con software de seguridad de terceros. Puede utilizar ESET AV Remover para eliminar otros programas antivirus de su equipo.

1. Crear un grupo dinámico, llamado *Sin producto de seguridad*.
a.Conviértalo en un grupo secundario del grupo predefinido **Equipos Windows** > **Windows (de escritorio)**.
b.Haga clic en **Nueva plantilla**.
c.Agregue la siguiente regla: **Equipo** > **Máscara de productos administrados**.
d.Como operador, seleccione **no igual**.
e.Seleccione la máscara **protegido con ESET: Escritorio**
f.Haga clic en **Finalizar** para guardar el grupo.
2. Vaya a **Tareas** > **Nueva** > **Tarea del cliente**.
✓ a.Seleccione **Instalación del software** en el menú desplegable Tarea y escriba el nombre de la tarea en **Nombre.**
b.Seleccione el paquete en la sección **Configuración** y establezca otros parámetros, de ser necesario.
c.Haga clic en **Finalizar** > **Crear desencadenador**.
d.En la sección **Objetivo**, haga clic en **Agregar grupos** y seleccione *Sin producto de seguridad*.
e.En la sección **Desencadenador**, seleccione **Desencadenador de grupo dinámico unido**.
f.Haga clic en **Finalizar** para guardar la tarea y el desencadenador.
Esta tarea se ejecutará en clientes conectados al grupo dinámico a partir de este momento. Deberá ejecutar esta tarea manualmente en los clientes que se encontraban en el grupo dinámico antes de que se creara la tarea.

Aplicar las políticas basadas en la ubicación

1. Crear un grupo dinámico, llamado *Red secundaria 120*.
a.Hacerlo un grupo secundario del grupo **Todos**.
b.Haga clic en **Nueva plantilla**.
c.Agregar la regla: **Direcciones IP de la red** > **Red secundaria de IP**.
d.Como operador, seleccione **igual**.
e.Ingrese la red secundaria que desea filtrar, por ejemplo, 10.1.120.0 (el último número tiene que ser 0 para filtrar todas las direcciones IP de la red secundaria 10.1.120.).
✓ f.Haga clic en **Finalizar** para guardar el grupo.
2. Vaya a **Políticas**.
a.Haga clic en **Nueva política** y **Nombre** la política.
b.En la sección **Configuración**, seleccione **Agente ESET Management**.
c.Realice el cambio en la política, por ejemplo, cambie el **Intervalo de conexión** a 5 minutos.
d.En la sección **Asignar**, haga clic en **Asignar** y seleccione la casilla de verificación junto a su grupo *Red secundaria 120* y haga clic en **Aceptar** para confirmar.
e.Haga clic en **Finalizar** para guardar la política.
Esta política se aplicará en clientes conectados al grupo dinámico a partir de este momento.

Consulte reglas de eliminación de políticas para saber qué ocurre con la configuración de la política aplicada cuando el equipo de cliente deja el grupo dinámico (las condiciones que se ajustan a la membresía del grupo dinámico ya no son válidas).

Consulte otros ejemplos de plantillas de grupos dinámicos.

Administración de licencias

Al comprar una licencia para cualquier producto comercial ESET, automáticamente recibe acceso a ESET PROTECT On-Prem. Puede administrar fácilmente sus licencias mediante ESET PROTECT On-Prem desde el menú principal, en la opción **Más** > **Administración de licencias**.Si ya tiene un nombre usuario y contraseña emitidos por ESET que desea convertir en una clave de licencia, consulte Convertir credenciales de licencia heredadas. El nombre de usuario y la contraseña se reemplazaron por una Clave de licencia/ID público. La Clave de licencia es una cadena única que se usa para identificar al propietario de la licencia y la activación en sí misma.

Puede activar su producto de negocios de ESET usando ESET PROTECT On-Prem.

Consulte también Preguntas frecuentes sobre licencias (usuarios empresariales).

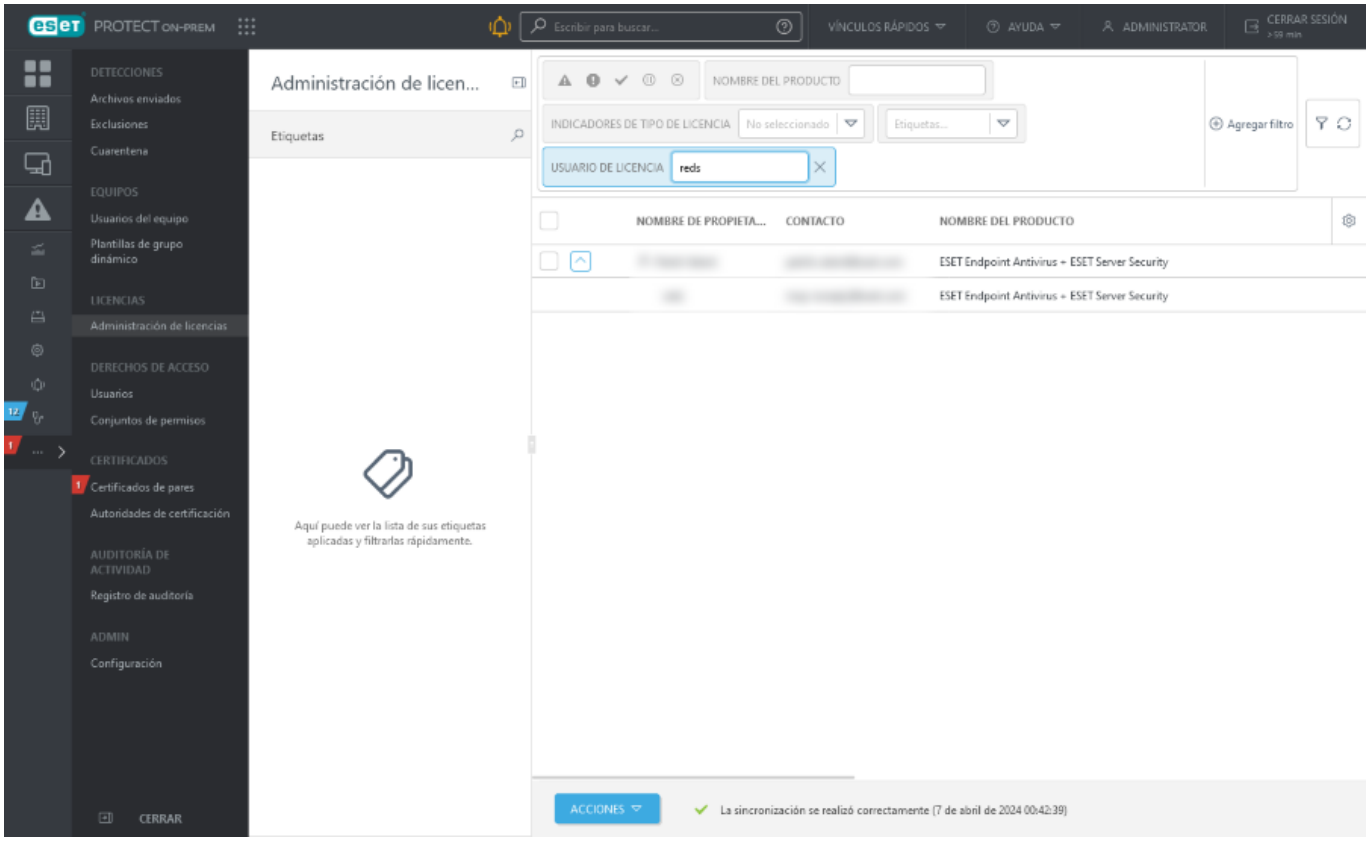
Permisos para la administración de licencias

A cada usuario se le pueden asignar permisos para licencias. Los permisos son válidos solamente para las licencias dentro del grupo estático donde se asigna el conjunto de permisos. Cada tipo de permiso le permite al usuario llevar a cabo diferentes acciones.

Solo los administradores cuyo grupo hogar está configurado en **Todos**, con permisos de **Escritura** para licencias en el grupo hogar pueden agregar o quitar licencias. Cada licencia se identifica con su **ID pública** y puede contener una unidad o más. Solo un administrador puede distribuir licencias a otros usuarios con permisos suficientes. Las licencias no son reducibles.

Las licencias de ESET MSP Administrator 2 se dividen en un conjunto para cada compañía. No puede mover una licencia fuera del grupo.

Administración de licencias en la consola web



Las licencias del mismo usuario ESET Business Account o de la misma empresa se agrupan en conjuntos de licencias. Haga clic en para ampliar el conjunto de licencias y ver los detalles de las licencias.

En ESET Business Account y ESET PROTECT On-Prem, cada licencia se identifica por:

- **ID pública**

- **Tipo de licencia**: **Negocios** (licencia paga), **Prueba** (licencia de prueba), **MSP** (licencia de Proveedor de servicios administrados) y **NFR** (no para el caso de licencia de reventa).

La información adicional sobre la licencia incluye:

- El **nombre del propietario** y el **contacto** de la licencia.

- Nombre y tipo de **usuario de licencia**: **Compañía**, **Sitio**, **Cliente de MSP**.

- El **nombre del paquete** para los que están pensados los productos de ESET. Obtenga más información sobre los niveles de protección de ESET.

- El **nombre del producto** de seguridad para la que está prevista su licencia.

- Estado **de licencia** (si la licencia caducó, se ha utilizado por demás o se encuentra en riesgo de vencerse o sufrir un sobreuso, se mostrará un mensaje de advertencia aquí).

- El número de **Unidades** que se pueden activar con esta licencia y la cantidad de unidades fuera de línea. En el caso de los productos ESET Mail Security, el uso de licencias se calcula en función de las **Subunidades** que se usan para la activación.

- La cantidad de **Subunidades** de los productos del servidor de ESET (buzones de correo, protección de puerta de enlace, conexiones).

• La **validez representa la** fecha de vencimiento de la licencia. Es posible que las licencias de suscripción no tengan fecha de expiración.

Puede filtrar las licencias por su **estado**:

OK: verde	Su licencia está activada exitosamente.
Error(es): rojo	La licencia no está registrada, ha vencido o está sobreusada.
Advertencia(s): naranja	Su licencia todavía está agotada o está a punto de vencer (el vencimiento es en 30 días).
Desactivado o suspendido	Su licencia se desactivó o fue suspendida.
Obsoleto	Su licencia está vencida.

Las licencias vencidas y sobreusadas (en estado **Error** u **Obsoleto**) no están visibles en la lista de licencias disponibles en el asistente del instalador todo en uno, en la tarea del cliente Activación del producto y en la tarea del cliente Instalación del software.

Haga clic en el botón **Acciones** para administrar el(los) conjunto(s) de licencia seleccionado(s):

Etiquetas	Editar etiquetas (asignar, desasignar, crear, quitar).
Agregar licencias	Haga clic en **Agregar licencias** y, luego, seleccione el método que desea usar para agregar sus licencias nuevas: 1.**ESET PROTECT Hub, ESET Business Account o ESET MSP Administrator**: conecte un ESET PROTECT Hub, ESET Business Account o EMA 2 y agregue todas sus licencias a la sección **Administración de licencias**. 2.**Clave de licencia**: ingrese una clave de licencia para una licencia válida y haga clic en **Agregar licencias**. La clave de licencia se verificará frente al servidor de activación y se agregará a la lista. 3.**Archivo de licencia sin conexión**: agregue un archivo de licencia (*.lf*) y haga clic en **Agregar licencia**. El archivo de licencia se verificará y se agregará la licencia a la lista. Puede ver cómo se agregó la licencia en función del ícono en la columna **Nombre de propietario**: **Archivo de licencia sin conexión**, **Clave de licencia** o **ESET PROTECT Hub, ESET Business Account o ESET MSP Administrator**.
Quitar licencias	Quitar el(los) conjunto(s) de licencia seleccionado(s). Se le pedirá que confirme esta acción. La eliminación de la licencia no ejecuta la desactivación del producto. Su producto de ESET permanecerá activado, aún después de que se haya eliminado la licencia en **Gestión de licencias** de ESET PROTECT On-Prem.
Grupo de acceso > **Mover**	Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen derechos suficientes para el grupo de destino. Cambiar el grupo de acceso es útil cuando se resuelven problemas de acceso con otros usuarios. El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario.
Sincronizar licencias	Actualice la información de la licencia en ESET PROTECT On-Prem de inmediato. Las licencias se sincronizan en forma automática una vez por día con los servidores de licencia de ESET. Si utiliza ESET Business Account o ESET MSP Administrator, las licencias se sincronizan de manera automática una vez por día también con estos servicios. Si se produce un error en la sincronización de licencias, asegúrese de que el nombre de host *edf.eset.com* y sus direcciones IP estén permitidos en la red.
Abrir EBA	Abra el portal de ESET Business Account. Esta acción solo está disponible si agregó licencias de ESET Business Account.
Abrir EMA	Abra el portal de ESET MSP Administrator. Esta acción solo está disponible si agregó licencias de ESET MSP Administrator.

Amplíe el conjunto de licencias y haga clic en una licencia para realizar las siguientes acciones. La acción definida depende del tipo de licencia seleccionada:

Licencia del usuario para activación	Ejecute la tarea de activación del producto haciendo uso de esta licencia.
Etiquetas	Editar etiquetas (asignar, desasignar, crear, quitar).
Administrar licencia	Si la licencia está sincronizada desde ESET Business Account o ESET MSP Administrator, puede administrar la licencia. Si la licencia se sobreusa, puede aumentar la capacidad de la licencia o desactivar algunos de sus dispositivos.
Renovar la licencia	Renueve la licencia que expiró, caducó, se suspendió o se desactivó en ESET Business Account o ESET MSP Administrator.
Actualizar licencia	Actualice la licencia de prueba en ESET Business Account o ESET MSP Administrator.
Registro de auditoría	Ver el registro de auditoría del elemento seleccionado.
Copiar ID pública de la licencia	Copie la ID pública de la licencia en el portapapeles.

Licencia de suscripción

ESET PROTECT On-Prem es compatible con la gestión de licencias de suscripción. Puede añadir ese tipo de licencia usando ESET PROTECT Hub, ESET Business Account o ESET MSP Administrator o una Clave de licencia. Puede revisar la validez de su suscripción en **Gestión de licencias** en la columna de **Validez** o en **Equipos** > Detalles. No es posible crear un archivo de licencia sin conexión desde una licencia de suscripción.

Soporte para sitios ESET Business Account

Ahora puede importar la estructura completa de su ESET Business Account, incluida la distribución de puestos de licencias entre sitios.

Activación de productos comerciales ESET

Puede distribuir licencias a productos de ESET desde ESET PROTECT On-Prem a través de dos tareas:

- la Tarea de instalación de software
- la Tarea de activación del producto

Desactivación de los productos comerciales ESET

Puede desactivar el producto comercial ESET (quitar la licencia del producto) de varias maneras a través de la consola web de ESET PROTECT:

- en **Equipos**, seleccione el equipo y la opción **Desactivar productos** - Quitar la licencia de todos los dispositivos seleccionados a través del servidor de licencias ESET. El producto se desactiva incluso si no se activó desde ESET PROTECT On-Prem o la licencia no la administra ESET PROTECT On-Prem.

> Si selecciona un solo equipo con más productos ESET instalados (por ejemplo, producto de terminal ESET y Connector de ESET Inspect), puede seleccionar la opción para desactivar productos individuales.

- Eliminar equipo de administración

- Cree la tarea Quitar equipos sin conexión con la opción **Desactivar licencia**.

Personalización del diseño y de los filtros

Puede personalizar la vista de la pantalla de la consola web actual:

- Administre el panel lateral y la tabla principal.
- Agregar filtro y filtros preestablecidos. Puede usar etiquetas para filtrar los elementos mostrados.

Compartir licencias entre administradores de sucursales

Hay tres usuarios y un Administrador, cada uno con su propio grupo hogar:
• *John*, *San Diego*
• *Larry*, *Sídney*
• *Makio*, *Tokio*
El administrador importa 3 licencias. Estas se encuentran dentro del grupo estático Todos y otros usuarios no pueden usarlas.
Para asignar una licencia a otro usuario, el administrador puede hacer seleccionar la casilla de verificación ubicada junto al conjunto de licencia al que quiere asignar a otro usuario y luego en el botón **Acciones**, después en Grupo de acceso **>** **Mover** y seleccionar el grupo en el cual el usuario tiene permiso. Para el usuario *John*, seleccione el grupo *San Diego*. *John* necesita permisos de Uso para **Licencias** en el grupo *San Diego* para usar la licencia.
Cuando el usuario *John* inicia sesión, únicamente puede ver y usar la licencia que se ha movido a su grupo. El administrador debe repetir el proceso para *Larry* y *Makio*; luego, los usuarios solo pueden ver su licencia, mientras que el administrador puede ver todas.

ESET PROTECT Hub, ESET Business Account o ESET MSP Administrator

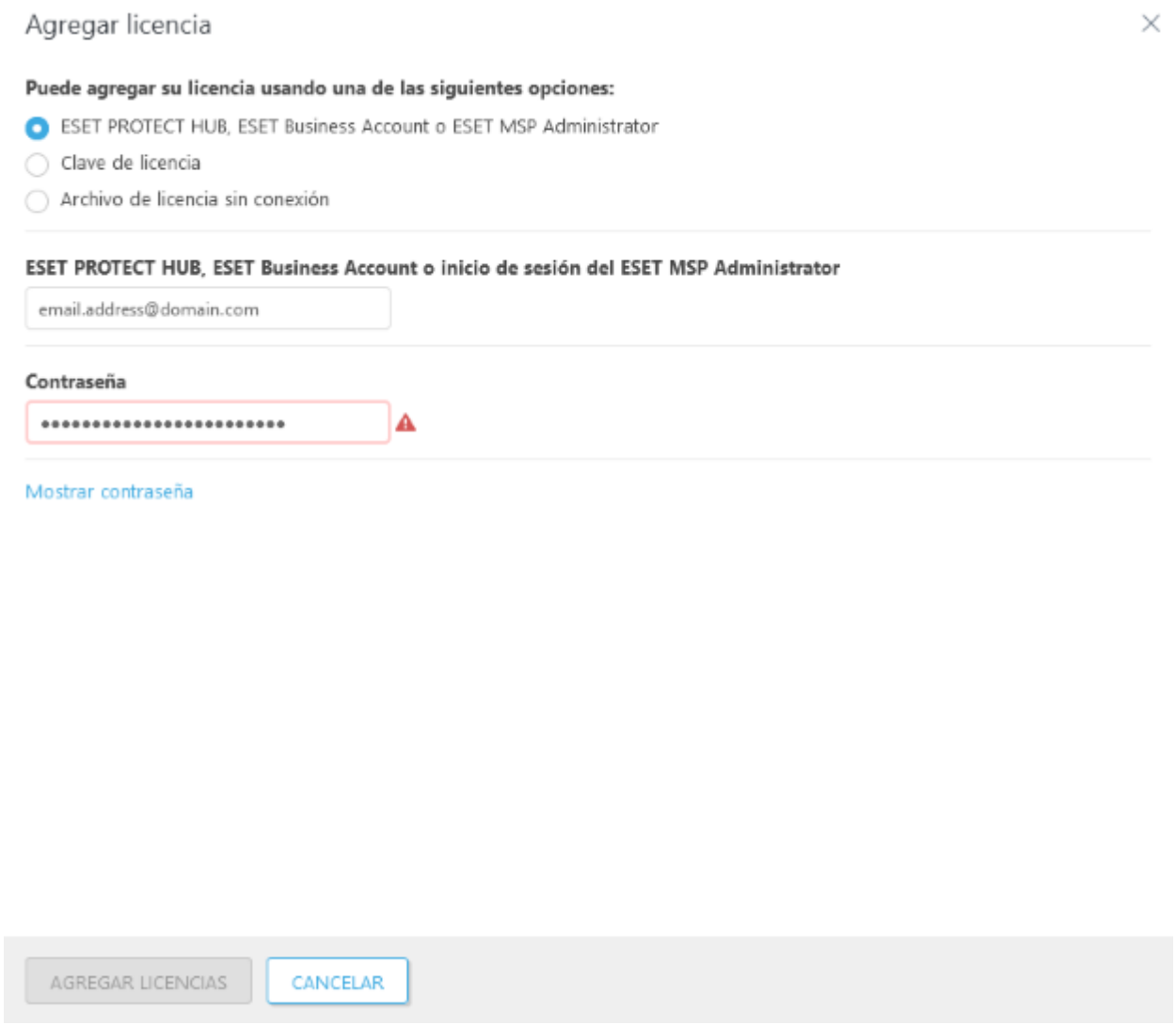
Solo los administradores cuyo grupo hogar está configurado en **Todos**, con permisos de **Escritura** para licencias en el grupo hogar pueden agregar o quitar licencias. Cada licencia se identifica con su **ID pública** y puede contener una unidad o más. Solo un administrador puede distribuir licencias a otros usuarios con permisos suficientes. Las licencias no son reducibles.

ESET Business Account o ESET MSP Administrator

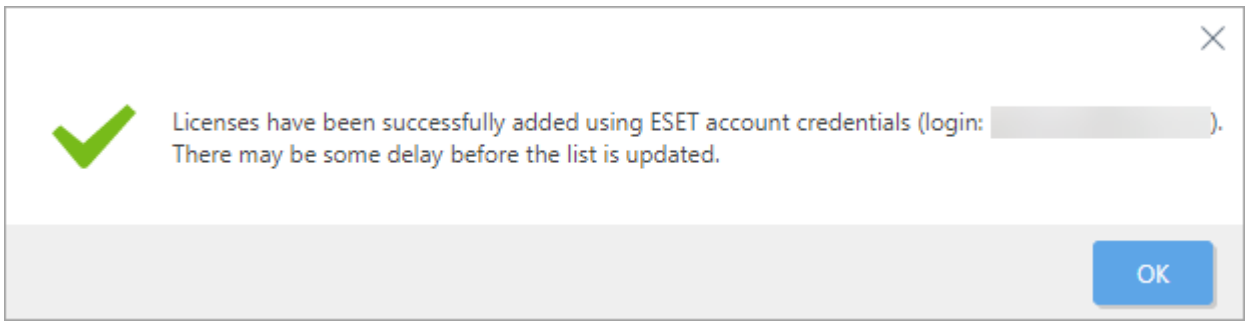
1. Haga clic en **Más** > **Administración de licencias** > **Licencia** > **Agregar licencia**.

2. Seleccione **ESET PROTECT Hub, ESET Business Account o ESET MSP Administrator**.

3. Ingrese las 2 credenciales de ESET PROTECT Hub, ESET Business Account o ESET MSP Administrator (ESET PROTECT On-Prem mostrará todas las licencias delegadas en administración de licencias de ESET PROTECT On-Prem).



4. Haga clic en **Agregar licencias** para confirmar.



5. ESET PROTECT On-Prem sincronizará su estructura ESET Business Account o ESET MSP Administrator con el Árbol de grupos estáticos en **Equipos** en la consola web.

Si se produce un error en la sincronización de licencias, asegúrese de que el nombre de host *edf.eset.com* y sus direcciones IP estén permitidos en la red.

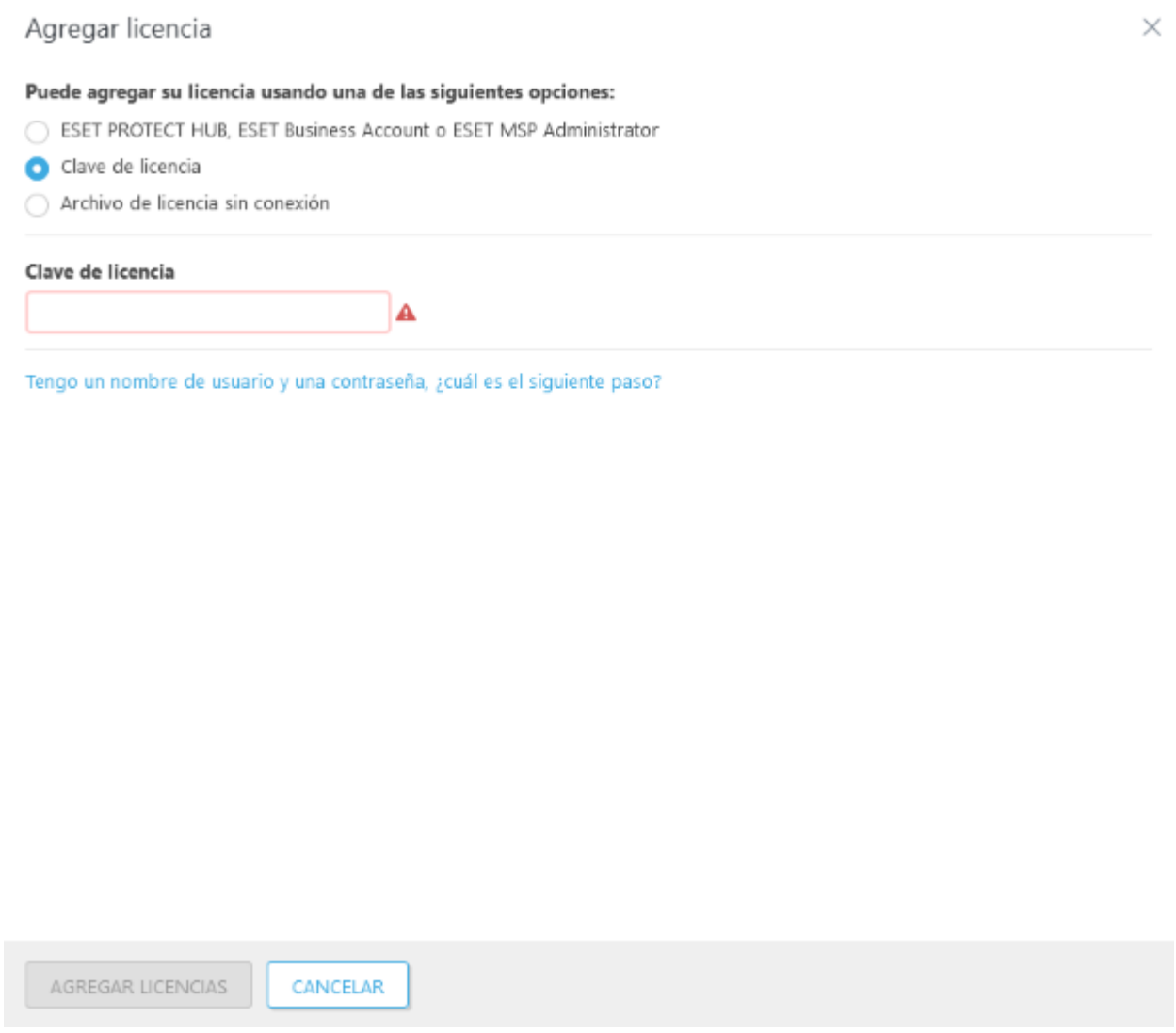
Agregar licencia - Clave de licencia

Solo los administradores cuyo grupo hogar está configurado en **Todos**, con permisos de **Escritura** para licencias en el grupo hogar pueden agregar o quitar licencias. Cada licencia se identifica con su **ID pública** y puede contener una unidad o más. Solo un administrador puede distribuir licencias a otros usuarios con permisos suficientes. Las licencias no son reducibles.

Clave de licencia

Escriba o copie y pegue la **Clave de licencia** que recibió cuando compró su solución de seguridad de ESET en el campo **Clave de licencia** y haga clic en **Agregar licencias**.

Si usa credenciales de la licencia de legado (un Nombre de usuario y contraseña), convierta las credenciales en una clave de licencia. Si la licencia no se ha registrado, se activará el proceso de registro, que se realiza en el portal de EBA (ESET PROTECT On-Prem le proporcionará una URL válida para continuar con el registro según el origen de la licencia).



Activación sin conexión

Puede usar un archivo de licencia del portal de ESET Business Account para activar ESET PROTECT On-Prem y otros productos de seguridad ESET.

- Cada archivo de licencia sin conexión se genera para un solo producto, por ej. ESET Endpoint Security.

- La licencia sin conexión se usará solo para clientes que nunca tendrán acceso a los servidores de Licencia de ESET (aún si un cliente está conectado a Internet a través de un proxy con acceso limitado a servicios de ESET, no usar una licencia sin conexión).

- No es posible crear un archivo de licencia sin conexión desde una licencia de suscripción.

Para reemplazar una licencia sin conexión, debe

1. Quitar la licencia anterior en ESET PROTECT On-Prem y el archivo de licencia en ESET Business Account.

2. Crear una nueva licencia sin conexión en ESET Business Account.
3. Importar la licencia nueva a ESET PROTECT On-Prem

4. Reactivar los productos con la licencia nueva.

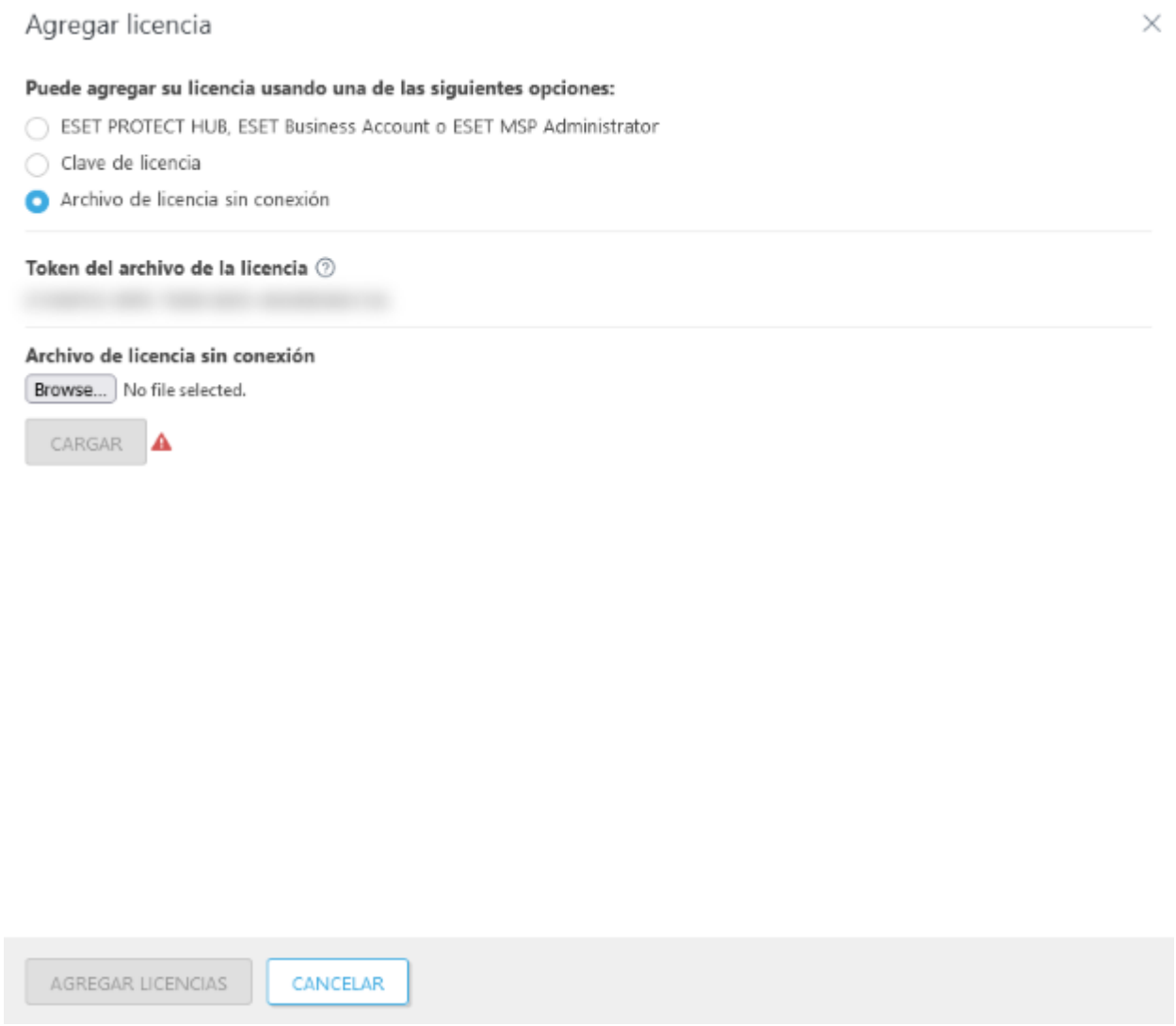
Solo los administradores cuyo grupo hogar está configurado en **Todos**, con permisos de **Escritura** para licencias en el grupo hogar pueden agregar o quitar licencias. Cada licencia se identifica con su **ID pública** y puede contener una unidad o más. Solo un administrador puede distribuir licencias a otros usuarios con permisos suficientes. Las licencias no son reducibles.

Archivo de licencia sin conexión

Para crear e importar un archivo de licencia sin conexión, siga este proceso:

1. Abra el **Administrador de licencias** de ESET PROTECT On-Prem y haga clic en **Acciones** > **Agregar licencias**.

2. Seleccione **Archivo de licencia sin conexión** y copie un **Token de archivo de licencia** específico.

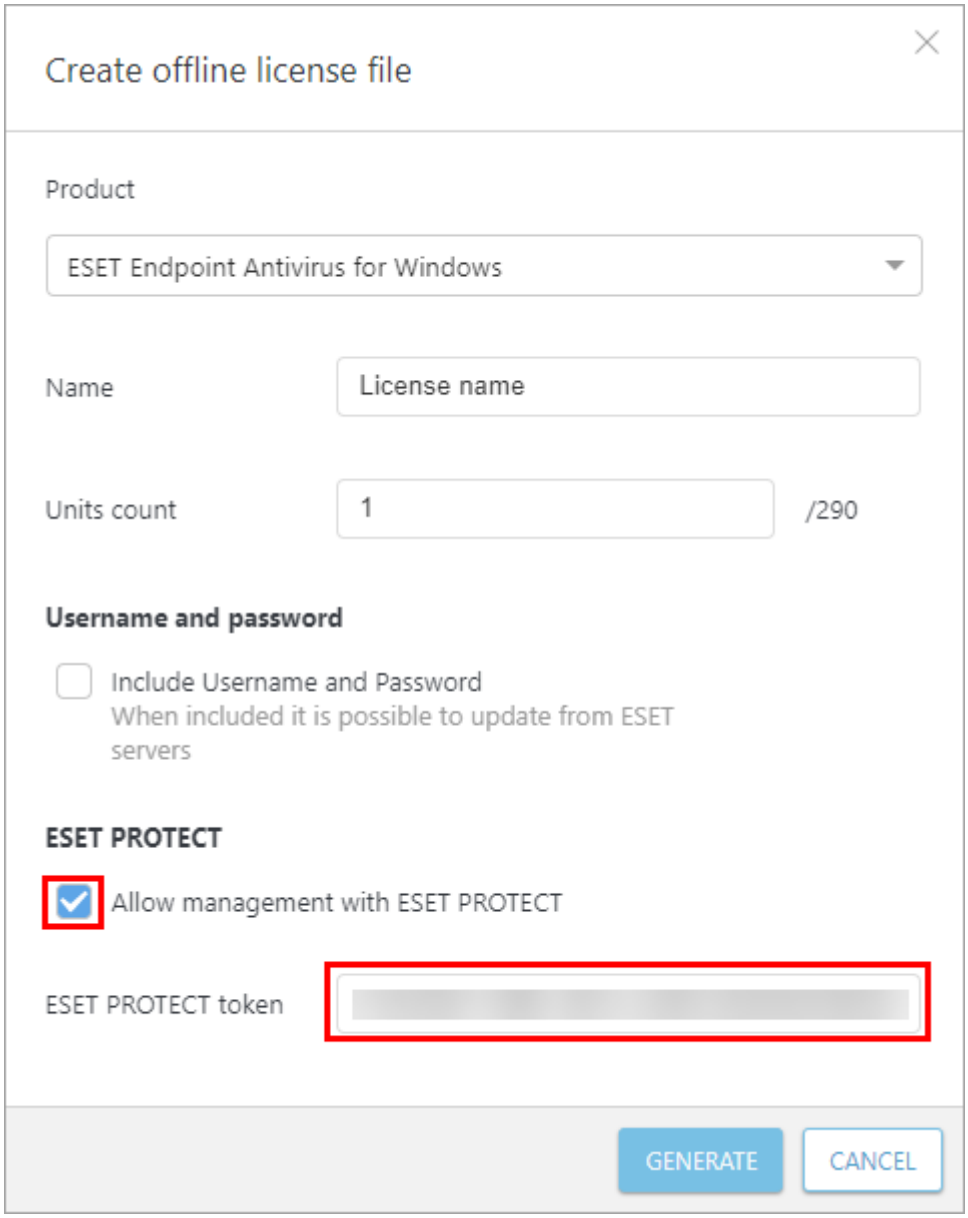


3.Inicie sesión en su ESET Business Account donde importó su licencia.

4.Seleccione la licencia que quiere exportar y seleccione **Crear archivo sin conexión**.

5.Seleccione un producto para este archivo de licencia, ingrese el **Nombre** del archivo y el **Recuento de unidades** (número de puestos exportados al archivo de licencia).

6.Seleccione la casilla de verificación junto a **Permitir administración con ESET PROTECT On-Prem** e ingrese el token de **ESET PROTECT On-Prem** (**token de archivo de licencia** de ESET PROTECT On-Prem).



7.Haga clic en **Generar**.

Para descargar el archivo siga este procedimiento:

1.Seleccione la licencia y haga clic en **Mostrar detalles**.

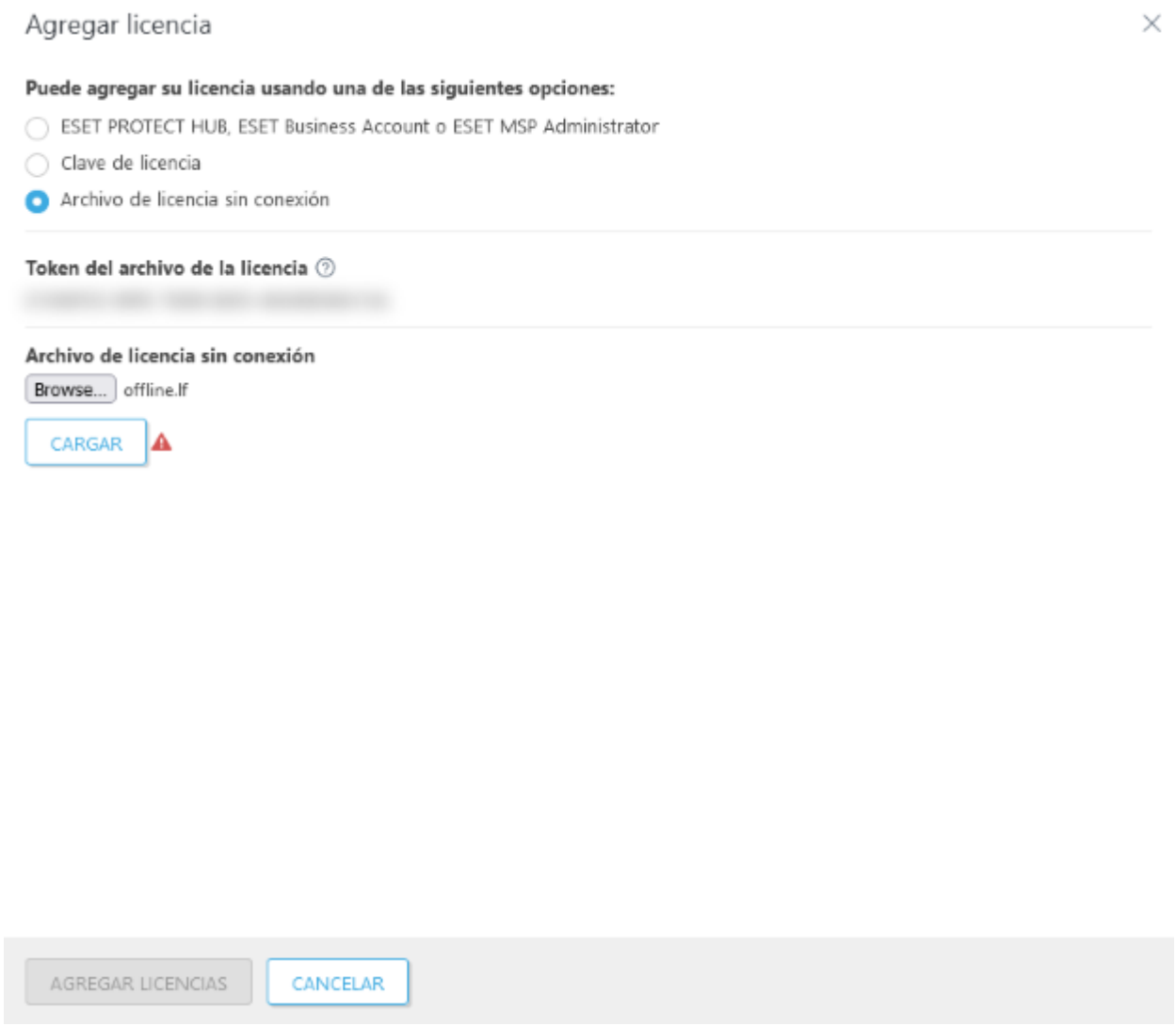
2.Seleccionar la pestaña **Archivos sin conexión**.

3.Haga clic en el archivo de licencia que creó, puede distinguirlo por el nombre y seleccione **Descargar**.

Vaya a **Administración de licencias** de ESET PROTECT On-Prem:

1.Haga clic en **Elegir archivo** y seleccione el archivo de licencia sin conexión que ha exportado en ESET Business Account.

2.Haga clic en **Cargar** y, luego, en **Agregar licencias**.



Derechos de acceso

Los derechos de acceso le permiten administrar los usuarios y los permisos de la consola web de ESET PROTECT.

El modelo de seguridad

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

Término	Explicación
Grupo hogar	El grupo hogar es aquel en el que todos los objetos (dispositivos, tareas, plantillas, etc.) que crea un usuario se almacenan automáticamente. Cada usuario debe contar con solo con un grupo hogar.
Objeto	Los objetos se ubican en **Grupos estáticos**. El acceso a los objetos se realiza por grupos, no usuarios (al proporcionar acceso por grupo, es más fácil acomodar varios usuarios, por ejemplo, si un usuario está de vacaciones). Las excepciones incluyen tareas del servidor y notificaciones que requieren un usuario "ejecutador".
Grupo de acceso	El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario.
Administrador	Un usuario que tiene un grupo hogar **Todos** y un conjunto de permisos completos sobre el grupo es efectivamente un administrador.
Derecho de acceso	El derecho de acceder a un objeto o de ejecutar una tarea se asigna con un conjunto de permisos. Para más información, consulte la lista de todos los derechos de acceso y sus funciones.
Conjunto de permisos	Un conjunto de permisos representa los permisos para usuarios que acceden a la consola web ESET PROTECT. Definen qué puede hacer o ver un usuario dentro de la consola web ESET PROTECT. Se le puede asignar diferentes conjuntos de permisos a un mismo usuario. Los conjuntos de permisos solo se aplican sobre objetos en grupos definidos. Estos **grupos estáticos** se configuran en la sección **Grupos estáticos** al crear o editar un conjunto de permisos.
Funcionalidad	Una funcionalidad es un tipo de objeto o acción. Por lo general, las funcionalidades obtienen estos valores: **Lectura**, **Escritura**, **Uso**. La combinación de funcionalidades aplicadas a un grupo de acceso se denomina conjunto de permisos.

Lista de ejemplos relacionados a los derechos de acceso

En la guía de administración se incluyen diferentes ejemplos con respecto a los derechos de acceso. Esta es una lista de ellos:

- Cómo duplicar políticas
- Diferencia entre Uso y Escritura
- Cómo crear una solución para administradores de sucursales
- Cómo compartir objetos a través de la duplicación
- Cómo dividir el acceso a certificados y autoridades
- Cómo permitir a un usuario crear instaladores
- Cómo eliminar las notificaciones
- Cómo crear políticas
- Permitir a los usuarios ver todas las políticas
- Compartir licencias entre administradores de sucursales

Usuarios

La administración de usuarios es parte de la sección **Más** de la consola web ESET PROTECT.

- Crear un Usuario nativo
- Acciones del usuario y detalles del usuario
- Cambiar contraseña de usuario
- Usuarios asignados
- Asignar un conjunto de permisos a un usuario

Hay dos tipos de usuario:

- Usuarios nativos: cuentas de usuarios creadas y administradas desde la consola web ESET PROTECT.
- Grupos de seguridad de dominio asignado: cuentas de usuario administradas y autenticadas por Active Directory.

Una configuración de ESET PROTECT On-Prem nueva tiene el **Administrador** (Usuario nativo con el grupo hogar **Todos** y acceso a todo) como el único usuario.
• No recomendamos que use esta cuenta de usuario regularmente. Le aconsejamos que cree otra cuenta de “administrador” o use Administradores de los grupos de seguridad de dominio asignado con el Conjunto de permisos del administrador asignado a ellos. Use la cuenta de administrador predeterminada solo como una opción de respaldo.
• Además, puede crear usuarios adicionales con derechos de acceso más estrechos basados en sus competencias deseadas.
• En forma optativa, puede establecer una Autenticación de dos factores para Usuarios Nativos y Grupos de seguridad de domino asignado. Esto aumentará la seguridad al iniciar sesión y acceder a la consola web ESET PROTECT.

Solución para admins de sucursal

Si una empresa tiene dos oficinas, cada una con admins locales, necesitan tener asignados más conjuntos de permisos para diferentes grupos.
Supongamos que tenemos los admins *John* en *San Diego* y *Larry* en *Sídney*. Ambos necesitan ocuparse solamente de sus equipos locales, usar **Tablero, Políticas, Informes** y **Plantillas de grupos dinámicos** con sus equipos. El *Administrador*central debe seguir estos pasos:
1.Crear nuevos Grupos estáticos: *Oficina de San Diego*, *Oficina de Sídney.*
2.Crear nuevos Conjuntos de permisos:
a)**Conjunto de permisos** llamado *Conjunto de permisos Sídney*, con el grupo estático *Oficina de Sídney* y con permisos de acceso completo (excluye **Configuración del servidor**).
b)**Conjunto de permisos** llamado *Conjunto de permisos San Diego*, con el grupo estático *Oficina de San Diego* y con permisos de acceso completo (excluye **Configuración del servidor**).
c)**Conjunto de permisos** llamado *Grupo Todos/Tablero* con el grupo estático *Todos* y los siguientes permisos:

- **Lectura** para **Tareas del cliente**
- **Uso** para **Plantillas de grupo dinámico**
- **Uso** para **Informes y tablero**
- **Uso** para **Políticas**
- **Uso** para **Enviar correos electrónicos**
- **Uso** para **Enviar captura SNMP**
- **Uso** para **Exportar informe a archivo**
- **Uso** para **Licencias**
- **Escritura** para **Notificaciones**

3.Cree un nuevo usuario *John* con el grupo de pertenencia *Oficina de San Diego*, asignado con los conjuntos de permisos *Conjunto de permisos de San Diego* y *Grupo Todos/Tablero*.
4.Crear un nuevo usuario *Larry* con grupo hogar *Oficina de Sídney,* con el conjunto de permisos asignado *Conjunto de permisos de Sídney* y *Grupo Todos/Tablero*.
Si los permisos se configuran de esta forma, *John* y *Larry* pueden utilizar las mismas tareas y políticas, informes y tablero, y plantillas de grupo dinámico sin restricciones. Sin embargo, cada uno solo puede utilizar las plantillas para los equipos dentro de sus grupos hogar.

Compartir objetos

Si un administrador desea compartir objetos, como plantillas de grupo dinámico, plantillas de informe o políticas, cuenta con las siguientes opciones para hacerlo:

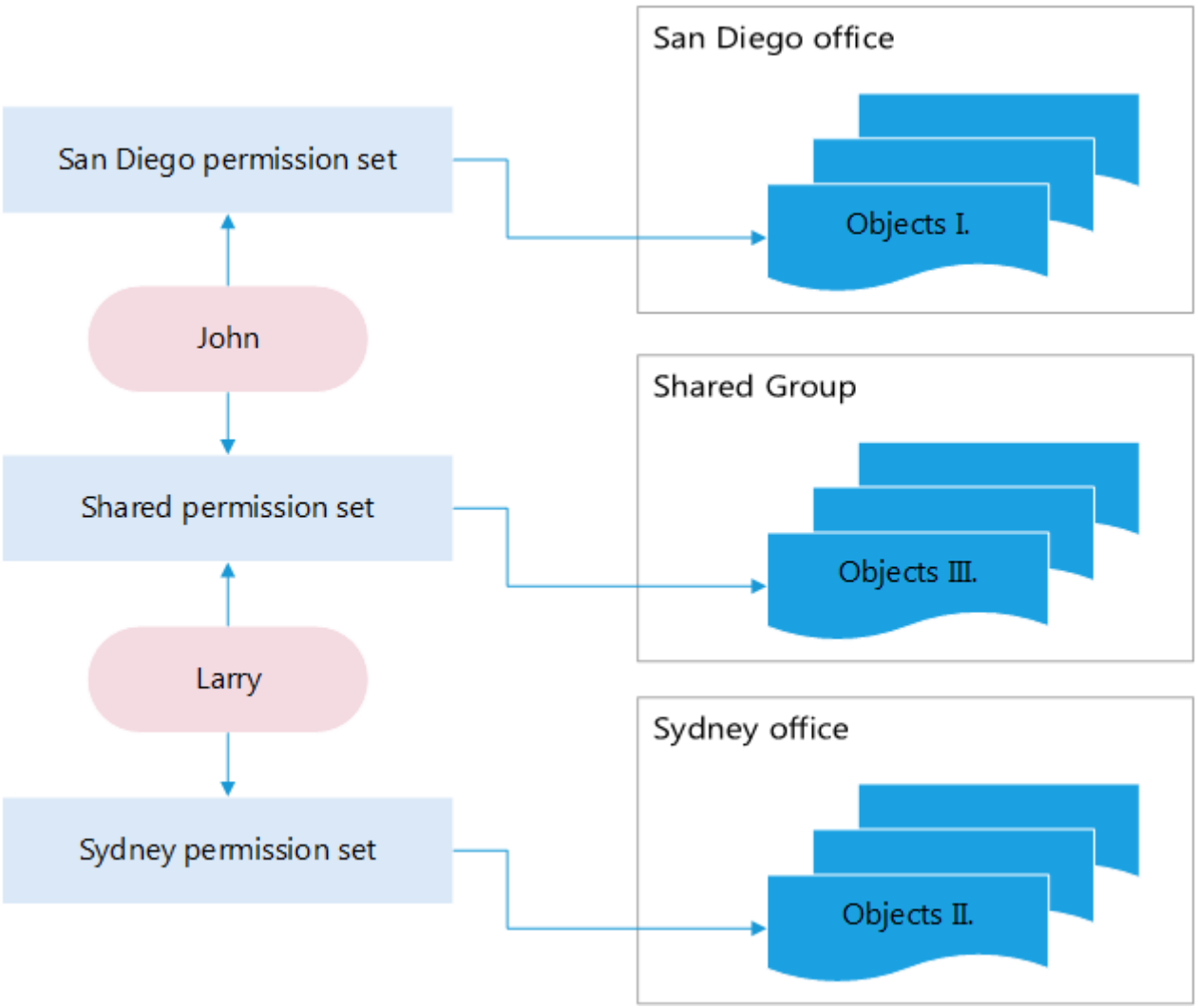
- Mover los objetos a grupos compartidos

- Crear objetos duplicados y moverlos a grupos estáticos que sean accesibles para otros usuarios (a continuación se presentan ejemplos)

Para duplicar un objeto, el usuario necesita contar con permisos de **Lectura** sobre el objeto original y permisos de **Escritura** sobre su **Grupo hogar** para este tipo de acción.
El *Administrador*, cuyo grupo hogar es *Todos,* desea compartir *Plantilla especial* con el usuario *John*. La plantilla fue creada originalmente por el *Administrador*, por lo que automáticamente es parte del grupo *Todos*. El *Administrador* seguirá estos pasos:
1.Irá a **Más** > **Plantillas de grupo dinámico**.
2.Seleccionará la *Plantilla especial* y hará clic en **Duplicar**, de ser necesario, configurará el nombre y la descripción, y hará clic en **Finalizar**.
3.La plantilla duplicada estará dentro del grupo hogar del *Administrador*, grupo *Todos*.
4.Irá a **Más** > **Plantillas de grupo dinámico** y seleccionará la plantilla duplicada, hará clic en **Grupo de acceso** > **Mover** y seleccionará el grupo estático de destino (donde *John* tiene permisos). Haga clic en **OK**.

Cómo compartir objetos entre usuarios a través de un Grupo compartido

Para comprender mejor cómo funciona el nuevo modelo de seguridad, consulte el siguiente esquema. Existe una situación donde el administrador creó dos usuarios. Cada uno cuenta con su propio grupo hogar con los objetos que él creó. El *Conjunto de permisos de San Diego* le otorga a *John* permisos para manipular *Objetos* en su grupo hogar. La situación es similar para *Larry*. Si estos usuarios necesitan compartir algunos objetos (por ejemplo, equipos), estos deben moverse a *Grupo compartido* (un grupo estático). Ambos usuarios deben tener un *conjunto de permisos compartidos* que cuenta con *Grupo compartido* dentro de la sección de **Grupos estáticos**.



Personalización del diseño y de los filtros

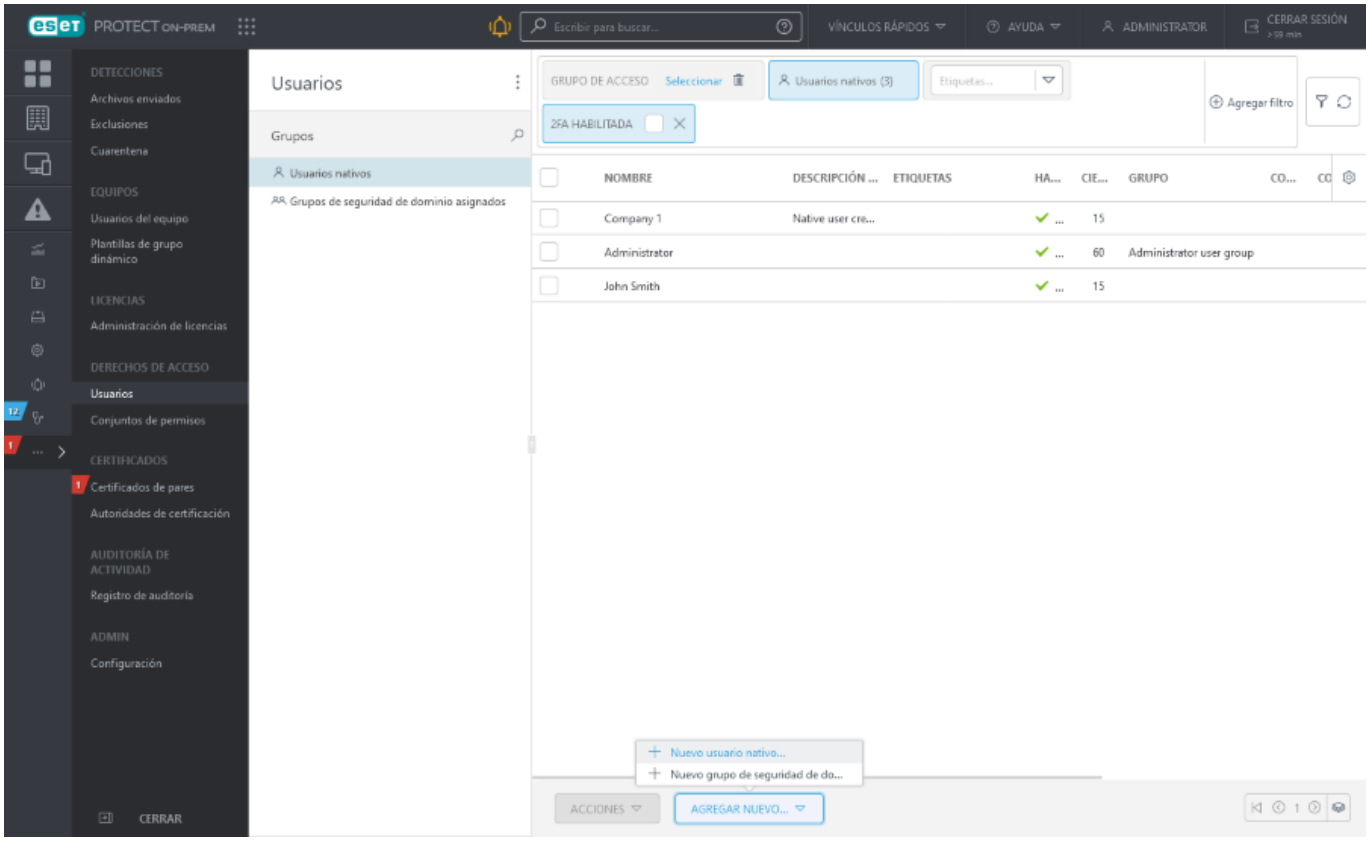
Puede personalizar la vista de la pantalla de la consola web actual:

- Agregar filtro y filtros preestablecidos.
- Puede usar etiquetas para filtrar los elementos mostrados.

Crear un Usuario nativo

Para crear un nuevo usuario nativo, haga clic en **Más** > **Usuarios** > **Agregar nuevo** > **Nuevo usuario nativo**.

> Para crear un usuario adecuadamente, recomendamos que siga estos pasos:
> 1.Decidir qué grupo estático será el grupo hogar del usuario. De ser necesario, crear el grupo.
> 2.Decidir cuál es el mejor conjunto de permisos para el usuario. De ser necesario, crear un nuevo conjunto de permisos.
> 3.Seguir este capítulo y crear el usuario.



Básica

Ingrese un **Nombre** y **Descripción** opcional para el nuevo usuario.

Haga clic en **Seleccionar etiquetas** para asignar etiquetas.

Seleccione **Grupo hogar**. Este es un grupo estático donde todos los objetos creados por el usuario se incluirán automáticamente.

Grupo de pertenencia: el grupo de pertenencia se detecta automáticamente según el conjunto de permisos

asignado del usuario activo en ese momento.

> Situación de ejemplo:
> La cuenta de usuario activa actualmente tiene el derecho de acceso de **Escritura** para la **tarea del cliente Instalación del software** y el **grupo de pertenencia** de la cuenta de usuario es "Department_1". Cuando el usuario cree una nueva **tarea del cliente Instalación del software**, se seleccionará automáticamente "Department_1" como **grupo de pertenencia** de la tarea del cliente.

Si el grupo de pertenencia seleccionado previamente no cumple con sus expectativas, podrá seleccionar el grupo de pertenencia de forma manual.

Establecer contraseña

La contraseña para el usuario debe tener al menos 8 caracteres. La contraseña no debe contener el nombre de usuario.

Cuenta

Habilitado: seleccione esta opción salvo que desee que la cuenta esté inactiva (previsto para uso posterior).

Se debe cambiar la contraseña: seleccione esta opción para forzar al usuario a cambiar su contraseña la primera vez que inicie sesión en la consola web de ESET PROTECT.

Expiración de la contraseña (días): esta opción define la cantidad de días durante los cuales la contraseña es válida (tras su vencimiento, es necesario cambiarla).

Cerrar sesión automáticamente (min): esa opción define el período de tiempo de inactividad (en minutos), luego del cual se cierra la sesión del usuario en la Consola web. Escriba **0** (cero) para desactivar el cierre de sesión automático del usuario.

Se puede definir el **Nombre completo**, el **Correo de contacto** y el **Teléfono de contacto** para ayudar a identificar al usuario.

Conjuntos de permisos

Puede asignar varios conjuntos de permisos a un usuario.

Puede elegir una competencia predefinida (de la lista de abajo), o bien, usar un conjunto de permisos personalizado.

- **Conjunto de permisos de revisor** (derechos de solo lectura para e grupo **Todo**)
- **Conjunto de permisos de administrador** (acceso completo al grupo **Todo**).
- **Conjunto de permisos de instalación asistida por servidor** (se necesita derechos de acceso mínimos para la instalación asistida por servidor)
- **Conjunto de permisos del revisor de ESET Inspect**: derechos de acceso mínimos de solo lectura (para el grupo **Todo**) necesarios para un usuario de ESET Inspect On-Prem.
- **Conjunto de permisos de servidor de ESET Inspect**: derechos de acceso (para el grupo **Todo**) necesarios

para el proceso de instalación de ESET Inspect On-Prem y otra sincronización automática entre ESET Inspect On-Prem y ESET PROTECT On-Prem.

- **Conjunto de permisos del usuario de ESET Inspect**: derechos de acceso de escritura (para el grupo **Todo**) necesarios para un usuario de ESET Inspect On-Prem.

Cada grupo de permisos otorga permiso únicamente para los objetos dentro de los **Grupos estáticos** seleccionados en el grupo de permisos.

Los usuarios sin ningún conjunto de permisos no podrán iniciar sesión en la consola web.

Todos los permisos predefinidos tienen el grupo **Todos** en la sección **Grupos estáticos**. Tenga esto en cuenta al asignarlo a un usuario. Los usuarios tendrán estos permisos sobre todos los objetos en ESET PROTECT On-Prem.

Resumen

Revise los ajustes configurados para este usuario y haga clic en **Finalizar** para crear el usuario.

Acciones del usuario y detalles del usuario

Para administrar un usuario, seleccione el usuario aplicable y una de las acciones disponibles:

Acciones

- **Mostrar detalles**: ver los detalles del usuario.
- **Registro de auditoría**: vea el registro de auditoría para todos los usuarios.
- **Registro de auditoría para usuario seleccionado**: vea el registro de auditoría para el usuario seleccionado.
- **Etiquetas** - Editar etiquetas (asignar, desasignar, crear, quitar).
- **Asignar conjuntos de permisos**: asignar un conjunto de permisos a un usuario.
- **Editar**: editar la configuración del usuario.
- **Quitar**: quita al usuario.

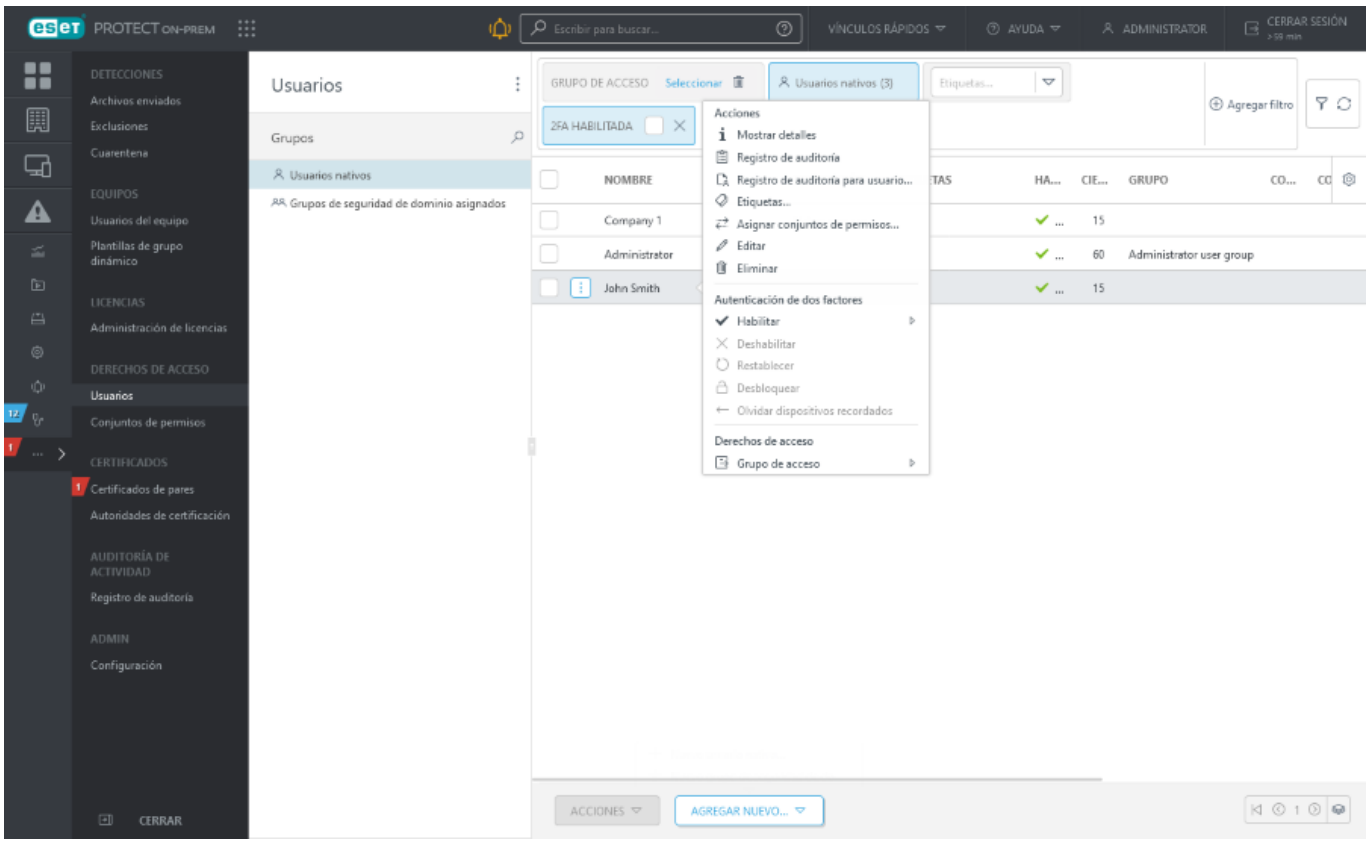
Autenticación de dos factores

- **Habilitar**: habilitar la autenticación de dos factores para el usuario.
- **Deshabilitar**: deshabilitar la autenticación de dos factores existente para el usuario.
- **Restablecer**: restablecer la configuración de la autenticación de dos factores para el usuario.
- **Desbloquear**: si el usuario se ha bloqueado, puede desbloquearlo con esta configuración.
- **Olvidar dispositivos recordados**: requiere la autenticación de dos factores en los dispositivos

recordados del usuario.

Derechos de acceso

- **Grupo de acceso** > **Mover** – Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen derechos suficientes para el grupo de destino. Cambiar el grupo de acceso es útil cuando se resuelven problemas de acceso con otros usuarios. El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario.



Detalles de usuario

Hay dos secciones en los detalles del usuario:

- **Descripción general**: información básica sobre el usuario. Puede administrar el usuario con los botones **Acciones** y **Autenticación de dos factores** situados en la parte inferior.

- **Conjuntos de permisos**: lista de conjuntos de permisos asignados al usuario. Haga clic en un conjunto de permisos para administrarlo.

Cambiar contraseña de usuario

Puede cambiar la contraseña para cualquier usuario respecto del cual tenga derechos de acceso. Debe tener permisos de escritura para el grupo estático en el que está almacenado el usuario. El usuario está almacenado en el grupo hogar del usuario principal.

1. Haga clic en **Más** > **Usuarios**.

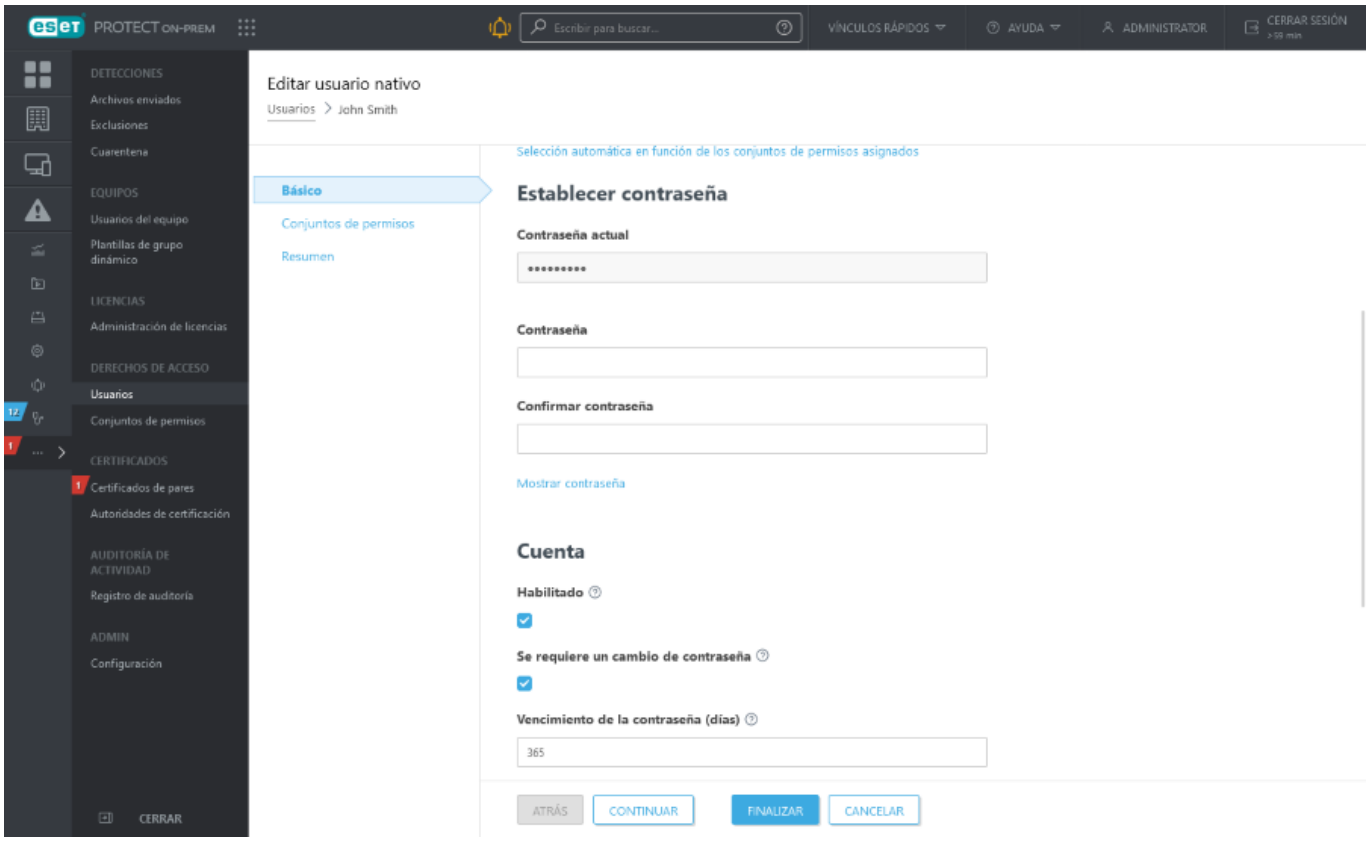
2. Seleccione el usuario y haga clic en **Editar**.

3. En la sección **Básica**, desplácese hasta **Definir contraseña**.

4. Si está editando el usuario que ha iniciado sesión, debe introducir la **contraseña actual**. Cuando se editan otros usuarios, el campo **Contraseña actual** se completa previamente.

5. Introduzca la nueva contraseña en el campo **Contraseña** y **Confirmar contraseña**.

6. Haga clic en **Finalizar**.

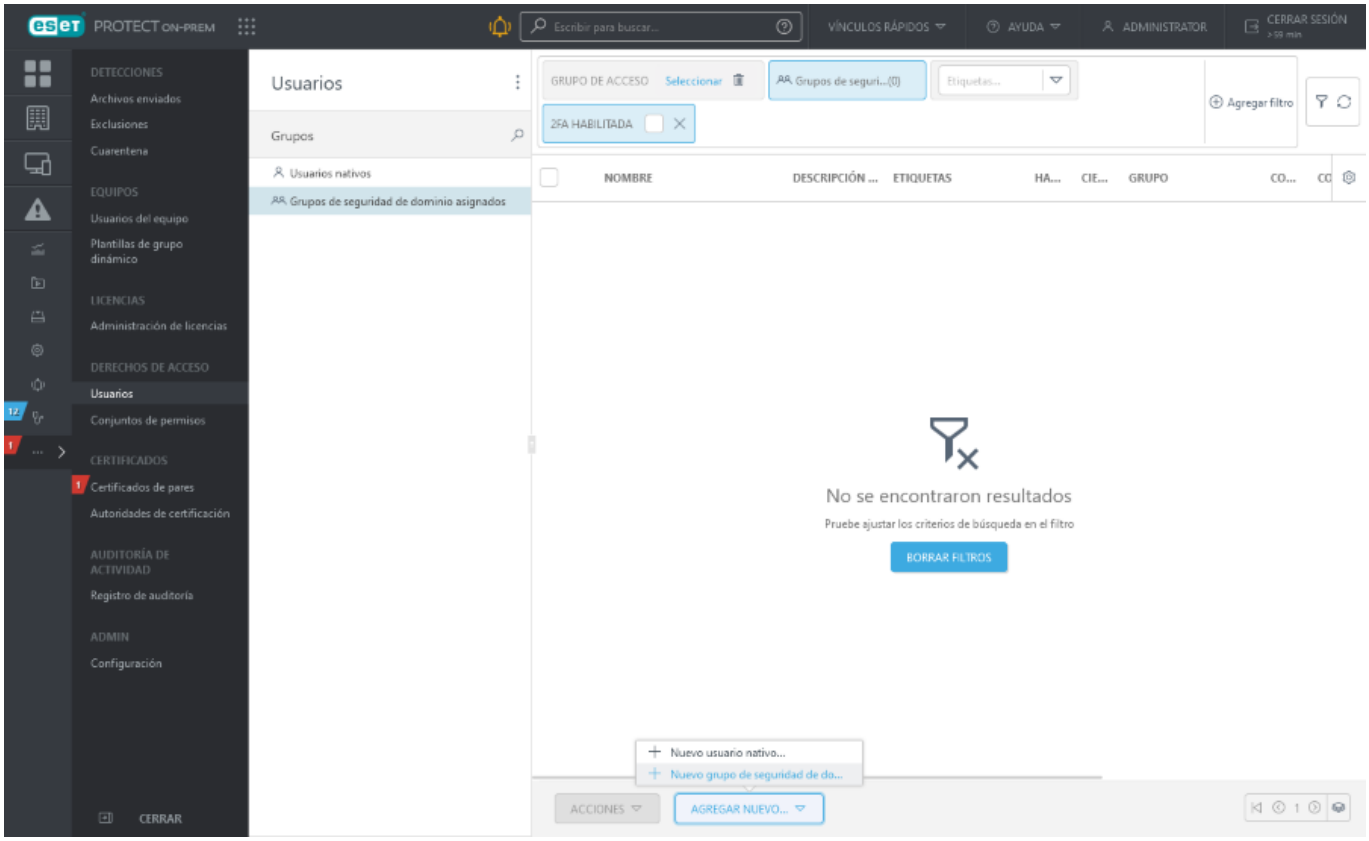


Asignar usuarios de grupo de seguridad de dominio

Puede asignar un grupo de seguridad de dominio al servidor ESET PROTECT y, así, permitir que los usuarios existentes (miembros de estos grupos de seguridad de dominio) se conviertan en usuarios de la consola web ESET PROTECT.

Esta característica está disponible únicamente para sistemas con Active Directory.

Para acceder al **Asistente de grupo de seguridad de dominio asignado**, ingrese en **Más** > **Usuarios** > **Agregar nuevo** > **Nuevo grupo de seguridad de dominio asignado**.



Básica

Grupo de dominio

Ingrese un **nombre** para la política. También puede escribir una **descripción** del grupo.

Haga clic en **Seleccionar etiquetas** para asignar etiquetas.

Seleccione **Grupo hogar**. Este es un grupo estático donde todos los objetos creados por los usuarios dentro del grupo de dominio se incluirán automáticamente.

Grupo de pertenencia: el grupo de pertenencia se detecta automáticamente según el conjunto de permisos asignado del usuario activo en ese momento.

> Situación de ejemplo:
> La cuenta de usuario activa actualmente tiene el derecho de acceso de **Escritura** para la **tarea del cliente Instalación del software** y el **grupo de pertenencia** de la cuenta de usuario es "Department_1". Cuando el usuario cree una nueva **tarea del cliente Instalación del software**, se seleccionará automáticamente "Department_1" como **grupo de pertenencia** de la tarea del cliente.

Si el grupo de pertenencia seleccionado previamente no cumple con sus expectativas, podrá seleccionar el grupo de pertenencia de forma manual.

Este grupo de dominio se definirá por un **SID del grupo** (identificador de seguridad). Haga clic en **Seleccionar** para elegir un grupo de la lista y, luego, en **Aceptar** para confirmar. Su servidor ESET PROTECT debe participar en un dominio; de lo contrario, no habrá grupos en la lista. Si utiliza Aparato virtual, consulte el capítulo relacionado.

- Si LDAPS no está disponible, puede asignar el grupo de seguridad de dominio mediante:
  - la desactivación temporal de la configuración de Active Directory en **Más** > Configuración > **Configuración avanzada** > **Active Directory**.
  - la escritura manual del SID del grupo.
- Si sigue recibiendo un mensaje de error luego de hacer clic en Seleccionar y AD está bien configurado, es posible que el proceso en segundo plano esté desactualizado. Puede hacer lo siguiente:
  - Introducir SID en forma manual para evitar este problema
  - Ingresar sus credenciales de AD en **Más** > Configuración > **Configuración avanzada** > **Active Directory**. ESET PROTECT On-Prem utiliza otra manera más rápida de recuperar la lista de SID.

Cuenta

Habilitado: seleccione esta opción salvo que desee que la cuenta esté inactiva (previsto para uso posterior).

Cerrar sesión automáticamente (min): esa opción define el período de tiempo de inactividad (en minutos), luego del cual se cierra la sesión del usuario en la Consola web.

Se puede definir el **Correo de contacto** y el **Teléfono** de contacto para ayudar a identificar al usuario.

Conjuntos de permisos

Asigne competencias (derechos) para los usuarios de este grupo.

Los conjuntos de permisos se configuran para el grupo de seguridad de dominio Active Directory (en lugar de para usuarios individuales, como en el caso de un **Usuario nativo**).

Puede asignar varios conjuntos de permisos a un grupo de seguridad de dominio.

Puede elegir una competencia predefinida (de la lista de abajo), o bien, usar un conjunto de permisos personalizado.

- **Conjunto de permisos de revisor** (derechos de solo lectura para e grupo **Todo**)
- **Conjunto de permisos de administrador** (acceso completo al grupo **Todo**).
- **Conjunto de permisos de instalación asistida por servidor** (se necesita derechos de acceso mínimos para la instalación asistida por servidor)
- **Conjunto de permisos del revisor de ESET Inspect**: derechos de acceso mínimos de solo lectura (para el grupo **Todo**) necesarios para un usuario de ESET Inspect On-Prem.
- **Conjunto de permisos de servidor de ESET Inspect**: derechos de acceso (para el grupo **Todo**) necesarios para el proceso de instalación de ESET Inspect On-Prem y otra sincronización automática entre ESET Inspect On-Prem y ESET PROTECT On-Prem.
- **Conjunto de permisos del usuario de ESET Inspect**: derechos de acceso de escritura (para el grupo **Todo**) necesarios para un usuario de ESET Inspect On-Prem.

Cada grupo de permisos otorga permiso únicamente para los objetos dentro de los **Grupos estáticos** seleccionados en el grupo de permisos.

Los usuarios sin ningún conjunto de permisos no podrán iniciar sesión en la consola web.

Todos los permisos predefinidos tienen el grupo **Todos** en la sección **Grupos estáticos**. Tenga esto en cuenta al asignarlo a un usuario. Los usuarios tendrán estos permisos sobre todos los objetos en ESET PROTECT On-Prem.

Resumen

Revise los ajustes configurados para este usuario y haga clic en **Finalizar** para crear el grupo.

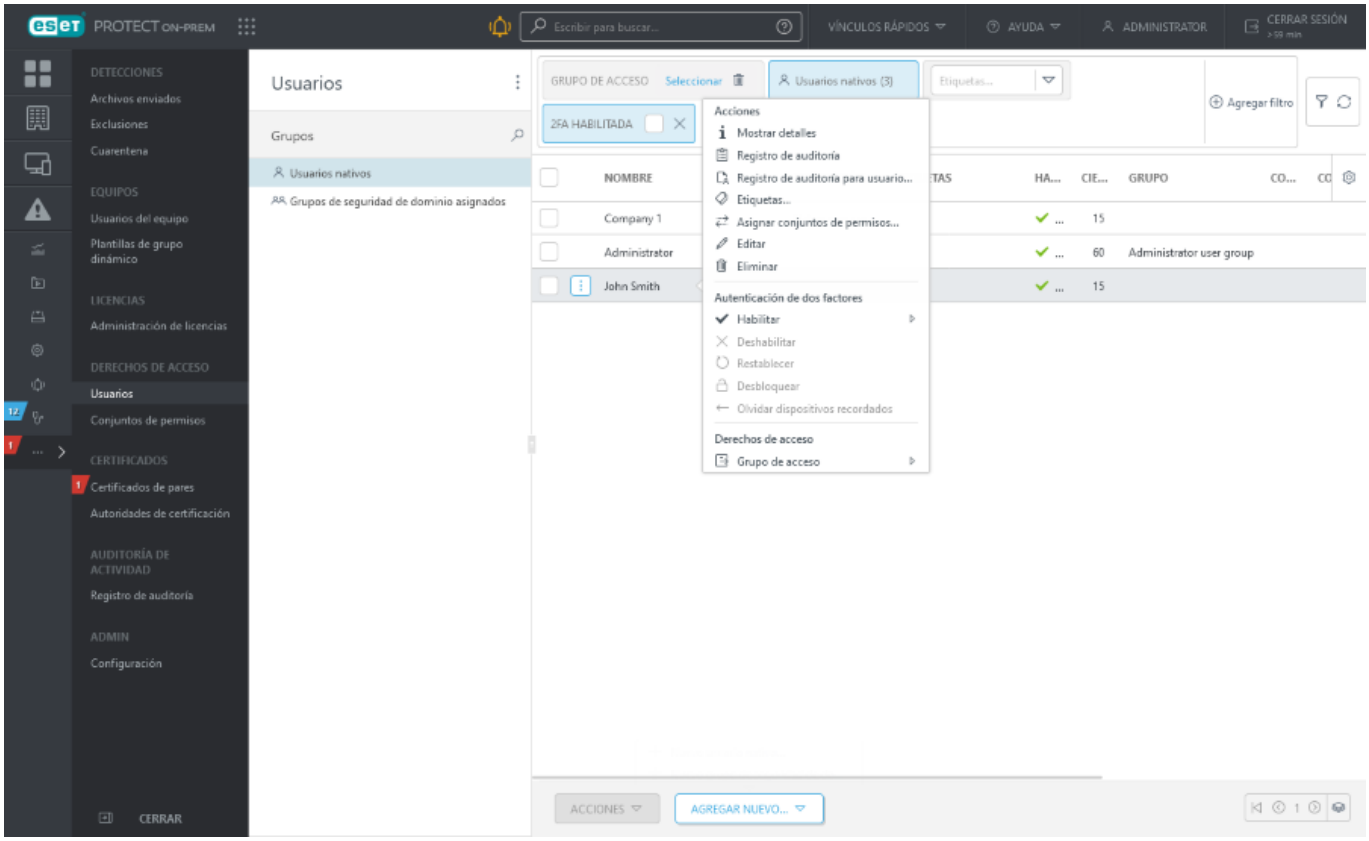
Los usuarios aparecerán en los **Grupos de seguridad de dominio asignados** luego del primer inicio de sesión.

Asignar un conjunto de permisos a un usuario

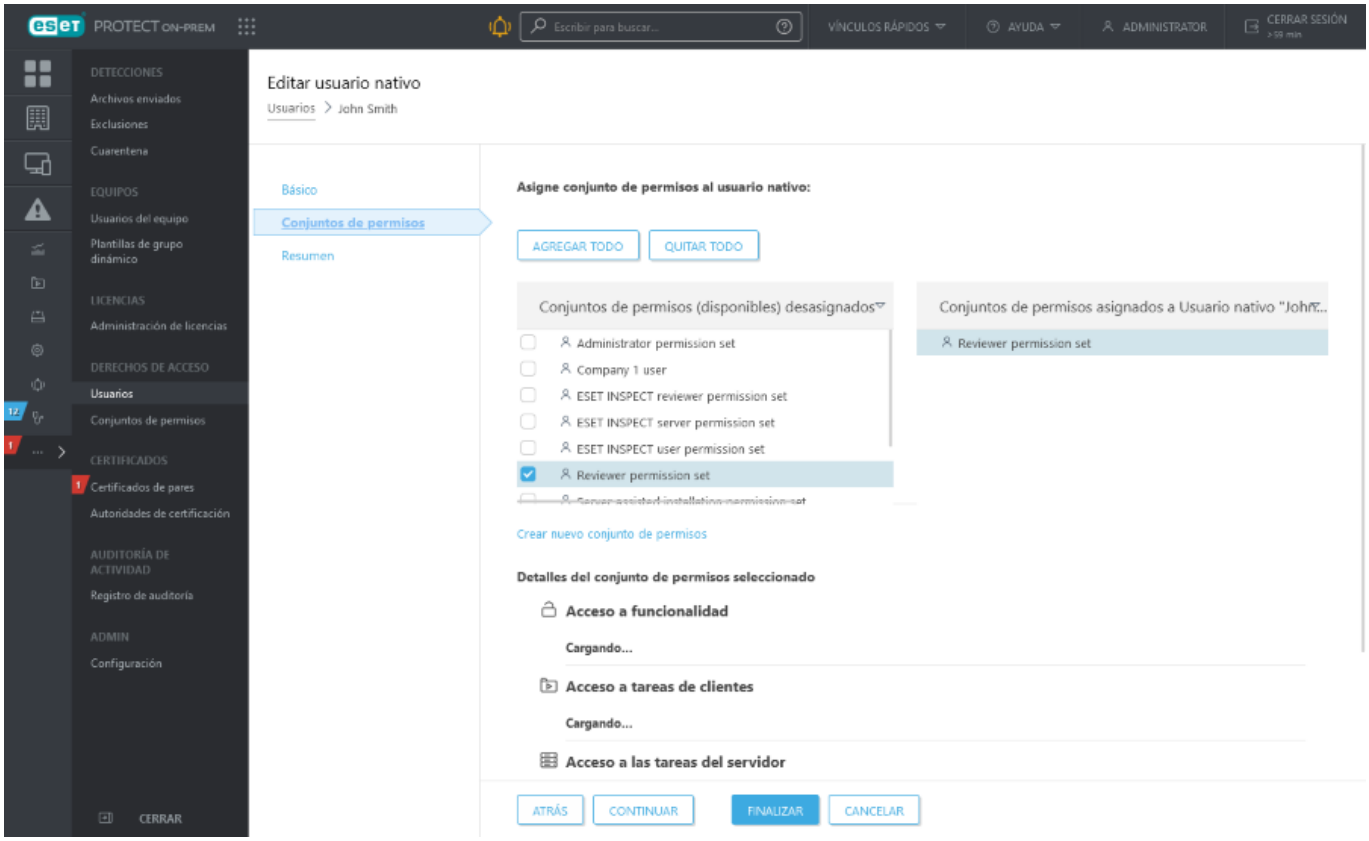
1. Hay dos maneras de asignar un conjunto de permisos a un usuario:

   a)Haga clic en **Más** > **Usuarios** y, luego, en un usuario y seleccione **Asignar conjuntos de permisos** para asignar conjuntos de permisos específicos para un usuario.

   b)En la sección **Usuarios**, edite un usuario específico al hacer clic en **Editar**.



2. Seleccione la casilla de verificación junto al Conjunto específico de permisos en la sección **Conjuntos de permisos no asignados (disponibles)**. Consulte Administrar conjuntos de permisos para obtener más detalles.



Autenticación de dos factores

La autenticación de dos factores (2FA) proporciona una manera más segura de iniciar sesión y acceder a la consola web ESET PROTECT. Los usuarios con la autenticación de dos factores habilitada tendrán que iniciar sesión en ESET PROTECT On-Prem usando ESET Secure Authentication o un autenticador de terceros.

- No hay límite para la cantidad de usuarios que pueden iniciar sesión en ESET PROTECT On-Prem mediante 2FA.
- La configuración del**proxy HTTP** no se aplica a la comunicación con la autenticación de dos factores (2FA).
- Puede habilitar 2FA también para la cuenta de Administrador.

Requisitos previos

- Para habilitar la autenticación de dos factores para otro usuario, el usuario actual necesita tener el permiso **Escritura** sobre ese usuario. Cuando se activa la autenticación de dos factores, el usuario debe configurar por sí mismo la autenticación de dos factores antes de iniciar sesión. Los usuarios recibirán un vínculo por mensaje de texto (SMS) que pueden abrir en el navegador de su teléfono para ver las instrucciones para configurar 2FA.
- 2FA no funciona sin acceso directo a la red para servidores de 2FA de ESET. Es necesario, como mínimo, permitir servidores de 2FA específicos en el firewall. Si el proxy está configurado en **Más** > **Configuración** > **Configuración avanzada** > **Proxy HTTP**, no se aplica para la 2FA.

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

Habilitar la Autenticación de dos factores para un usuario de Consola web

1. Cree un nuevo usuario o use uno existente.

2. Haga clic en **Más** > **Usuarios** en la Consola web de ESET PROTECT.

3. Haga clic en el usuario y seleccione **Autenticación de dos factores** > **Habilitar** y seleccione la opción que desee utilizar:

   • **ESET Secure Authentication**: la autenticación de dos factores es proporcionada por ESET usando la tecnología ESET Secure Authentication. No tiene que implementar o instalar la ESET Secure Authentication en su entorno, ya que ESET PROTECT On-Prem se conecta automáticamente con los servidores de ESET para autenticar los usuarios que inician sesión en su consola web ESET PROTECT.

   • **Autenticación de terceros**: en la versión 9.1 y las versiones posteriores de ESET PROTECT On-Prem, puede utilizar un cliente de autenticación de terceros que admita el protocolo TOTP necesario. Hemos probado las siguientes aplicaciones: Google Authenticator, Microsoft Authenticator o Authy.

4. La próxima vez que el usuario inicie sesión, escriba el número de teléfono del usuario cuando se le solicite.

5. Instale la aplicación móvil de ESET Secure Authentication o una aplicación de autenticación de terceros en el teléfono móvil del usuario usando el enlace del SMS o el código QR.

6. Cuando instala la aplicación utilizando el token, su instancia ESET PROTECT On-Prem se agrega a la aplicación.

7. Proceda a ingresar y escribir la contraseña de un solo uso desde la aplicación móvil a la Consola web cuando se le pida. Se genera una nueva contraseña por única vez cada 30 segundos.

8. Opcionalmente, seleccione la casilla de verificación **Recordar este dispositivo** para autorizar a su dispositivo a no solicitar la autenticación de dos factores por cada inicio de sesión.

Puede olvidar los dispositivos recordados del usuario activo en la Configuración del usuario.

9. Haga clic en **Enviar**.

Solución de problemas

El usuario se bloqueará al escribir la contraseña por única vez incorrectamente diez veces. El administrador puede desbloquear al usuario en **Más** > **Usuarios** > hacer clic en el usuario y seleccionar **Desbloquear**.

Si un usuario de la consola web no puede iniciar sesión en la consola web con la autenticación de dos factores, siga estos pasos:

1. Creación de copias de seguridad de la base de datos ESET PROTECT.

2. Seleccione la opción correspondiente:

   • Puede acceder al número de teléfono configurado para la autenticación de dos factores:

   a)Durante el inicio de sesión en la consola web, haga clic en **Restablecer token** en la ventana de autenticación de dos factores.

b)Se envía un SMS de verificación al número de teléfono configurado para la autenticación de dos factores.

No puede cambiar el número de teléfono almacenado en la base de datos de ESET PROTECT. Si no se puede acceder al teléfono, siga los pasos a continuación.

• No se puede acceder al número de teléfono configurado para la autenticación de dos factores (el teléfono se pierde, se daña, etc.)

a)Restablezca la contraseña de la consola web para desactivar la autenticación de dos factores en la cuenta de administrador.

El estado de la autenticación de dos factores de otras cuentas de usuario de ESET PROTECT On-Prem no se ve afectado.

b)El usuario puede iniciar sesión en la consola web sin la autenticación de dos factores y, a continuación, volver a activar la autenticación de dos factores tras iniciar sesión.

Conjuntos de permisos

Un conjunto de permisos representa los permisos para usuarios que acceden a la consola web ESET PROTECT. Definen qué puede hacer o ver un usuario dentro de la consola web. Los usuarios nativos cuentan con sus propios permisos, mientras que los usuarios de dominio cuentan con los permisos correspondientes a su grupo de seguridad asignado. Cada conjunto de permisos cuenta con su propio dominio de aplicación (grupos estáticos). Los permisos que se seleccionan en la sección **Funcionalidad** afectarán a los objetos en los grupos configurados en la sección de **Grupos estáticos** para cada usuario asignado por este conjunto de permisos. Tener acceso a un determinado Grupo estático automáticamente implica tener acceso a cada uno de los subgrupos. Con una configuración adecuada de los grupos estáticos es posible crear diferentes secciones para los admins locales (ver el ejemplo).

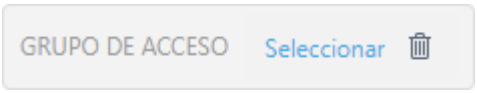
Se le puede asignar un conjunto de permisos a un usuario sin ser capaz de verlo. Un conjunto de permisos también es un objeto almacenado automáticamente en el grupo hogar del usuario que lo crea. Cuando se crea una cuenta de usuario, el usuario se almacena como un objeto en el grupo hogar del usuario que lo creó. Generalmente el administrador crea usuarios, por lo que se almacenan en el grupo *Todos*.

Los conjuntos de permisos son acumulativos. Si asigna más de un conjunto de permisos a un solo usuario, la suma de todos los conjuntos de permisos es el acceso resultante que tiene el usuario.

Combinar más conjuntos de permisos

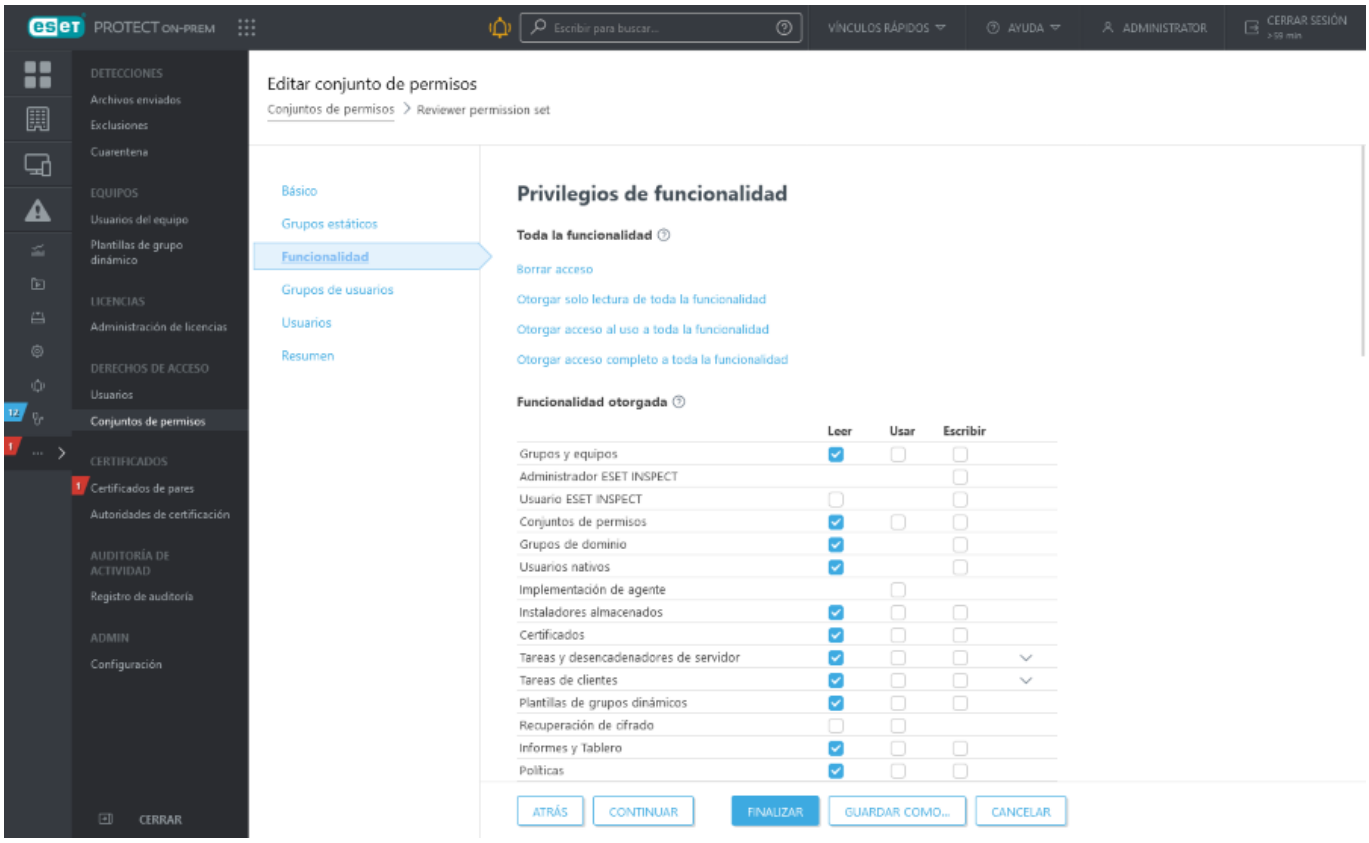
El acceso final que tiene un usuario a un objeto es el resultado de la combinación de todos los conjuntos de permisos asignados al usuario. Por ejemplo, un usuario tiene dos conjuntos de permisos, uno para el grupo doméstico con permisos completos y otro para un grupo con computadoras, con permisos únicamente a Lectura, Uso del equipo y Grupos. Este usuario puede ejecutar todas las tareas desde el grupo doméstico en los equipos del otro grupo.

En general, un usuario puede ejecutar objetos desde un grupo estático sobre objetos en otro grupo estático, siempre y cuanto el usuario tenga permisos para ciertos tipos de objetos en un grupo determinado.



El botón de filtro **Grupo de acceso** le permite a los usuarios seleccionar un grupo estático y filtrar los objetos mostrados en función del grupo en el que se encuentran.

Puede usar etiquetas para filtrar los elementos mostrados.



Buena práctica para trabajar con permisos:
- Nunca le otorgue acceso a la ESET PROTECTConfiguración del servidor a usuarios in experiencia; solo el administrador debería tener este acceso.
- Considerar restringir el acceso a las **Tareas del cliente** > **Ejecutar comando**: se trata de una tarea muy poderosa que podría ser abusada.
- Los usuarios que no son de nivel de administrador no deben tener permisos para **conjuntos de permisos**, **usuarios nativos** y **configuración del servidor**.
- Si se necesita un modelo de permisos más complejo, no dude en crear más conjuntos de permisos y asignarlos según corresponda.

El permiso Registro de auditoría le posibilita al usuario ver las acciones iniciadas por todos los demás usuarios y dominios, incluso las relacionadas con activos para los cuales el usuario no tiene derechos de visualización suficientes.

Luego de configurar los permisos para la funcionalidad de ESET PROTECT On-Prem, también puede asignar acceso de **Lectura**, **Uso**, **Escritura** a Grupos de usuarios.

Duplicación

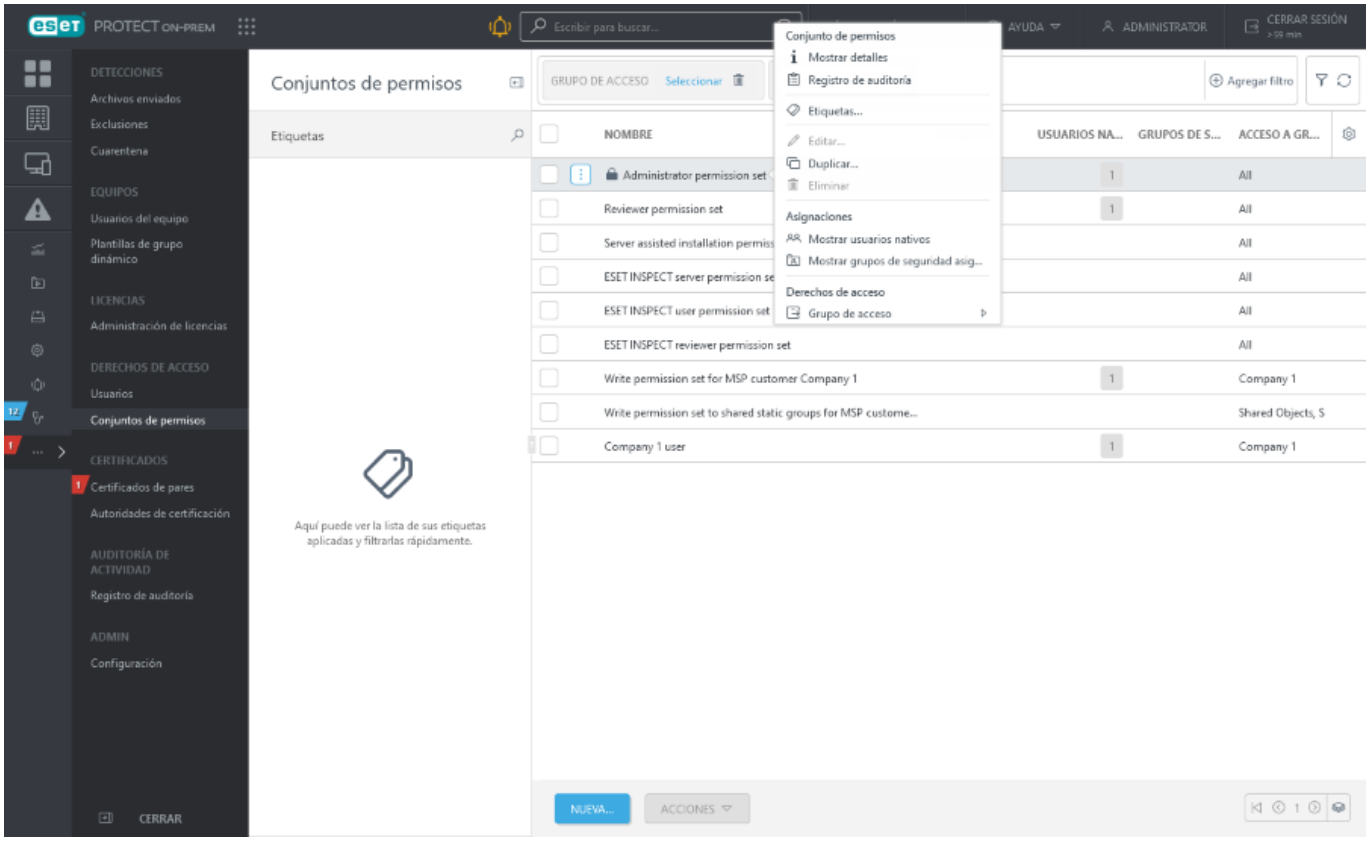
Para duplicar un objeto, el usuario necesita contar con permisos de **Lectura** sobre el objeto original y permisos de **Escritura** sobre su **Grupo hogar** para este tipo de acción.
John, cuyo grupo hogar es *Grupo de John,* desea duplicar la *Política 1,* que fue creada originalmente por *Larry*, por lo que se encuentra automáticamente en el grupo hogar de Larry, *Grupo de Larry*.
1.Creación de un nuevo grupo estático. Nombrarlo, por ejemplo, *Políticas compartidas*.
2.Asignarle a *John* y a *Larry* permisos de **Lectura** para las **Políticas** en el grupo *Políticas compartidas*.
3.*Larry* mueve la *Política 1* al grupo *Políticas compartidas*.
4.Asignarle a *John* permisos de **Escritura** para las **Políticas** en su grupo hogar.
5.*John* ahora puede **Duplicar** la *Política 1:* el duplicado aparecerá en su grupo hogar.

Diferencia entre Uso y Escritura

Si el *Administrador* no desea que el usuario *John* pueda modificar políticas en el grupo *Políticas compartidas* creará un conjunto de permisos con:
- Funcionalidad **Políticas**: Permisos de **Lectura** y **Uso** seleccionados
- **Grupos estáticos**: Políticas compartidas

Con estos permisos asignados a *John*, *John* puede ejecutar estas políticas pero no puede editarlas, quitarlas ni crear nuevas políticas. Si un administrador agregara permisos de **Escritura**, John podría crear nuevas políticas, editarlas y quitarlas dentro del grupo estático seleccionado (*Políticas compartidas*).

Administrar conjuntos de permisos



Para administrar un conjunto de permisos, haga clic en el conjunto de permisos y seleccione una de las acciones disponibles:

Conjunto de permisos

- **Mostrar detalles**: ver detalles del conjunto de permisos.

- **Registro de auditoría** - Ver el registro de auditoría del elemento seleccionado.
- **Etiquetas** - Editar etiquetas (asignar, desasignar, crear, quitar).
- **Editar**: editar el conjunto de permisos.
- **Duplicar**: crea un conjunto de permisos duplicado que puede modificar y asignar a un usuario específico. El duplicado se almacenará en el grupo hogar del usuario que lo duplicó.
- **Quitar**: quitar el conjunto de permisos.

Asignaciones

- **Mostrar usuarios nativos**: muestra la lista de usuarios nativos asignados.
- **Mostrar grupos de seguridad asignados**: muestra la lista de los grupos de seguridad de dominio asignado.

Derechos de acceso

- **Grupo de acceso** > **Mover** – Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen derechos suficientes para el grupo de destino. Cambiar el grupo de acceso es útil cuando se resuelven problemas de acceso con otros usuarios. El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario.

Todos los permisos predefinidos tienen el grupo **Todos** en la sección **Grupos estáticos**. Tenga esto en cuenta al asignarlo a un usuario. Los usuarios tendrán estos permisos sobre todos los objetos en ESET PROTECT On-Prem.

Crear o editar un conjunto de permisos

Para crear un nuevo conjunto de permisos, haga clic en **Nuevo**. Para editar un conjunto de permisos existente, seleccione el conjunto de permisos correspondiente y haga clic en **Editar**.

Básica

Ingrese un **Nombre** para el conjunto (configuración obligatoria). También puede introducir una **Descripción** y **Etiquetas**.

Haga clic en **Seleccionar etiquetas** para asignar etiquetas.

Grupos estáticos

Puede **seleccionar** un Grupo estático (o múltiples grupos estáticos) o **crear un nuevo grupo** que contará con esta habilidad. Los permisos seleccionados en la sección **Funcionalidad** se aplicarán en los objetos dentro de los grupos seleccionados en esta sección.

Funcionalidad

Seleccione módulos individuales para los cuales desea otorgar acceso. El usuario con esta competencia tendrá acceso a estas tareas específicas. Es posible establecer diferentes permisos para cada tipo de tarea del servidor y tarea del cliente. Hay cuatro conjuntos de funcionalidad disponibles definidos previamente. Seleccione una de las cuatro casillas de verificación de la funcionalidad o selecciónelas de manera manual.

Otorgar permisos de **Escritura** otorga automáticamente derechos de **Uso** y **Lectura**; otorgar derechos de **Uso** automáticamente otorga derechos de **Lectura**.

Grupos de usuarios

Puede agregar un Grupo de usuarios (o varios Grupos de usuarios) cuyos parámetros de usuarios puedan usarse dentro de una política (por ejemplo Administración de dispositivos móviles de ESET para iOS o Modo de anulación).

Usuarios

Seleccione un usuario al que asignarle este conjunto de permisos. Los usuarios disponibles se enumeran a la izquierda. Seleccione los usuarios específicos o seleccione todos los usuarios con el botón **Agregar todos**. Los usuarios asignados se enumeran a la derecha. No es obligatorio asignar un usuario; puede hacerlo más tarde.

Resumen

Revise los ajustes configurados para esta competencia y haga clic en **Finalizar**. El conjunto de permisos se almacena en el Grupo hogar del usuario que lo creó.

Haga clic en **Guardar como** para crear un nuevo conjunto de permisos basado en el permiso que está editando. Se le pedirá que ingrese un nombre para el nuevo conjunto de permisos.

Lista de permisos

Tipos de permisos

Al crear o editar un conjunto de permisos en **Más** > **Conjuntos de permisos** > **Nuevo/Editar** > **Funcionalidad** existe una lista de todos los permisos disponibles. Los permisos de la consola web de ESET PROTECT se dividen en categorías. Por ejemplo, **Grupos y equipos**, **Políticas**, **Tareas del cliente**, **Informes**, **Notificaciones** y más. Un conjunto de permisos puede brindar acceso de **Lectura**, **Uso** o **Escritura**. En general:

- Los permisos de **lectura** son buenos para usuarios de auditoria. Pueden ver los datos, pero no pueden modificarlos.
- Los permisos **Uso** permiten a los usuarios utilizar objetos y ejecutar tareas, pero no modificar ni eliminar.
- Los permisos de **Escritura** permiten a los usuarios modificar objetos respectivos y/o duplicarlos.

Ciertos tipos de permisos (enumerados a continuación) controlan a los procesos, no un objeto. Es por eso que funcionan a un nivel global, por lo que no importa a qué grupo estático se aplica el permiso, funcionará de todos modos. Si se le permite un proceso a un usuario, puede utilizarlo solo sobre objetos para los cuales tenga

suficientes permisos. Por ejemplo, el permiso **Exportar informe a archivo** habilita la funcionalidad de exportación; sin embargo, otros permisos determinan los datos contenidos en el informe.

Lea el artículo de la base de conocimiento para acceder a ejemplos de tareas y conjuntos de permisos que el usuario necesita para completar correctamente las tareas.

No están disponibles (están atenuadas) las funcionalidades a las que el usuario actual no tiene derechos de acceso.

Se les puede asignar permisos a los usuarios para los siguientes procesos:

- **Implementación del agente**
- **Informes y tablero** (solo la funcionalidad del tablero estará disponible; las plantillas de informes utilizables aún dependen de los grupos estáticos accesibles)
- **Enviar correo electrónico**
- **Exportar informe a archivo**
- **Enviar captura SNMP**
- **Configuración del servidor**
- **ESET Inspect Administrador**
- **ESET Inspect Usuario**
- **Informes completos**

Tipos de funcionalidad:

Grupos y equipos

Lectura: lista de quipos, grupos y equipos dentro de un grupo.

Uso: usar un equipo/grupo como objetivo para una política o tarea.

Escritura: crear, modificar y eliminar equipos. Esto también incluye cambiar el nombre de un equipo o grupo.

ESET Inspect Administrador

Escritura: realizar funciones ejecutivas en ESET Inspect On-Prem.

ESET Inspect Usuario

Lectura: acceso de solo lectura a ESET Inspect On-Prem. Un usuario de la consola web necesita permiso de

Lectura o superior para **Acceder a ESET Inspect** o permiso de **Lectura** o superior para el usuario **ESET Inspect**.

Escritura: acceso de lectura y escritura a ESET Inspect On-Prem.

Conjuntos de permisos

Lectura: leer la lista de conjuntos de permisos y la lista de derechos de acceso que contienen.

Uso: asignar/eliminar los conjuntos de permisos existentes para los usuarios.

Escritura: crear, modificar y eliminar conjuntos de permisos de escritura.

Al asignar o anular la asignación de un conjunto de permisos a un usuario, se requiere permiso de **escritura** para **grupos de dominio** y **usuarios nativos**.

Grupos de dominios

Lectura: lista de grupos de dominio.

Escribir: otorga permisos de autorizar/revocar conjuntos de permisos. Crear, modificar y eliminar grupos de dominio.

Usuarios nativos

Lectura: lista de usuarios nativos.

Escribir: otorga permisos de autorizar/revocar conjuntos de permisos. Crear, modificar y eliminar usuarios nativos.

Implementación del agente

Uso: permite el acceso para implementar el agente mediante **vínculos rápidos** o agregar equipos cliente de manera manual en la consola web de ESET PROTECT.

Instaladores almacenados

Lectura: lista de instaladores almacenados.

Uso: exportar instaladores almacenados.

Escritura: crear, modificar y eliminar instaladores almacenados.

Certificados

Lectura: leer la lista de certificados de pares y autoridades de certificación.

Uso: exportar autoridades de certificación y certificados de pares y usarlos en instaladores o tareas.

Escritura: crear nuevos certificados de pares o autoridades de certificación y revocarlos.

Tareas y desencadenadores de servidor

Lectura: leer la lista de tareas y sus configuraciones (a excepción de campos sensibles, como contraseñas).

Uso: ejecutar una tarea existente con Ejecutar ahora (como el usuario actualmente registrado en la consola web).

Escritura: crear, modificar y eliminar tareas de servidor.

Para expandir las categorías, se puede hacer clic en el signo y se pueden seleccionar tareas únicas o múltiples del servidor.

Tareas de clientes

Lectura: leer la lista de tareas y sus configuraciones (a excepción de campos sensibles, como contraseñas).

Uso: programar la ejecución de las tareas de cliente existentes o cancelar su ejecución. Tenga en cuenta que para la asignación de tareas (o cancelar la asignación) a objetos (equipos o grupos) se necesitan permisos de Uso adicionales para los objetos meta.

Escritura: crear, modificar o eliminar tareas de cliente existentes. Tenga en cuenta que para la asignación de tareas (o cancelación de asignación) a destinos (equipos o grupos), se necesitan permisos de **Uso** adicionales para los objetos de destino.

Para expandir las categorías, se puede hacer clic en el signo más y seleccionar tareas únicas o múltiples del servidor.

Plantillas de grupos dinámicos

Lectura: lectura de la lista de plantillas de grupos dinámicos.

Uso: usar plantillas existentes para grupos dinámicos.

Escritura: crear, modificar y eliminar plantillas de grupos dinámicos.

Recuperación de cifrado

Leer

Uso: gestionar el proceso de recuperación de cifrado.

Informes y Panel

Lectura: lista de plantillas de informe y sus categorías. Generar informes con base en plantillas de informe. Leer sus propios tableros con base en los tableros predeterminados.

Uso: modificar sus propios tableros con las plantillas de informe disponibles.

Escritura: crear, modificar y eliminar plantillas de informes existentes y sus categorías. Modificar tableros predeterminados.

Políticas

Lectura: leer la lista de políticas y la configuración que contienen.

Uso: asignar políticas existentes a objetos (o cancelar su asignación). Tenga en cuenta que para los objetos afectados se necesitan permisos de **Uso** adicionales.

Escritura: crear, modificar y eliminar políticas.

Enviar correo electrónico

Uso: enviar correos electrónicos. (Útil para tareas del servidor Notificación y Generar informe.)

Enviar captura SNMP

Uso: permite enviar capturas SNMP (útil para notificaciones).

Exportar informe a archivo

Uso: le permite almacenar informes en el sistema de archivos del equipo del servidor ESET PROTECT. Útil para tareas del servidor Generar informe.

Licencias

Lectura: leer la lista de licencias y sus estadísticas de uso.

Uso: usar la licencia para activación.

Escritura: agregar y eliminar licencias. (El usuario debe tener el grupo hogar configurado a Todos. Por defecto, solo el administrador puede hacerlo.)

Notificaciones

Lectura: leer la lista de notificaciones y su configuración.

Uso: asignar etiquetas.

Escritura: crear, modificar y eliminar notificaciones. Para una gestión de notificaciones adecuada se pueden necesitar derechos de acceso de **Uso** para **Enviar capturas SNMP** o **Enviar correos electrónicos**, en función de la configuración de las notificaciones.

Configuración del servidor

Lectura: leer ESET PROTECT configuración del servidor.

Escritura: modificar la ESET PROTECTconfiguración del servidor.

Registro de auditoría

Lectura: vea el informe Registro de auditoría y lea el informe del registro de auditoría.

Informes completos

Uso: generar la plantilla de informe MDR.

Funcionalidad de ESET Inspect otorgada

Esta es una lista de funciones individuales de ESET Inspect a las que tendrá acceso el usuario. Para obtener más información, consulte la ESET Inspect Guía del usuario. Un usuario de la consola web necesita permiso de **Lectura** o superior para **Acceder a ESET Inspect** o permiso de **Lectura** o superior para el usuario **ESET Inspect**.

Certificados

Los certificados son un elemento importante de ESET PROTECT On-Prem, ya que son necesarios para la comunicación segura entre los componentes de ESET PROTECT y el servidor de ESET PROTECT, y también para establecer una conexión protegida de la consola web de ESET PROTECT.

Para asegurarse de que todos los componentes se comunican correctamente, los Certificados de pares necesitan ser válidos y estar firmados por la misma Autoridad de certificación.

Obtenga más información sobre los certificados de ESET PROTECT On-Prem en nuestro artículo de la base de conocimiento.

Usted tiene algunas opciones cuando se trata de certificados:

- Puede usar los certificados creados automáticamente durante la instalación de ESET PROTECT On-Prem.
- Puede crear una nueva autoridad de certificación (AC) o Importar una clave pública que usará para firmar el certificado de pares para cada uno de los componentes (agente ESET Management, servidor ESET PROTECT, MDM ESET PROTECT).
- Puede usar su Autoridad de certificación personalizada y certificados.

Si planea migrar de un servidor ESET PROTECT a un nuevo equipo de servidor, debe exportar/realizar copias de seguridad de todas las autoridades de certificación que usa y del certificado del servidor ESET PROTECT. De lo contrario, ninguno de los componentes de ESET PROTECT se podrán comunicar con su nuevo servidor ESET PROTECT.

Puede crear una nueva **Autoridad de certificación** y **Certificados de pares** en la consola web ESET PROTECT; siga las instrucciones en esta guía para:

- Crear nueva autoridad de certificación
  - Importar una clave pública
  - Exportar una clave pública
  - Exportar una clave pública en formato BASE64
- Crear un nuevo certificado de pares
  - Crear un certificado
  - Exportar un certificado
  - Crear un certificado APN/ABM
  - Revocar un certificado
  - Usar el certificado
  - Establecer el nuevo certificado del servidor ESET PROTECT
  - Certificados personalizados con ESET PROTECT On-Prem
  - Certificado vencido - informe y reemplazo

macOS no es compatible con certificados con vencimientos a partir del 19 de enero de 2038. Los agentes ESET Management que se ejecuten en macOS no podrán conectarse al servidor ESET PROTECT.

Para todos los certificados y las autoridades de certificación que se crean durante la instalación de los componentes de ESET PROTECT, el valor Válido desde se establece a 2 días antes de la creación del certificado.
Para todos los certificados y las autoridades de certificación que se crean durante la consola web ESET PROTECT, el valor Válido desde se establece a 1 día antes de la creación del certificado. La razón para esto es cubrir todas las posibles discrepancias de tiempo entre los sistemas afectados.
Por ejemplo, una autoridad de certificación y un certificado, que se crean el 12 de enero de 2017 durante la instalación, tendrán un valor predefinido de Válido desde el 10 de enero de 2017 00:00:00, y una autoridad de certificación y un certificado que se crean el 12 de enero de 2017 en la consola web ESET PROTECT tendrá un valor predefinido Válido desde el 11 de enero de 2017 00:0:00.

Certificados de pares

Si su sistema cuenta con una Autoridad de certificación, debería crear un certificado de pares para los componentes individuales de ESET PROTECT. Cada componente (agente ESET Management y servidor ESET PROTECT) necesita de un certificado específico.

Nueva

Esta opción se usa para crear un nuevo certificado. Estos certificados son usados por el agente ESET Management y el servidor ESET PROTECT.

Certificado APN/ABM

Esta opción se usa para crear un nuevo certificado APN/ABM. Este certificado es usado por el MDM. Esta acción requiere una licencia válida.

Uso del certificado

También puede verificar qué clientes usan este certificado de ESET PROTECT.

Etiquetas

Editar etiquetas (asignar, desasignar, crear, quitar).

Editar

Seleccione esta opción para editar una **descripción** de un certificado existente de la lista.

Registro de auditoría

Ver el registro de auditoría del elemento seleccionado.

Exportar o **Exportar Base64...**

Exportar un certificado como un archivo *.pfx* o *.txt* (Base64). Este archivo es necesario si instala el agente ESET Management de manera local en un equipo, o si instala un MDM.

Revocar

Si ya no desea utilizar un certificado, seleccione **Revocar**. Esta opción invalida el certificado de manera permanente, y quedará en la lista negra efectivamente. Esta información se envía a agentes ESET Management

durante la siguiente conexión. Los certificados revocados no serán aceptados por ESET PROTECT On-Prem.

> Asegúrese de que no haya agentes ESET Management (u otros componentes) que usen este certificado antes de revocarlo. Una vez que se haya revocado el certificado, los componentes no podrán conectarse al servidor ESET PROTECT. Vuelva a instalar los componentes usando un certificado válido para restaurar la funcionalidad.

Grupo de acceso

Un certificado o una autoridad certificado se pueden mover a otro grupo. Luego pasan a estar disponibles para los usuarios con permisos suficientes para este grupo. Para encontrar fácilmente el grupo hogar de un certificado, seleccione el certificado y haga clic en **Grupo de acceso** en el menú desplegable. El grupo hogar del certificado se muestra en la primera línea del menú emergente (por ejemplo /Todos/San Diego. Consulte nuestro escenario de muestra para más información sobre compartir certificados).

> Solo verá los certificados en su grupo hogar (siempre y cuando tenga permisos de **lectura** para ellos). Los certificados creados durante la instalación de ESET PROTECT On-Prem se encuentran en el grupo **Todos** y solo los administradores pueden acceder a ellos.

Haga clic en el botón **Mostrar revocados** para ver todos los certificados revocados.

Certificado de agente para la instalación asistida por servidor - Este certificado se genera durante la instalación del servidor si selecciona la opción **Generar certificados**.

Personalización del diseño y de los filtros

Puede personalizar la vista de la pantalla de la consola web actual:

- Administre el panel lateral y la tabla principal.
- Agregar filtro y filtros preestablecidos. Puede usar etiquetas para filtrar los elementos mostrados.

Crear una nuevo certificado

Como parte del proceso de instalación, ESET PROTECT On-Prem requiere que cree un certificado de pares para los agentes. Estos certificados se utilizan para autenticar la comunicación entre el agente en el dispositivo de cliente y ESET PROTECT Server.

> Existe una excepción, un **Certificado de agente para la instalación asistida por servidor** no se puede crear manualmente. Este certificado se genera durante la instalación del servidor, siempre y cuando se haya seleccionado la opción **Generar certificados**.

Para crear un certificado nuevo en la consola web **ESET PROTECT**, vaya a **Más** > **Certificados de pares** y haga clic en **Acciones** > **Nuevo**.

Básica

Descripción: escriba una descripción del certificado.

Haga clic en **Seleccionar etiquetas** para asignar etiquetas.

Producto: seleccione el tipo de certificado que desea crear desde el menú desplegable.

Host: deje el **valor predeterminado (un asterisco) en el campo Host** para permitir la distribución de este certificado sin vinculación a un nombre DNS o dirección IP específica.

Cuando crea el certificado de MDM, complete la dirección de IP o nombre de host del dispositivo host MDM. El valor predeterminado (un asterisco) no es válido para este tipo de certificado.

Frase de contraseña: recomendamos que deje este campo en blanco, pero puede fijar una frase de contraseña para el certificado que se requerirá cuando los clientes intentan activar.

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

Atributos (asunto)

estos campos no son obligatorios, pero puede usarlos para incluir información más detallada sobre este certificado.

Nombre común: este valor debe contener la cadena “Agente”, o “Servidor”, según el **Producto** seleccionado. Si lo desea, puede ingresar una descripción acerca del certificado. Ingrese los valores **Válido desde** y **Válida hasta** para asegurarse de que el certificado sea válido.

Para todos los certificados y las autoridades de certificación que se crean durante la instalación de los componentes de ESET PROTECT, el valor Válido desde se establece a 2 días antes de la creación del certificado.
Para todos los certificados y las autoridades de certificación que se crean durante la consola web ESET PROTECT, el valor Válido desde se establece a 1 día antes de la creación del certificado. La razón para esto es cubrir todas las posibles discrepancias de tiempo entre los sistemas afectados.
Por ejemplo, una autoridad de certificación y un certificado, que se crean el 12 de enero de 2017 durante la instalación, tendrán un valor predefinido de Válido desde el 10 de enero de 2017 00:00:00, y una autoridad de certificación y un certificado que se crean el 12 de enero de 2017 en la consola web ESET PROTECT tendrá un valor predefinido Válido desde el 11 de enero de 2017 00:0:00.

Firmar

Seleccionar entre dos métodos de firma:

- **Autoridad de certificación**: si desea firmar con la **Autoridad de certificación de ESET PROTECT** (AC creada automáticamente durante la instalación de ESET PROTECT On-Prem).
  - Seleccione la **Autoridad de certificación de ESET PROTECT** de la lista de autoridades de certificación
  - Cree una nueva autoridad de certificación
- **Archivo pfx personalizado**: Para utilizar un archivo *.pfx* personalizado, haga clic en **Examinar**, vaya a su archivo *.pfx* personalizado y haga clic en **Aceptar**. Seleccione **Cargar** para cargar este certificado al servidor. No puede utilizar el certificado personalizado.

Si desea firmar un nuevo certificado con la AC de ESET PROTECT On-Prem (creada durante la instalación de ESET PROTECT On-Prem) en la aplicación virtual de ESET PROTECT, es necesario ingresar una **Frase de contraseña de la autoridad de certificación. Ésta es** la contraseña que especificó durante la configuración de la aplicación virtual de ESET PROTECT

Resumen

Revise la información del certificado que ingresó y haga clic en **Finalizar**. El certificado se creó correctamente y estará disponible en la lista de **Certificados** para usarse durante la instalación del Agente. El certificado se creará en su grupo hogar.

Como alternativa a la creación de un nuevo certificado, puede Importar una clave pública, Exportar una clave pública o Exportar un certificado de pares.

Exportar certificado de pares

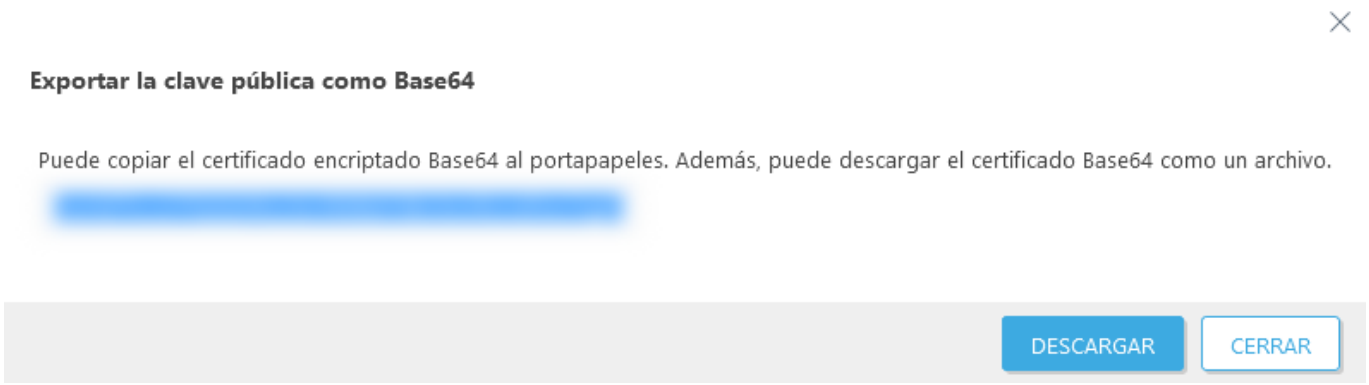
Exportar certificados de pares

1.Seleccione los **Certificados de pares** que desee usar de la lista y seleccione la casilla de verificación junto a esa autoridad.

2.En el menú contextual seleccione **Exportar**. El certificado se exportará (incluida la clave privada) como un archivo *.pfx*. Escriba el nombre del certificado y haga clic en **Guardar**.

Exportar como Base64 desde certificados de pares

Los certificados para los componentes de ESET PROTECT están disponibles en la consola web. Para copiar los contenidos de un certificado en formato Base64, haga clic en **Más** > **Certificados de pares**, seleccione un certificado y, luego, seleccione **Exportar como Base64**. También puede descargar el certificado con cifrado Base64 como un archivo. Repita este paso para los certificados de los otros componentes, al igual que para su Autoridad de certificación.



Para exportar un certificado, el usuario necesita tener derechos de **Uso** para los **Certificados**. Consulte la lista completa de derechos de acceso para obtener más información.

Certificado APN/ABM

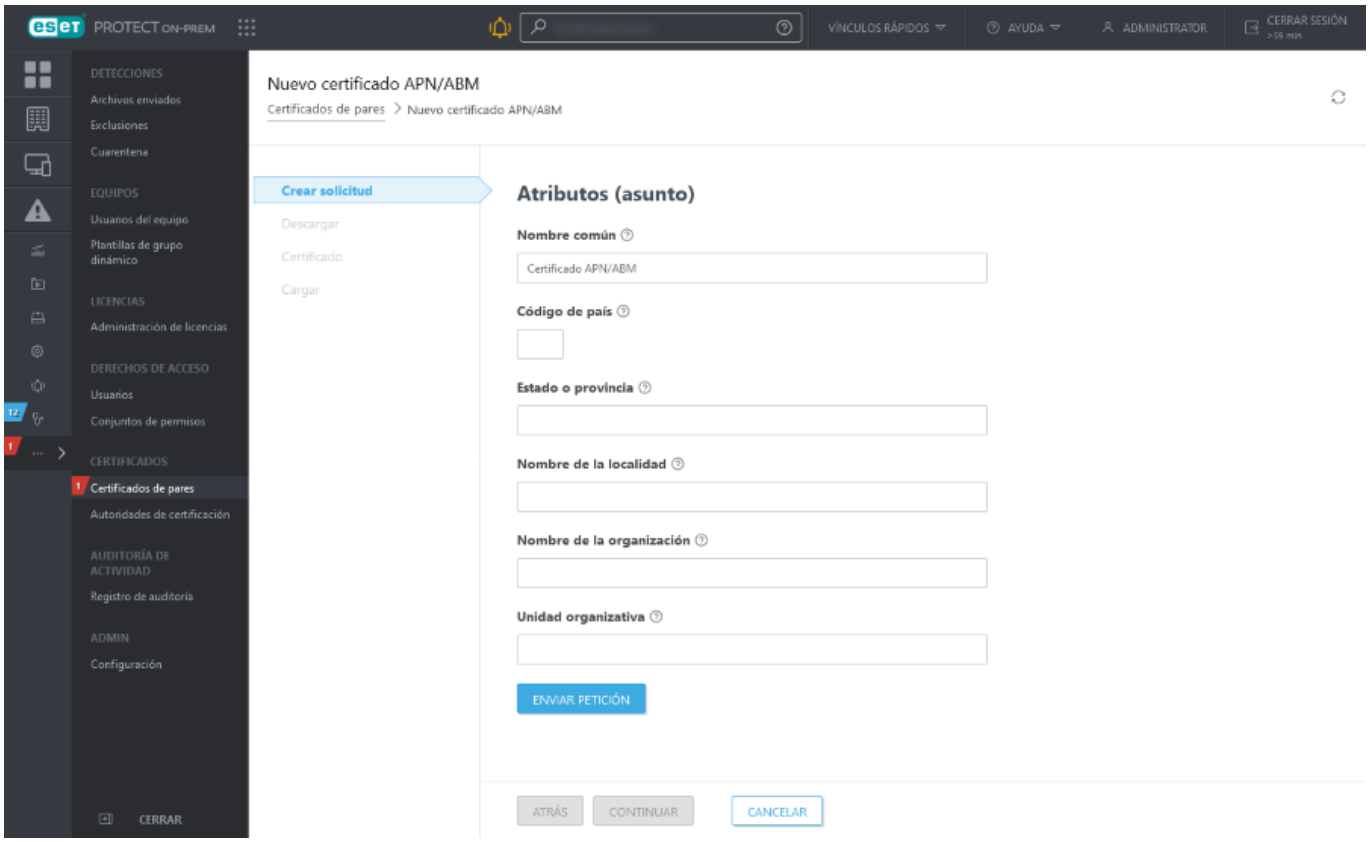
El MDM de ESET PROTECT usa un certificado APN (notificación Push de Apple)/ABM (Apple Business Manager) para el registro de dispositivos iOS. Necesita crear un **Certificado push provisto por Apple** y hacerlo firmar por Apple antes de poder inscribir dispositivos iOS en ESET PROTECT On-Prem. Asegúrese también de tener una licencia válida para ESET PROTECT On-Prem.

Haga clic en la pestaña **Más** > **Certificados de pares**, haga clic en **Nuevo y, luego,** seleccione **Certificado de APN/ABM**.

Para un obtener un certificado APN, necesita un Apple ID. Esta ID es necesaria para que Apple firme el certificado.
El certificado de APN tiene 1 año de validez. Si su certificado está por expirar, siga estos pasos y, en el paso 2 de la parte del certificado, seleccione **Renovar**.
Para obtener un token de inscripción ABM, necesita una cuenta ABM de Apple.

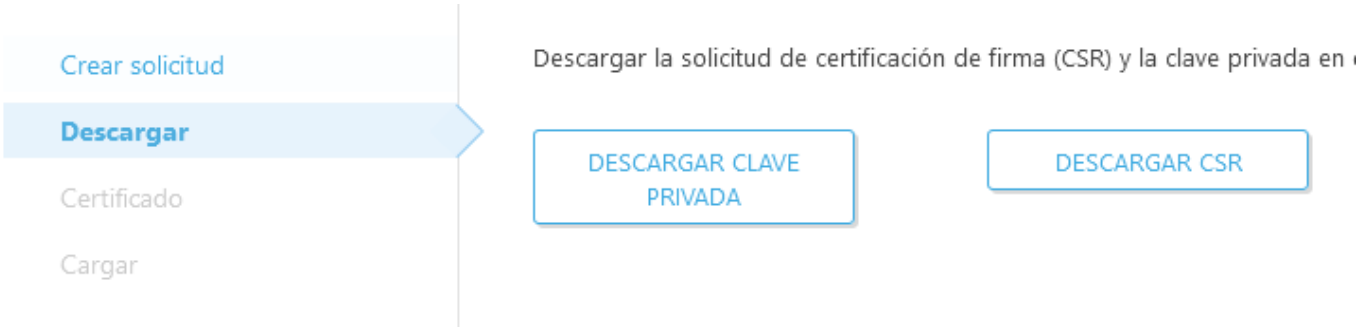
Crear solicitud

Especifique los atributos del certificado (código de país, nombre de la organización, etc.) y haga clic en **Enviar solicitud**.



Descargar

Descargue la **CSR** (Solicitud de certificación de firma) y una **Clave privada**.



Certificado

1.Abra el Portal de certificados Push de Apple e inicie sesión con su ID de Apple.

2.Haga clic en **Crear un certificado**.

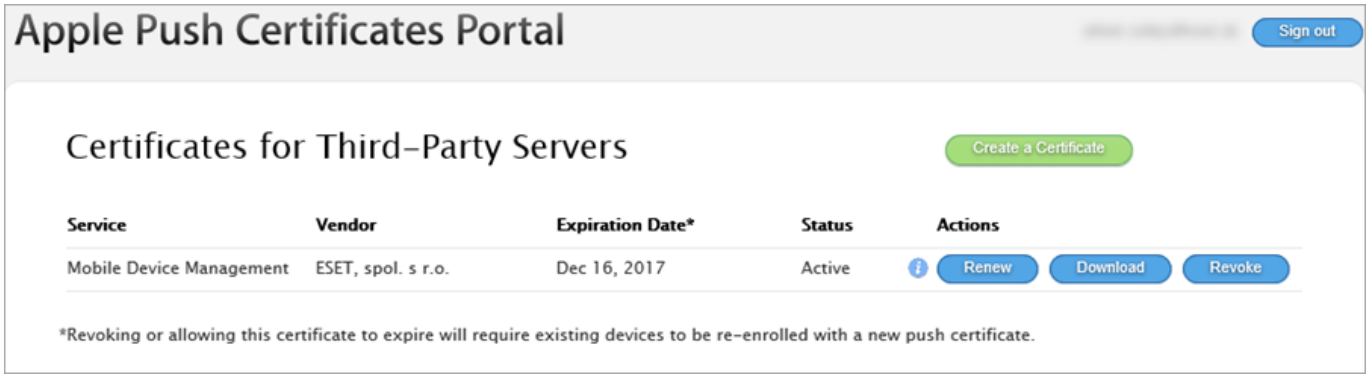
3.Complete la nota (opcional). Haga clic en **Seleccionar archivo** y cargue el archivo CSR que descargó en el paso anterior, luego haga clic en **Cargar**.

4.Luego de unos momentos verá una nueva ventana de confirmación con la notificación de que el certificado APNS para el servidor de administración de dispositivos móviles de ESET se ha creado con éxito.

5.Haga clic en **Descargar** y guarde el archivo *.pem* en su equipo.

6.Cierre el portal de certificado push de Apple y proceda a la sección de Carga a continuación.

Se necesita el certificado APNS para políticas MDC ABM y no ABM.
Siga estas instrucciones para crear un certificado de inscripción de ABM.



Cargar

Una vez que haya completado los pasos anteriores, podrá crear una Política para que MDC active APNS para la inscripción de iOS. Luego puede inscribir cualquier dispositivo iOS ingresando a

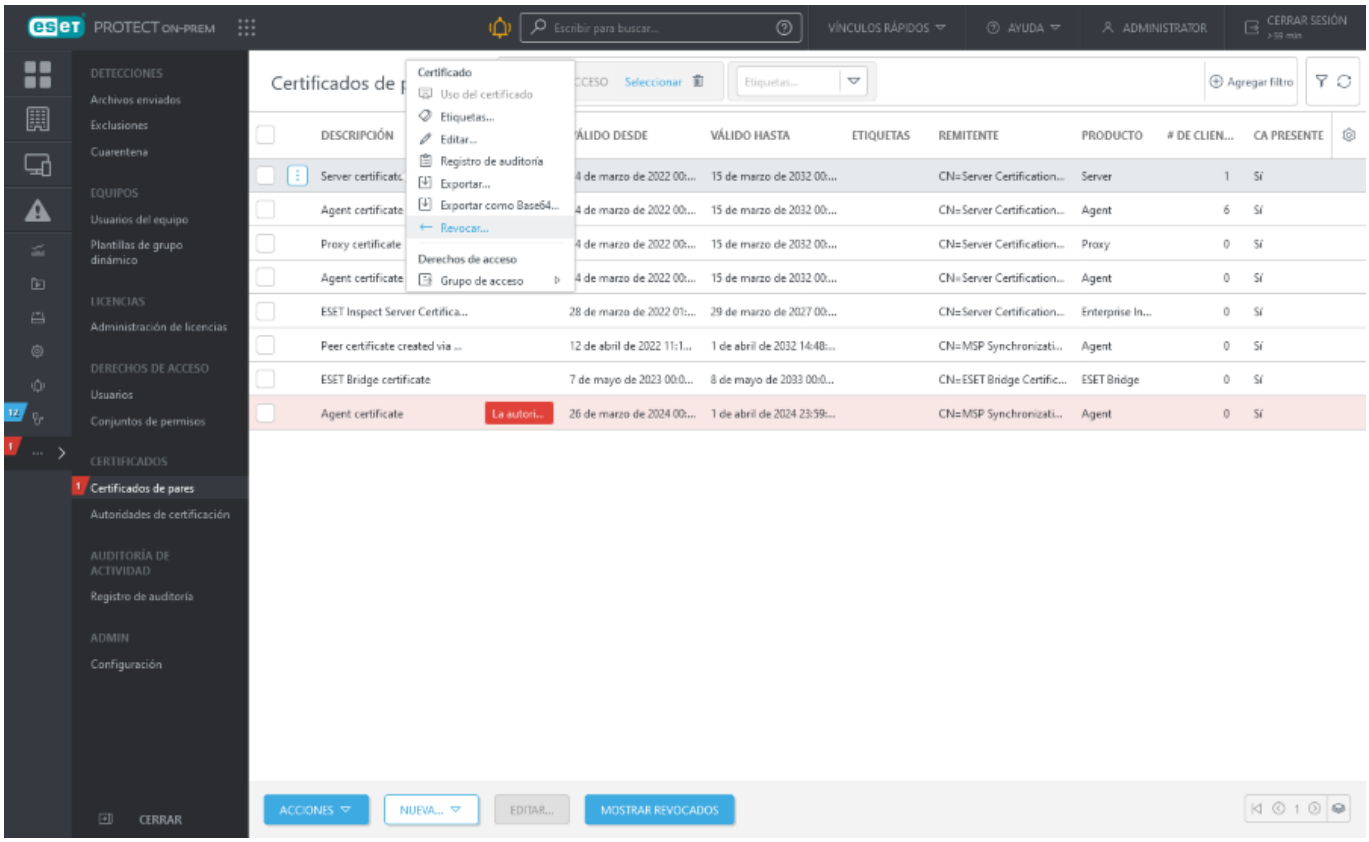
https://<mdmcore>:<enrollmentport>/unique_enrollment_token desde el navegador del dispositivo.

Mostrar revocados

La lista muestra todos los certificados que se han creado y, luego, invalidado por el servidor ESET PROTECT. Los certificados revocados se eliminarán automáticamente desde la pantalla principal de **Certificado de pares**. Haga clic en **Mostrar revocado para ver** certificados que se han revocado desde la ventana principal.

Para revocar un certificado, siga estos pasos:

1. Vaya a **Más** > **Certificado de pares** >, seleccione un certificado y haga clic en **Revocar**.



2. Especifique el **Motivo** para la revocación y haga clic en **Revocar**.

3. Haga clic en **OK**. Este certificado desaparecerá del listado de Certificado de pares. Para consultar los certificados revocados anteriormente, haga clic en el botón **Mostrar revocados**.

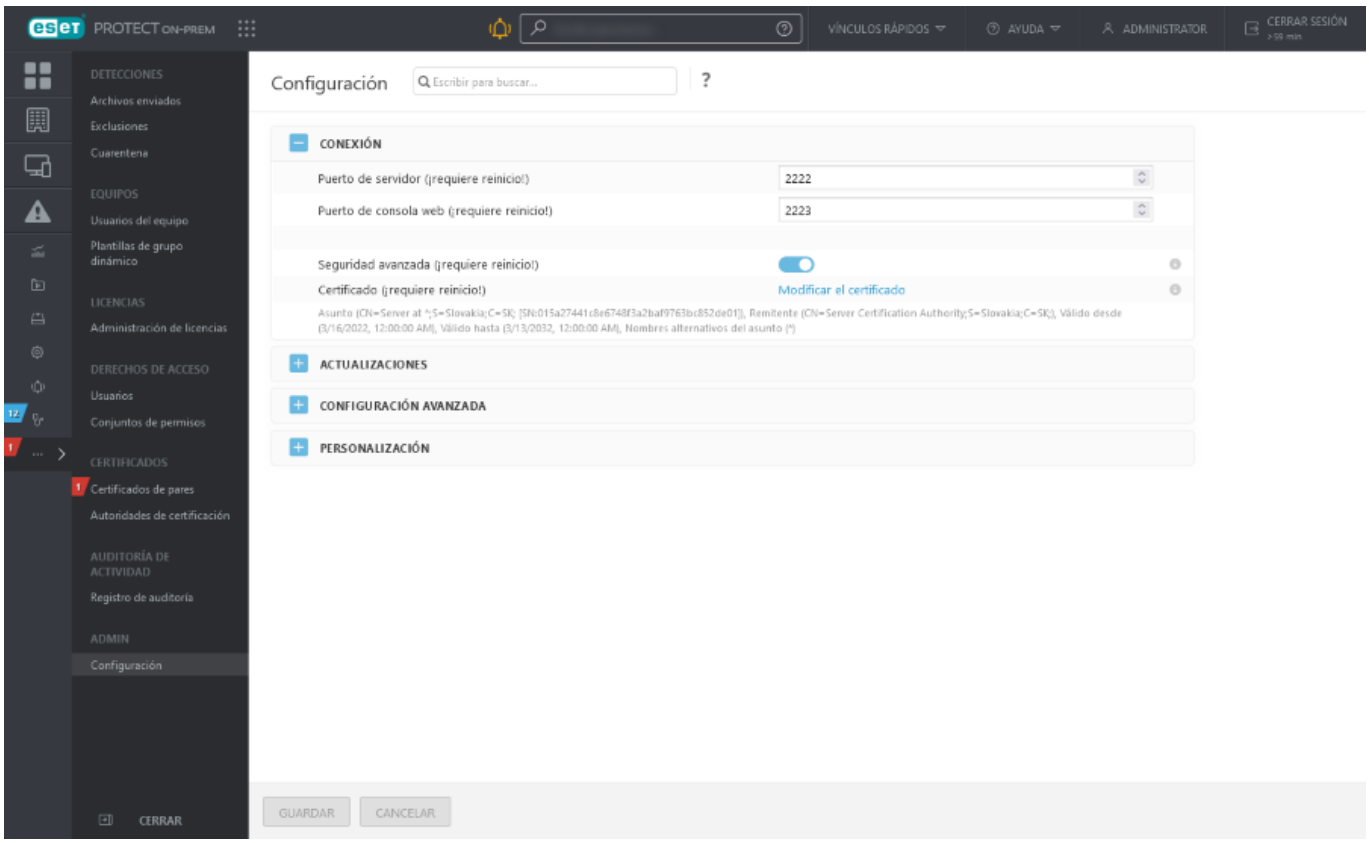
Establecer el nuevo certificado del servidor ESET PROTECT

Su certificado del servidor ESET PROTECT se crea durante la instalación y se distribuye a los agentes ESET Management y otros componentes para permitir la comunicación con el servidor ESET PROTECT.

- De ser necesario, puede configurar el servidor ESET PROTECT para usar un certificado de pares diferentes. Puede usar el certificado del servidor ESET PROTECT (generado automáticamente durante la instalación) o un **certificado personalizado**.

- El certificado del servidor ESET PROTECT es necesario para una conexión TLS segura y para la autenticación. El certificado del servidor se usa para asegurar que los agentes ESET Management y los proxy ESET PROTECT On-Prem no se conecten a un servidor ilegítimo.

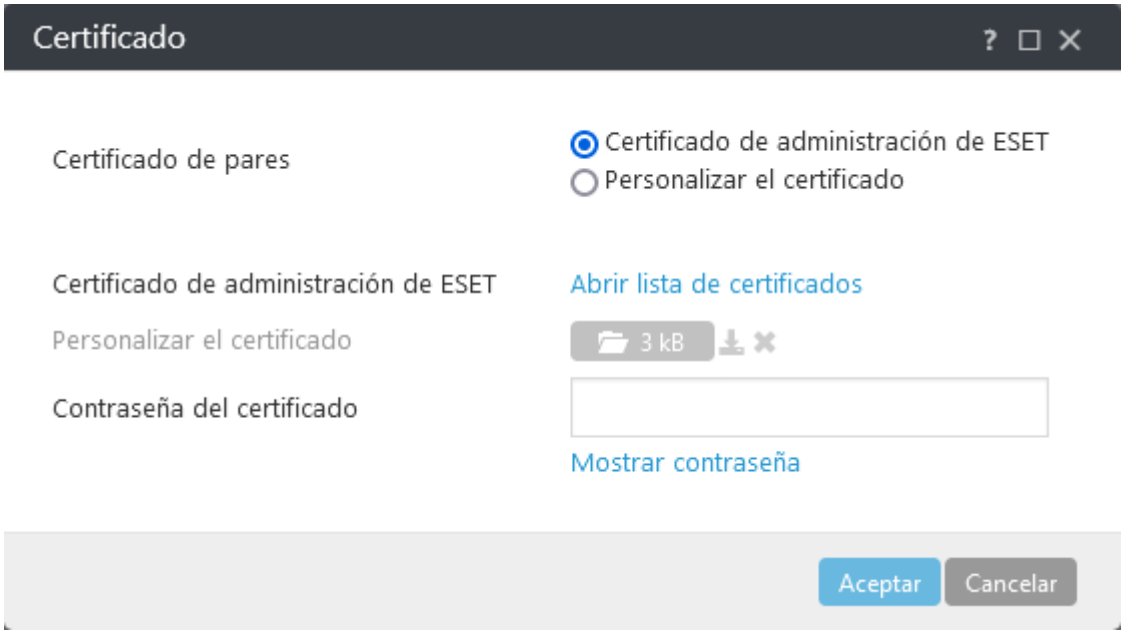
1. Haga clic en **Más** > **Configuraciones** >, expanda la sección **Conexión**, y seleccione **Cambiar certificado**.



2. Seleccione entre los dos tipos de certificado de pares:

- **Certificado de ESET Management:** haga clic en **Abrir lista de certificados** y seleccione el certificado que se va a usar.

- **Certificado personalizado:** busque su certificado personalizado y, luego, haga clic en **Aceptar** y **Guardar**. Si está realizando una migración, seleccione el archivo *.pfx* de certificado del servidor de ESET PROTECT que exportó de su servidor de ESET PROTECT anterior.



3. **Reinicie** el servicio del servidor ESET PROTECT, consulte nuestro artículo en la Base de conocimiento.

Certificados personalizados con ESET PROTECT On-Prem

Si tiene su propia PKI (infraestructura de clave pública) y desea ESET PROTECT On-Prem usar sus certificados personalizados para comunicación entre sus componentes, vea los siguientes ejemplos. Este ejemplo se realiza en Windows Server 2012 R2. Las capturas de pantalla pueden variar en otras versiones de Windows, aunque el procedimiento general permanece igual.

- No utilice certificados con una validez corta (por ejemplo, Let's Encrypt que sean válidos durante 90 días) para evitar el procedimiento complejo de su sustitución frecuente.
- Si administra dispositivos móviles, no se recomienda utilizar certificados autofirmados (incluidos certificados firmados por la autoridad de certificación ESET PROTECT On-Prem), ya que no todos los dispositivos móviles permiten a los usuarios aceptar certificados autofirmados. Se recomienda utilizar un certificado personalizado proporcionado por una autoridad certificadora de terceros.

Puede utilizar OpenSSL para crear nuevos certificados autofirmados. Para más información, consulte nuestro artículo de la Base de conocimiento.

Roles de servidor necesarios:

- Servicios de dominio de Active Directory.
- Servicios de certificados de Active Directory con el AC raín independiente.

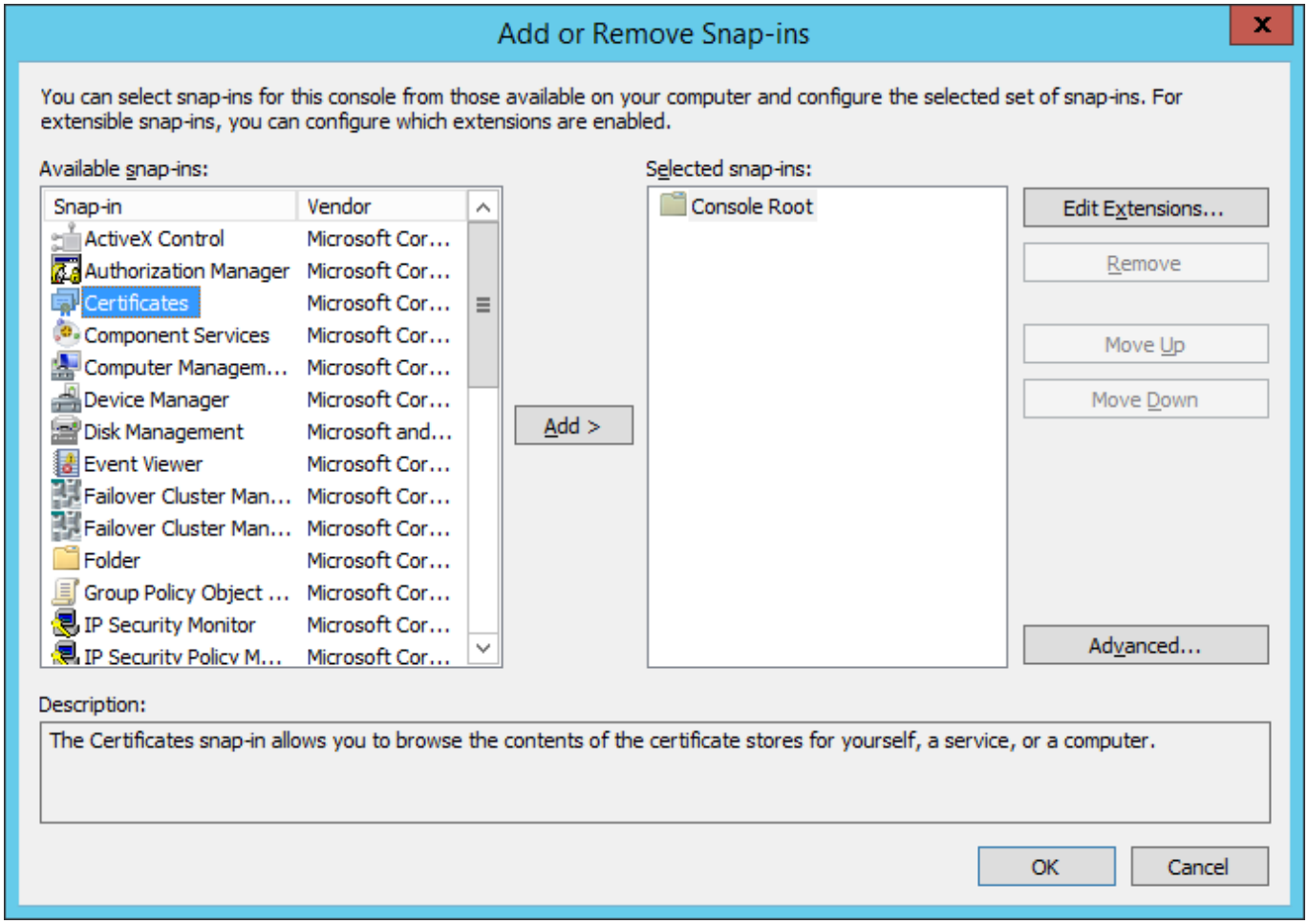
1. Abra la **Consola de gestión** y agregue las extensiones de los **Certificados**:

   a)Inicie sesión en el servidor como miembro del grupo de administrador local.

   b)Ejecute mmc.exe para abrir la consola de administración.

   c)Haga clic en el **Archivo** y seleccione **Agregar/Eliminar extensión…** (**o presione CTRL+M**).

d)Seleccione **Certificados** en el panel izquierdo y haga clic en **Agregar**.



e)Seleccione **Cuenta del equipo** y haga clic en **Siguiente**.

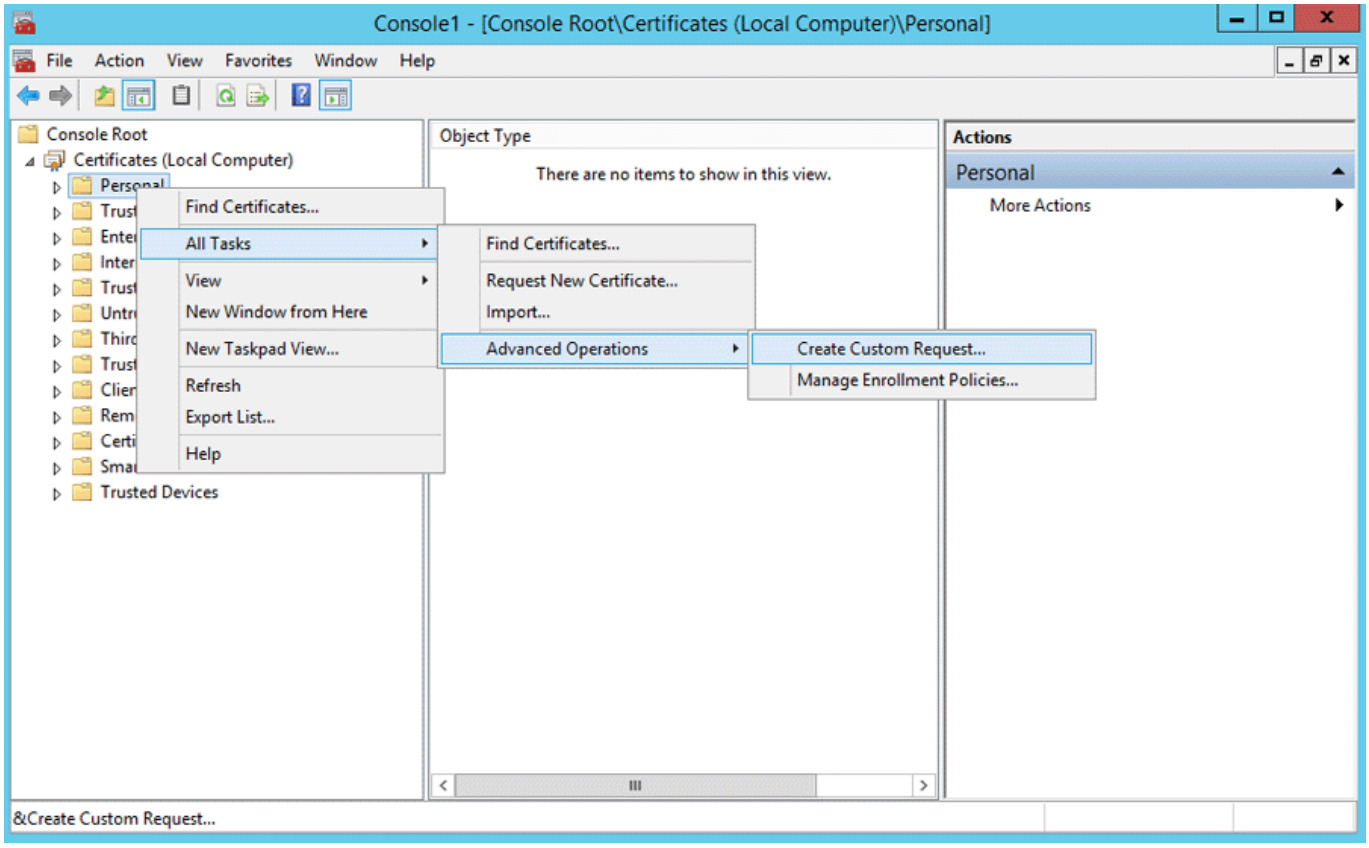
f)Asegúrese de seleccionar **Equipo local** (predeterminado) y haga clic en **Finalizar**.

g)Haga clic en **OK**.

2. Cree una **Solicitud de certificado personalizado**:

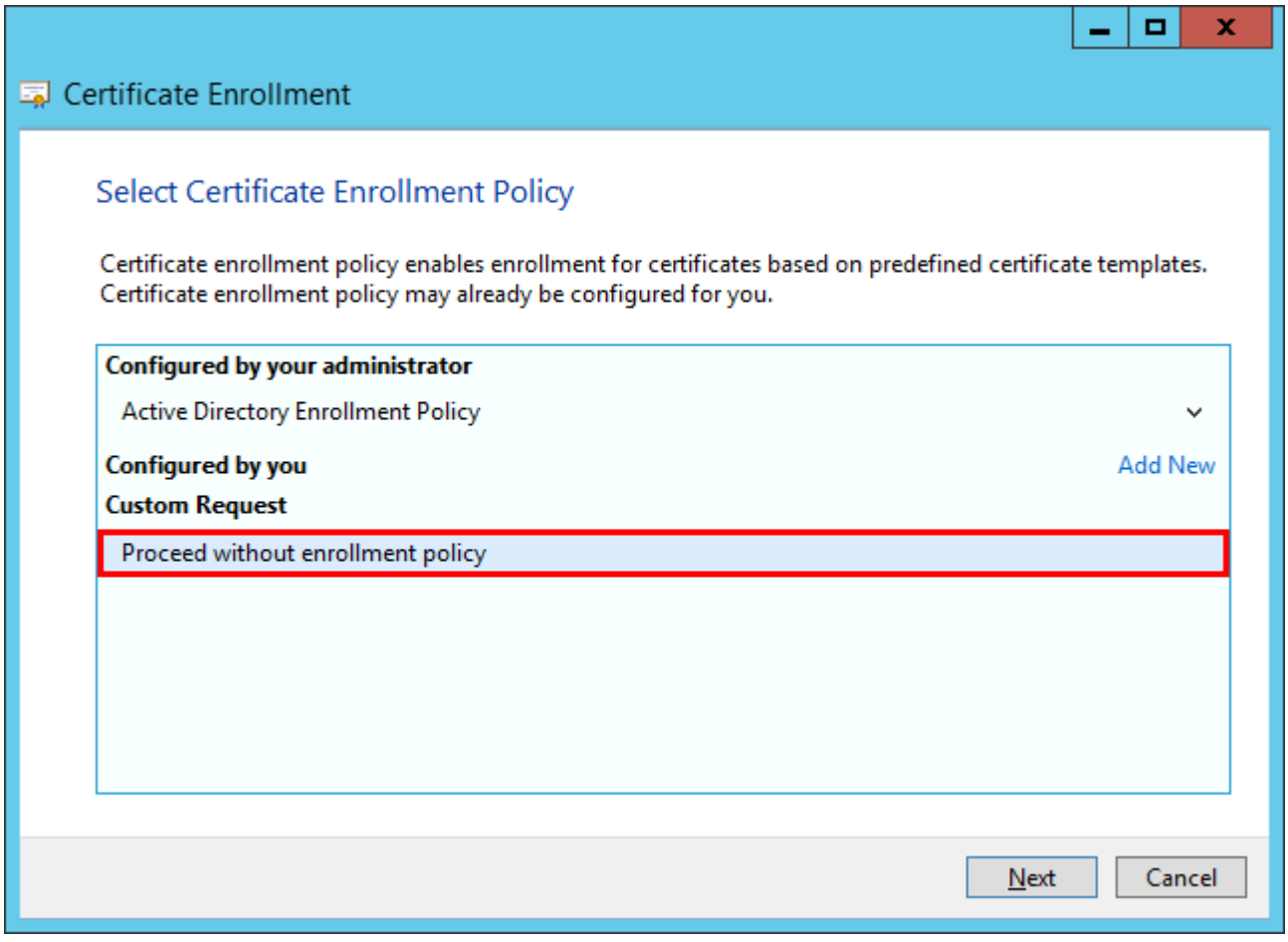
a)Haga doble clic en **Certificados (Equipo local)** para expandirlo.

b)Haga doble clic en Personal para expandirlo. Haga clic con el botón secundario en Certificados y seleccione Todas las tareas > Operaciones avanzadas y elija Crear solicitud personalizada

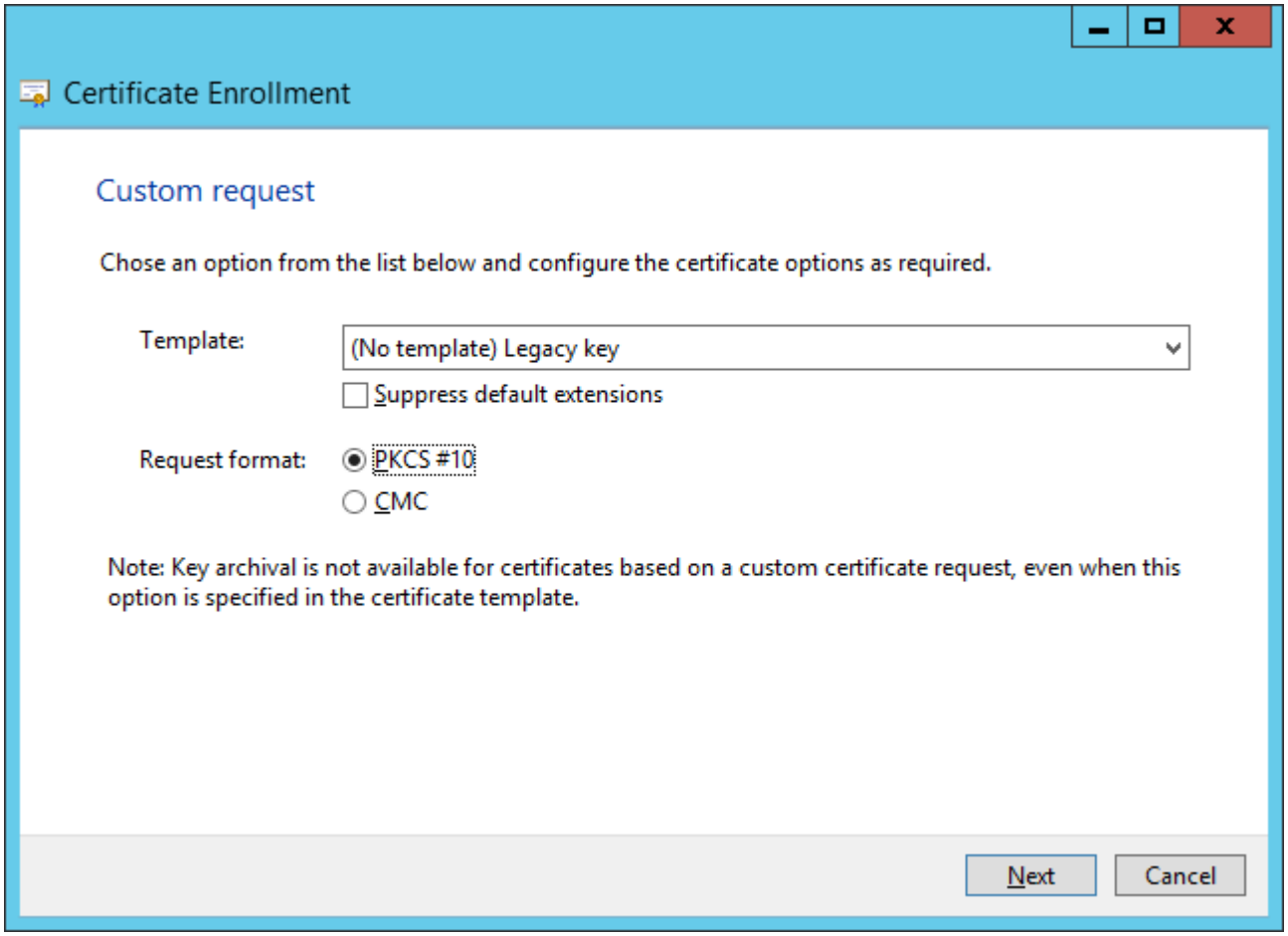


c)Se abrirá la ventana del asistente de inscripción de certificados, haga clic en **Siguiente**.

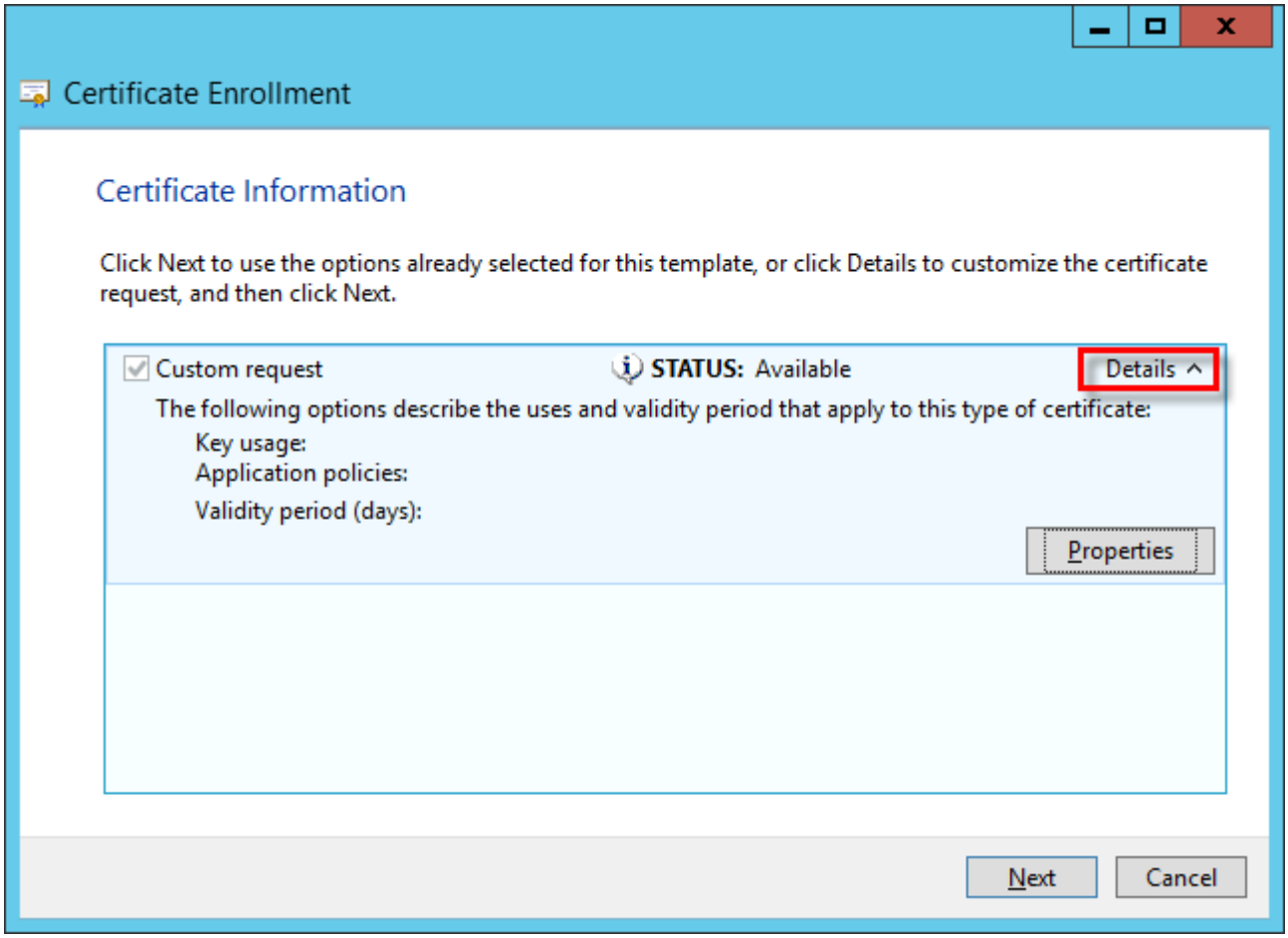
d)Seleccione la opción **Continuar sin política de inscripción** y haga clic en **Siguiente** para continuar.



e)Elija **Clave heredada (sin plantilla)** de la lista desplegable y asegúrese de seleccionar el formato de solicitud **PKCS #10**. Haga clic en **Siguiente**.



f)Haga clic en la flecha para expandir la sección **Detalles** y, luego, haga clic en **Propiedades**.



g)En la pestaña **General**, escriba un **nombre simple** para su certificado o también puede escribir la Descripción (opcional).

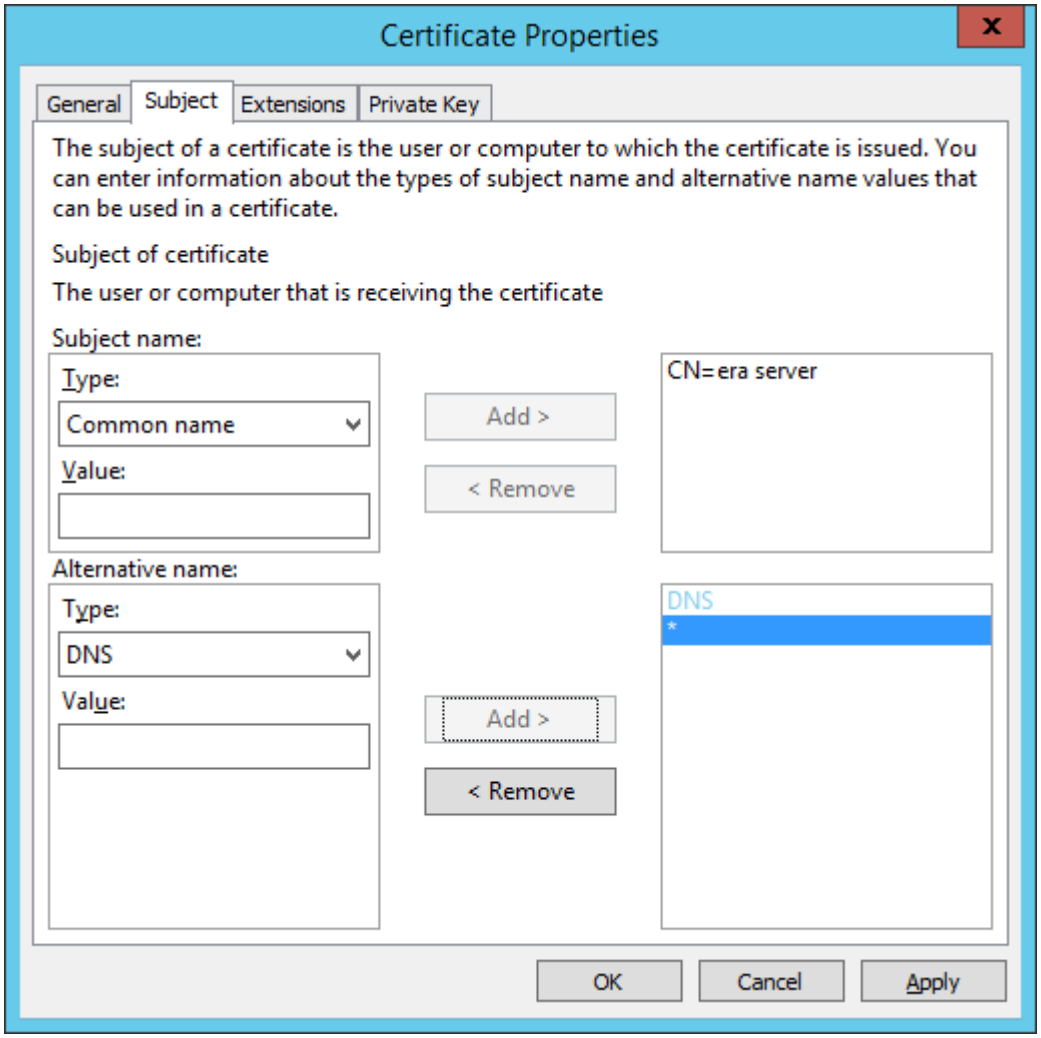
h)En la pestaña **Asunto**, haga lo siguiente:

En la sección **Nombre del asunto**, seleccione **Nombre común** de la lista desplegable en **Tipo** e ingrese `era server` en el campo **Valor**, luego haga clic en **Agregar**. **CN=era server** aparecerá en el cuadro de información de la derecha. Si está creando una solicitud de certificado para el agente ESET Management, ingrese `era agent` en el campo del valor del nombre común.

El nombre común debe contener una de las siguientes cadenas: "**servidor**« o "**agente**"", según qué solicitud de certificado desea crear.

i)En la sección **Nombre alternativo**, seleccione **DNS** de la lista desplegable en **Tipo** y escriba * (asterisco) en el campo **Valor** y, luego, haga clic en el botón **Agregar**.

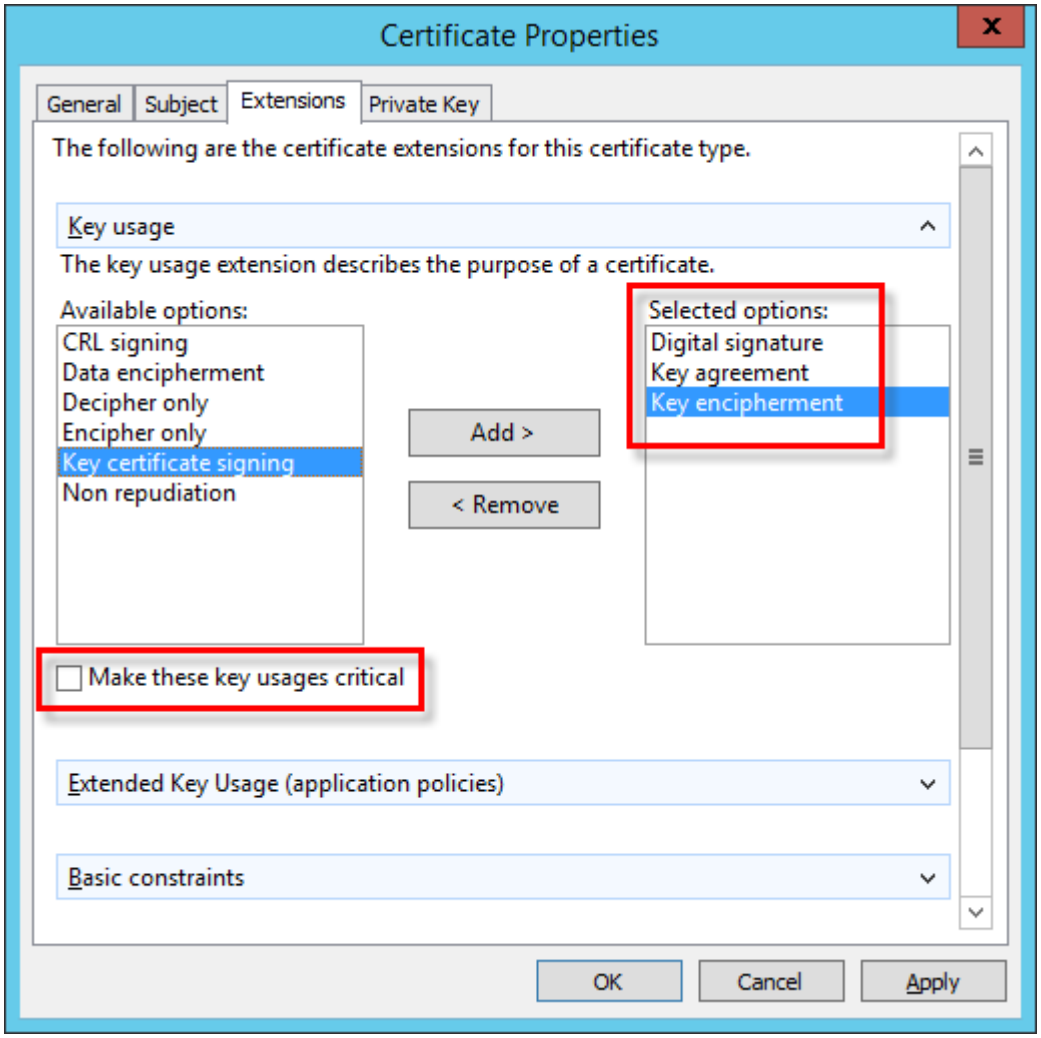
El Nombre Alternativo del Sujeto (SAN) debería definirse como “DNS:*” para el servidor de ESET PROTECT y todos los agentes.



j)En la pestaña **Extensiones**, expanda la sección **Uso de clave**; para ello, haga clic en la flecha. Agregue lo siguiente a partir de las opciones disponibles: **Firma digital**, **Acuerdo clave**, **Cifrado de claves**. Anule la selección de la opción **Hacer críticos estos usos de claves**.

Asegúrese de seleccionar estas 3 opciones en **Uso de claves** > **Firma de certificados clave**:

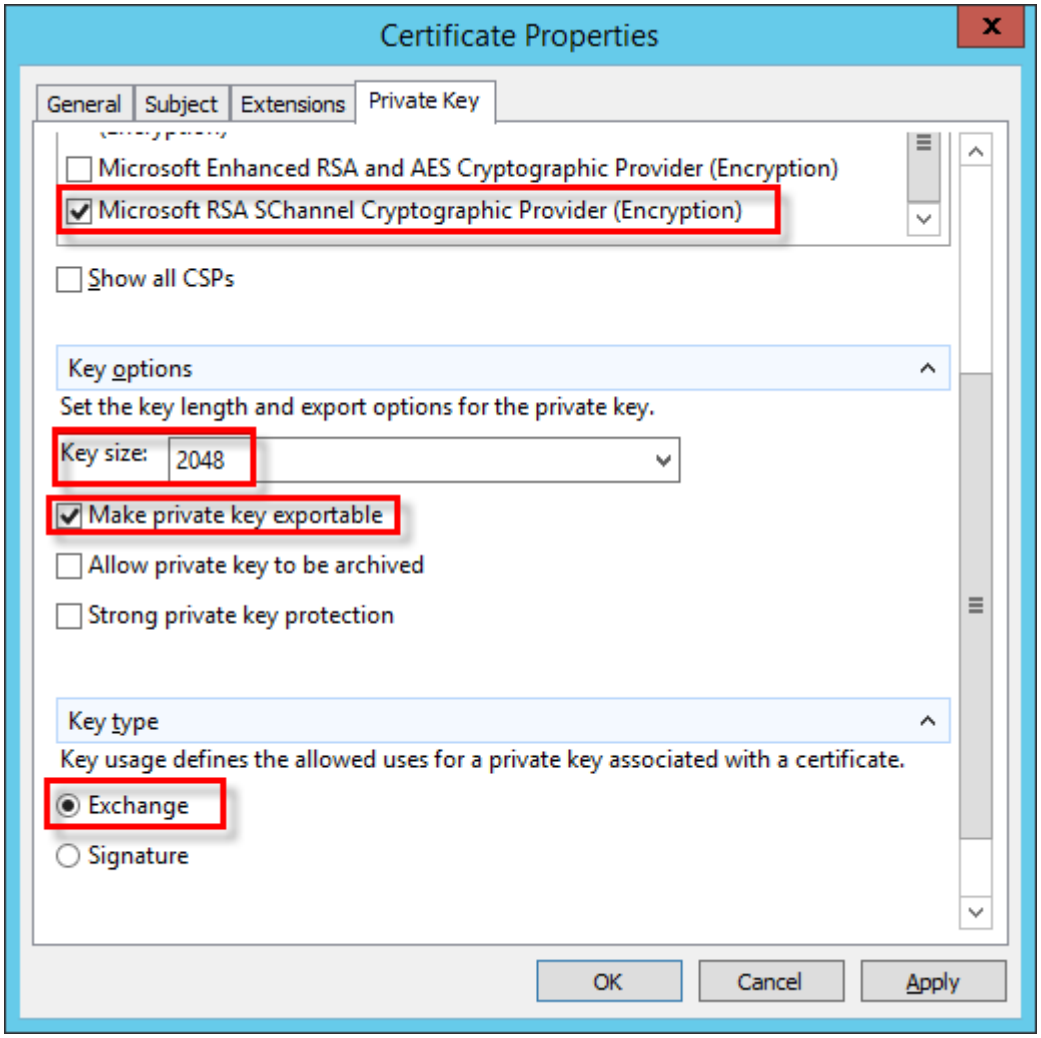
- **Firma digital**
- **Acuerdo clave**
- **Cifrado de clave**



k)En la pestaña **Clave privada**, haga lo siguiente:

i.Expanda la sección **Proveedor de servicios criptográficos**; para ello, haga clic en la flecha. Se mostrará una lista de proveedores de servicio criptográficos (CSP). Asegúrese de seleccionar solo **Proveedor criptográfico de canales S de Microsoft RSA (Cifrado)**.

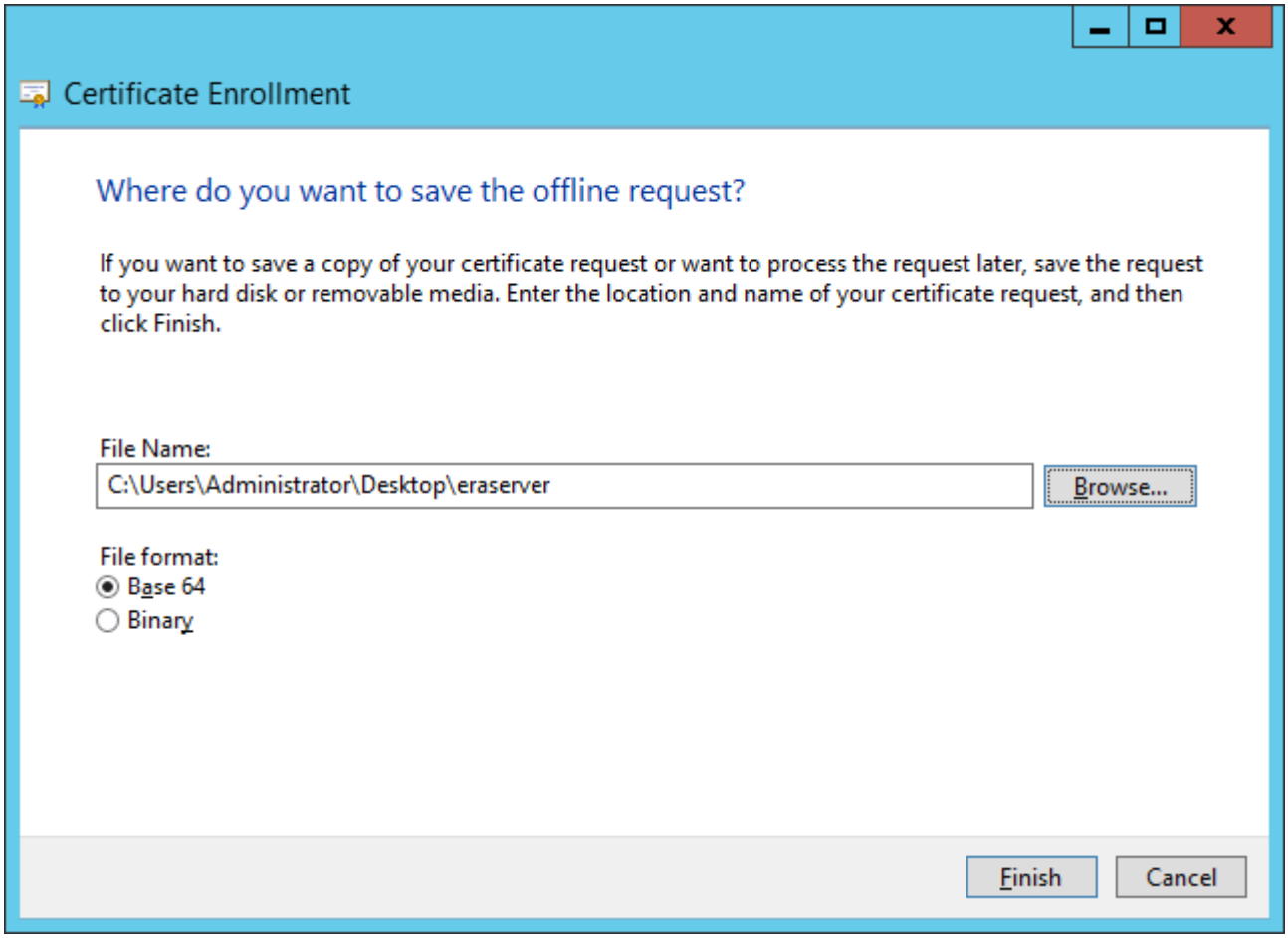
> Anule la selección de los demás CSP, excepto la opción **Proveedor criptográfico de canales S de Microsoft RSA (Cifrado)**.



i.Expanda la sección **Opciones de claves**. En el menú **Tamaño de claves**, configure un valor de al menos **2048**. Seleccione **Hacer exportable la clave privada**.

ii.Expanda la sección **Tipo de clave** y seleccione **Exchange**. Haga clic en **Aplicar** y compruebe su configuración.

l)Haga clic en **OK**. Se mostrará la información de los certificados. Haga clic en el botón **Siguiente** para continuar. Haga clic en **Navegar** para seleccionar la ubicación donde se guardará la solicitud de firma del certificado (CSR). Escriba el nombre del archivo y asegúrese de que esté seleccionada **Base 64**.

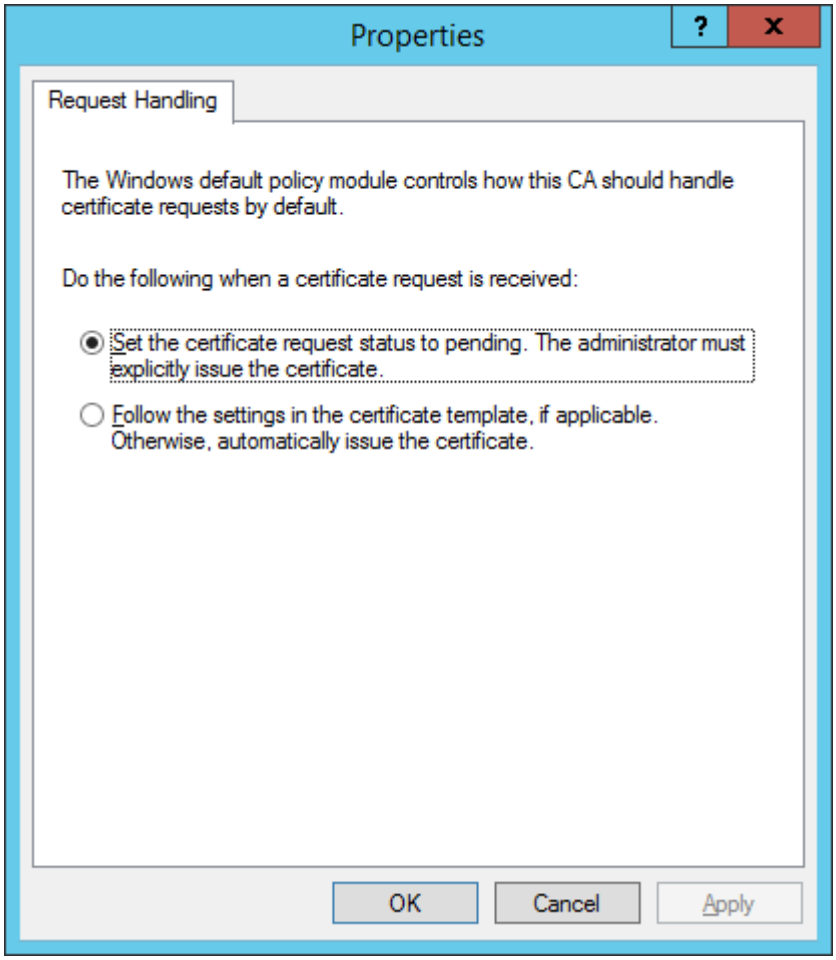


m)Haga clic en **Finalizar** para generar el CSR.

3. Para importar la solicitud de certificados personalizados, siga los siguientes pasos:

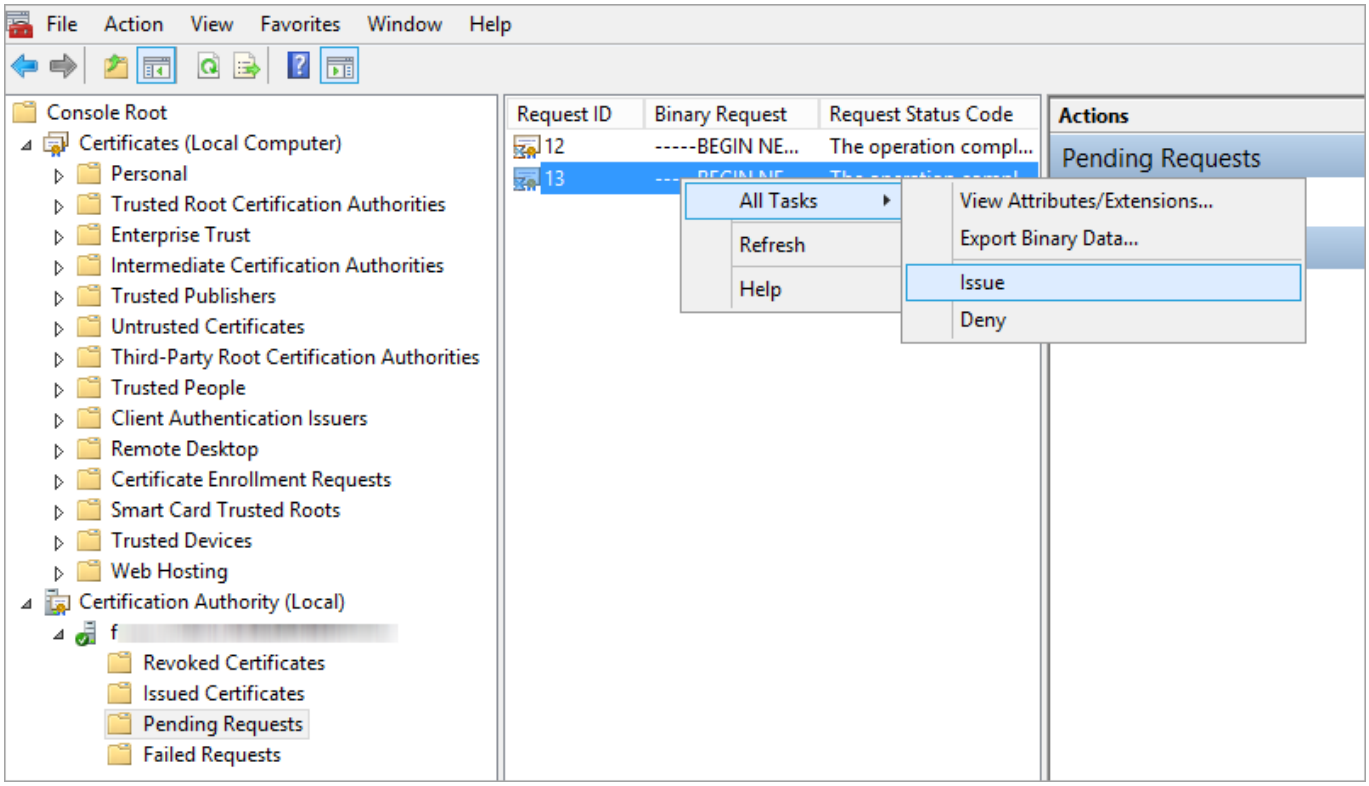
a)Abra Server Manager y haga clic en **Herramientas** > **Autoridad de certificación**.

b)En el árbol **Autoridad de certificación (Local)**, seleccione la pestaña **Su servidor** (generalmente FQDN) > **Propiedades** y seleccione la pestaña **Módulo de políticas**, Haga clic en **Propiedades** y seleccione **Configurar el estado de solicitud del certificado a pendiente. El administrador debe emitir explícitamente el certificado**. De lo contrario, no funcionará de manera adecuada. Debe reiniciar los servicios del certificado Active Directory si necesita cambiar esta configuración.



c)En el árbol **Autoridad de certificación (Local)**, seleccione **Su servidor (generalmente FQDN)** > **Todas las tareas** > **Enviar nueva solicitud...** y vaya al archivo **CSR** generado previamente en el paso 2.

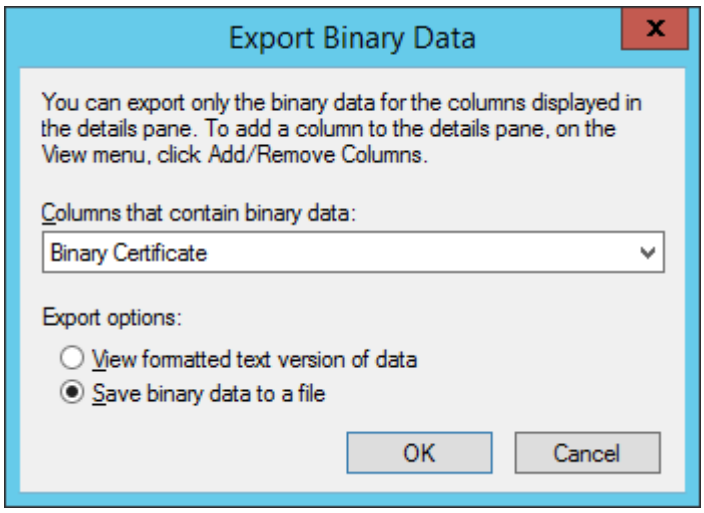
d)El certificado se agregará a **Solicitudes pendientes**. Seleccione **CSR** en el panel de navegación derecha. En el menú **Acción**, seleccione **Todas las tareas** > **Emitir**.



4. Exporte el **Certificado personalizado emitido** al archivo *.tmp*.

a)Seleccione Certificados **Emitidos** en el panel izquierdo. Haga clic con el botón secundario en el certificado que desea exportar y haga clic en **Todas las tareas** > **Exportar datos binarios**.

b)En el diálogo **Exportar datos binarios**, elija **Certificado binario** de la lista desplegable. En las **opciones Exportar**, haga clic en **Guardar datos binarios a un archivo** y luego haga clic en **Aceptar**.



c)En el cuadro de diálogo Guardar datos binarios, desplácese hacia la ubicación del archivo donde desea guardar el certificado y, luego, haga clic en **Guardar**.

5. Importe el archivo *..tmp*.

a)Vaya a Certificado (Equipo local) > haga clic con el botón secundario en Personal y seleccione Todas las tareas > Importar.

b)Haga clic en **Siguiente**.

c)Encuentre el archivo binario *.tmp* guardado previamente mediante **Explorar** y haga clic en **Abrir**. Seleccione Colocar todos los certificados en el siguiente almacenamiento > **Personal**. Haga clic en **Siguiente**.

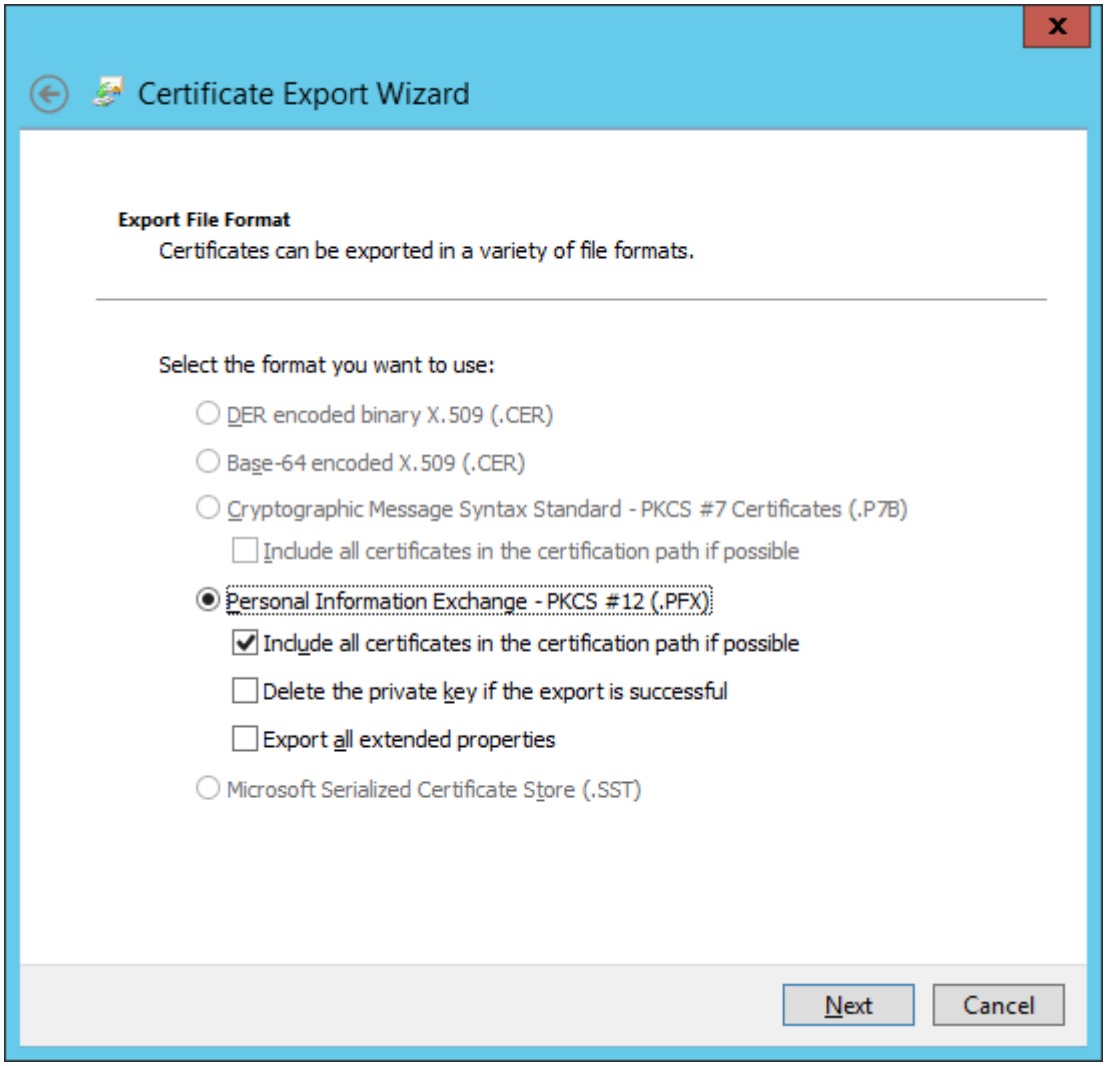
d)Haga clic en **Finalizar** para importar el certificado.

6. Exporte el certificado, incluida una clave privada al archivo *.pfx*.

a)En **Certificados (Equipo local)** expanda **Personal** y haga clic en **Certificados**, seleccione su nuevo certificado que desea exportar, en el menú **Acción**, apunte a **Todas las tareas** > **Exportar**...

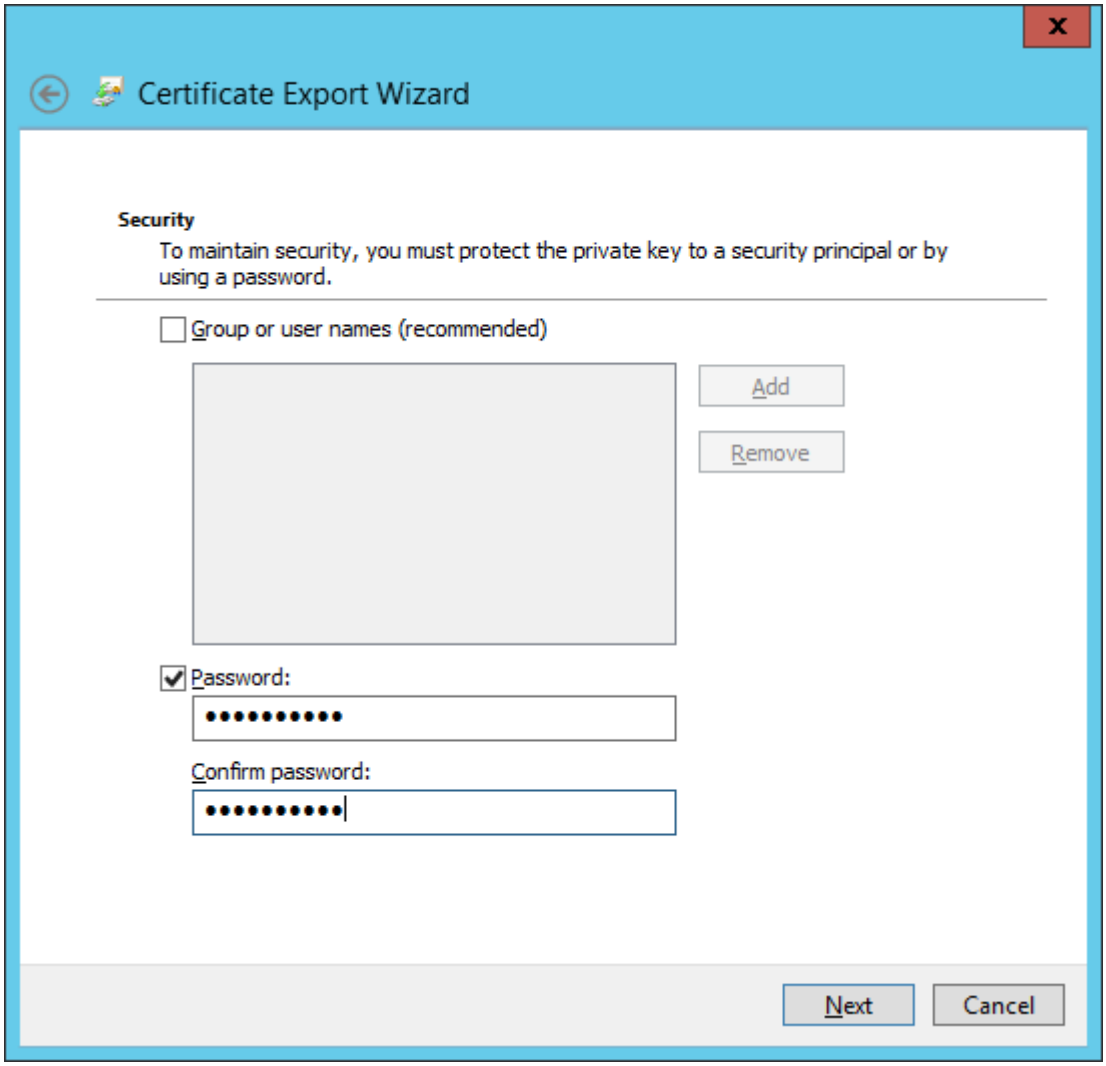
b)En el **Asistente de exportación de certificados**, haga clic en **Sí, exporte la clave privada**. (Esta opción aparecerá solo si la clave privada está marcada como exportable y tiene acceso a la clave privada).

c)En Formato de archivo de exportación, seleccione **Intercambio de información personal -PKCS #12 (.PFX)**, seleccione la casilla de verificación **Incluir todos los certificados en la ruta de certificación si es posible** y luego haga clic en **Siguiente**.



d)**Contraseña**, escriba una contraseña para cifrar la clave privada que está exportando. En el campo **Confirmar contraseña**, vuelva a escribir la misma contraseña y luego haga clic en **Siguiente**.

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



e)En **Nombre de archivo**, escriba un nombre de archivo y ruta para el archivo *.pfx* que almacenará el certificado exportado y la clave privada. Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

El ejemplo anterior le muestra cómo crear una certificado del servidor ESET Management. Repita los mismos pasos para los certificados del servidor ESET PROTECT.
Ahora puede usar este certificado para firmar otro certificado nuevo en la Consola Web.

7. Exportar autoridad de certificación:

a)Abra Server Manager y haga clic en **Herramientas** > **Autoridad de certificación**.

b)En el árbol **Autoridad de certificación (Local)**, seleccione la pestaña **Su servidor (generalmente FQDN)** > **Propiedades** > **General** y haga clic en **Ver certificado**.

c)En la pestaña **Detalles**, haga clic en **Copiar a archivo**. Se abrirá el **Asistente de exportación de certificados**.

d)En la ventana **Exportar formato de archivos**, seleccione **DER codificado binario X.509 (.CER)** y haga clic en **Siguiente**.

e)Haga clic en **Navegar** para seleccionar la ubicación donde se guardará el archivo *.cer* y haga clic en **Siguiente**.

f)Haga clic en **Finalizar** para exportar la autoridad de certificación.

Para obtener instrucciones paso a paso para usar certificados personalizados en ESET PROTECT On-Prem, consulte el siguiente capítulo.

Cómo usar un certificado personalizado con ESET PROTECT On-Prem

Para continuar desde el capítulo anterior:

1. Importe su autoridad de certificación de terceros en la consola web de ESET PROTECT.

2. Configure un nuevo certificado de servidor personalizado en la consola web ESET PROTECT.

Si ya conectó los agentes ESET Management al servidor ESET PROTECT, aplique una política para cambiar el certificado personalizado por los agentes ESET Management:
1.Abra la consola web ESET PROTECT.
2.Haga clic en **Políticas** > **Nuevo**. Ingrese un nombre para la política.
3.Expanda **Configuración** y seleccione el agente **ESET Management** en el menú desplegable.
4.Expanda **Conexión** y haga clic en **Cambiar certificado** junto a **Certificado**.
5.Haga clic en **Certificado personalizado** y seleccione el certificado personalizado para el agente ESET Management.
6.Ingrese una contraseña para el certificado y haga clic en **Aceptar**.
7.Asigne esta política a todos los clientes.

3. Vaya a **Inicio** > **Programas y características**, haga clic con el botón derecho en **Agente ESET Management** y seleccione **Cambiar**.

4. Haga clic en el botón **Siguiente** y ejecute **Reparar**.

5. No cambie la configuración del servidor y el puerto del servidor y haga clic en **Siguiente**.

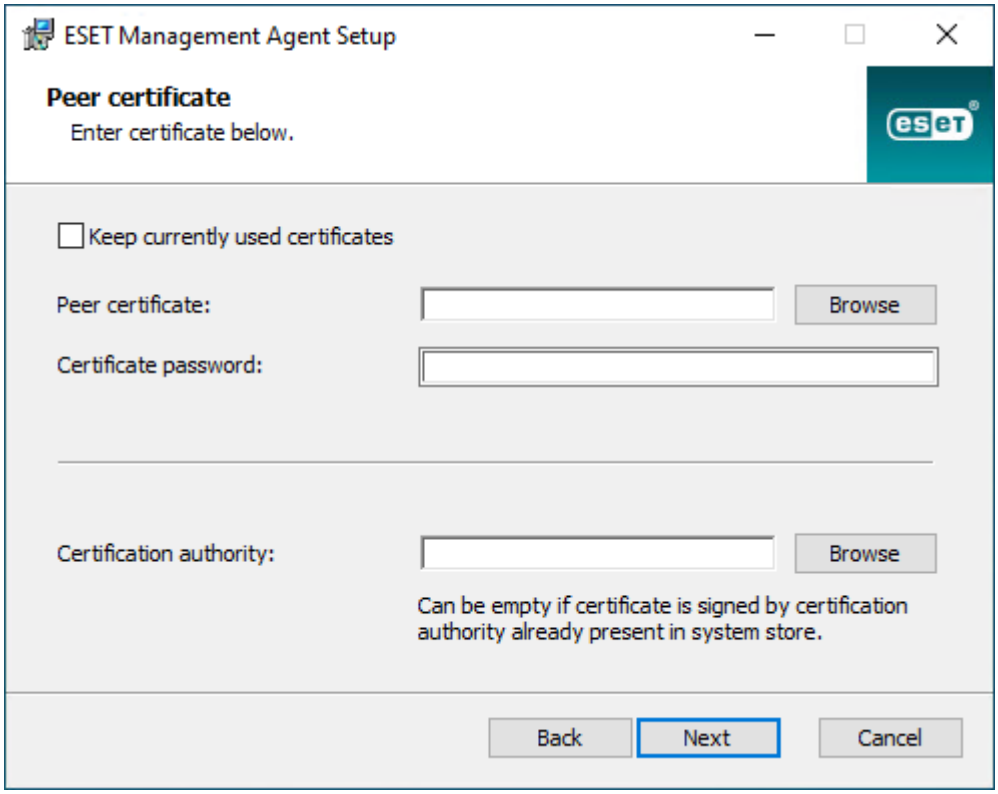
6. Haga clic en el botón **Navegar** junto a **Certificado de pares** y encuentre el archivo personalizado.*pfx*.

7. Escriba la contraseña del certificado que especificó en el paso 6.

8. Haga clic en **Navegar** junto a la **autoridad de certificación y seleccione el archivo** .der (clave pública) exportado desde la consola web. Debe ser una clave pública que firma el certificado personalizado.

9. Haga clic en **Siguiente** y complete la reparación.

10. Ahora, el agente ESET Management usa un certificado *.pfx*.



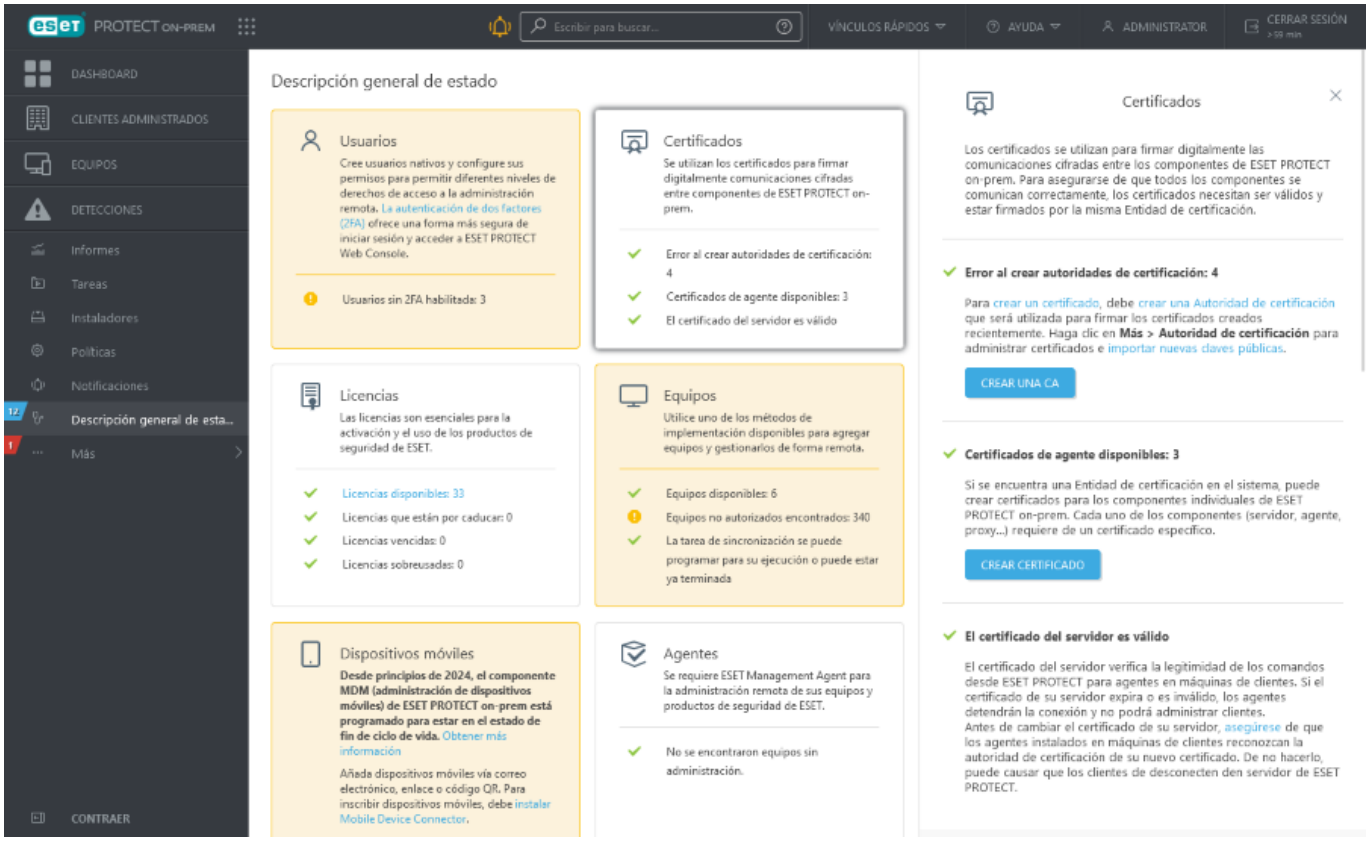
Certificado vencido - informe y reemplazo

ESET PROTECT On-Prem está habilitado para notificarle acerca de un certificado o una autoridad de certificación que se vencerá. Existen **Notificaciones** predefinidas para el certificado de ESET PROTECT y para la autoridad de certificación de ESET PROTECT en la pestaña de **Notificaciones**.

Para activar esta característica, haga clic en **Editar la notificación** y especifique los detalles en la sección Distribución, como la dirección de correo electrónico o la captura de SNMP. Cada usuario puede ver únicamente las notificaciones de aquellos certificados en su grupo hogar (siempre y cuando tenga permisos de **Lectura** para **Certificados**).

> Asegúrese de primero haber configurado los ajustes de la conexión SMTP en **Más** > **Ajustes.** Una vez realizado, puede editar la notificación para agregar una dirección de correo electrónico de distribución.

La consola web de ESET PROTECT informa de una advertencia si un certificado o una entidad de certificación está a punto de caducar en menos de 90 días. La advertencia aparece en Equipos, Información general sobre el estado, Certificados del mismo nivel y Entidades de certificación.



Para reemplazar una Autoridad de certificación o Certificado vencido, siga estos pasos:

1. Cree una nueva autoridad de certificación con un nuevo período de validez (si el anterior está por vencer), de ser posible que sea válida inmediatamente.

2. Cree un nuevo Certificados de pares para el Servidor de ESET PROTECT y otros componentes (agente/MDM) dentro del período de validez de la nueva autoridad de certificación.

3. Cree directivas para establecer nuevos Certificados del mismo nivel. Aplique las políticas a los componentes de ESET PROTECT, MDM y al agente ESET Management en todos los equipos clientes de la red.

4. Espere hasta que la nueva Autoridad de certificación y Certificados del mismo nivel se apliquen y se repliquen en los clientes.

> Le recomendamos esperar 24 horas o comprobar si todos los componentes (agentes) de ESET PROTECT se han replicado al menos dos veces. Puede replicar el agente en **Equipos** haciendo clic en el equipo y seleccionando **Enviar llamada de reactivación**.

5. Reemplace el certificado del servidor en Configuración del servidor ESET PROTECT así los clientes están habilitados para la autenticación usando los nuevos certificados de pares.

6. Reinicie el servicio del Servidor ESET PROTECT.

7. Una vez que haya completado todos los pasos anteriores, cada cliente se conecta a ESET PROTECT On-Prem y todo funciona como se espera, revoque los certificados de pares anteriores y la autoridad de certificación anterior.

Autoridades de certificación

En la sección **Autoridades de certificado,** se enumeran y administran las Autoridades del certificado. Si dispone de varias autoridades de certificación, puede aplicar un filtro para ordenarlos.

> Se acceden a las autoridades de certificación y a los certificados con los mismos permisos que para la función **Certificados**. Los certificados y las autoridades creados durante la instalación, y aquellos que el administrador cree luego, se encuentra en el grupo estático **Todos**. Consulte la lista de permisos para obtener más información sobre los derechos de acceso.

Haga clic en **Acciones** para administrar la Autoridad de certificación seleccionada:

- **Nuevo**: cree una nueva autoridad de certificación
- **Etiquetas** - Editar etiquetas (asignar, desasignar, crear, quitar).
- **Editar**: edita la descripción de la autoridad de certificación.
- **Registro de auditoría** - Ver el registro de auditoría del elemento seleccionado.
- **Quitar**: quite la Autoridad de certificación seleccionada
- Importar clave pública
- Exportar clave pública: utilice esta opción para hacer una copia de seguridad de sus autoridades de certificación.
- **Grupo de acceso** > **Mover** – Mueva el objeto a otro grupo estático en el que esté disponible para los usuarios que tienen derechos suficientes para el grupo de destino. Cambiar el grupo de acceso es útil cuando se resuelven problemas de acceso con otros usuarios. El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario.

Personalización del diseño y de los filtros

Puede personalizar la vista de la pantalla de la consola web actual:

- Administre el panel lateral y la tabla principal.
- Agregar filtro y filtros preestablecidos. Puede usar etiquetas para filtrar los elementos mostrados.

Cómo dividir el acceso a certificados y autoridades

Si el *Administrador* no desea que el usuario *John* pueda acceder a las autoridades de certificación de ESET PROTECT, pero necesita que pueda trabajar con certificados, el administrador debe seguir estos pasos:

1. Crear un nuevo grupo estático llamado *Certificados*.
2. Crear un nuevo Conjunto de permisos.
   a. Nombrar este conjunto de permisos *Permisos para certificados*.
   b. Agregar un grupo llamado *Certificados* en la sección **Grupos estáticos**.
   c. En la sección **Funcionalidad**, seleccionar **Escribir** para **Certificados**.
   d. En la sección **Usuarios**, hacer clic en **Usuarios nativos** y seleccionar *John.*
   e. Hacer clic en **Finalizar** para guardar el conjunto de permisos.
3. Mover los certificados desde el grupo **Todos** al recientemente creado *grupo* **Certificados:**
   a. Navegar a **Más** > **Certificados de pares**.
   b. Seleccionar las casillas de verificación junto a los certificados que desea mover.
   c. Hacer clic en **Acciones** > **Grupo de acceso**, seleccionar el grupo **Certificados** y, luego, hacer clic en **Aceptar**.

Ahora *John* puede modificar y usar los certificados trasladados. Sin embargo, las autoridades de certificación se encuentran almacenadas fuera del alcance de este usuario. *John* no será capaz, incluso, de usar las autoridades existentes (del grupo **Todos**) para firmar certificados.

Cree una nueva autoridad de certificación

Para crear una nueva autoridad certificadora, vaya a **Más** > **Autoridad de certificación** y haga clic en **Acción** > **Nuevo** , en la parte inferior de la página.

Autoridad de certificación

Ingrese una **Descripción** de la Autoridad de certificación y seleccione una **Frase de contraseña**. Esta **Frase de contraseña** debe contener al menos 12 caracteres.

Atributos (asunto)

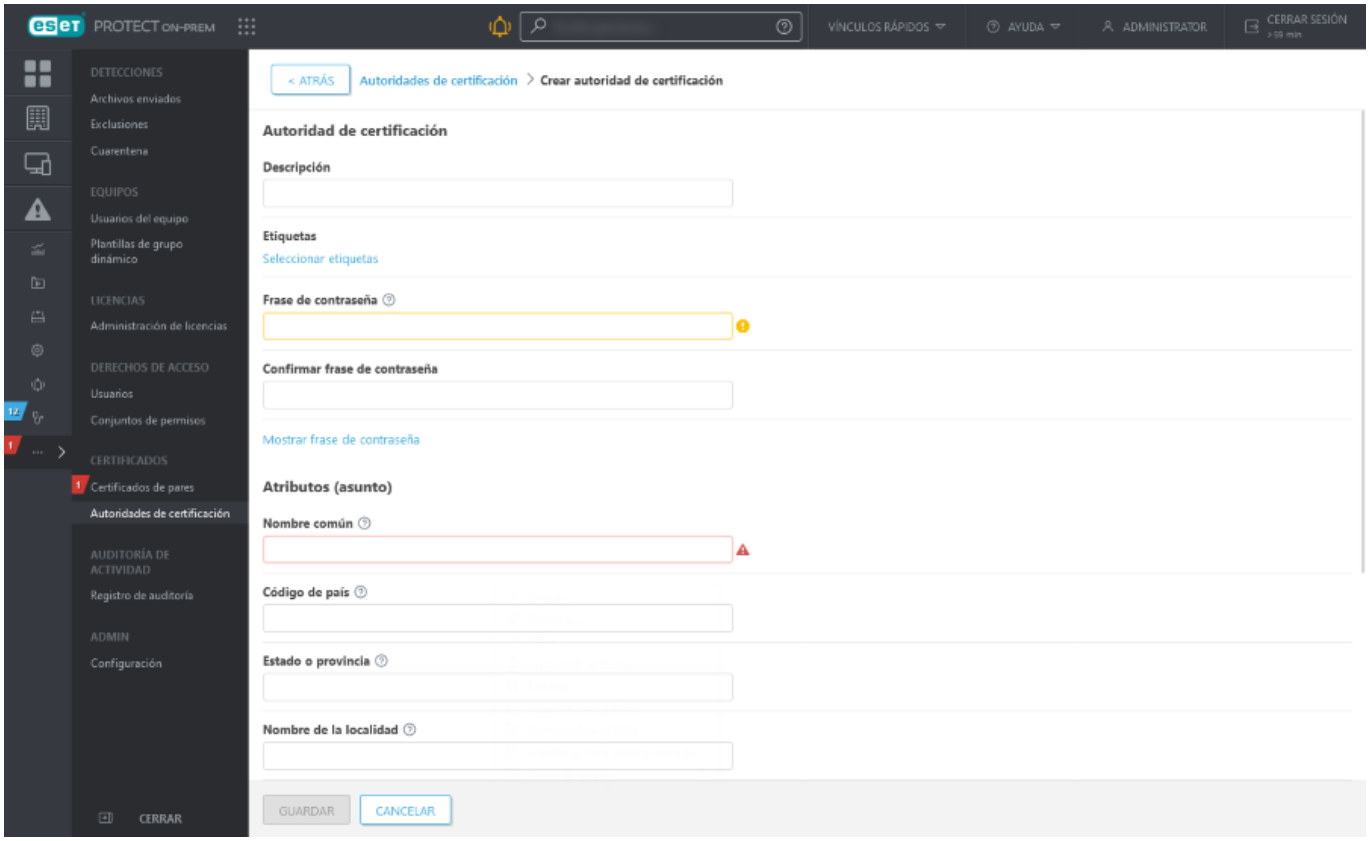
1. Ingrese un **Nombre común** (nombre) de la Autoridad de certificación. Seleccione un nombre único para diferenciar las varias Autoridades de certificado. Opcionalmente, puede ingresar una descripción acerca de la Autoridad del certificado.

2. Ingrese los valores **Válido desde** y **Válida hasta** para asegurarse de que el certificado sea válido.

Para todos los certificados y las autoridades de certificación que se crean durante la instalación de los componentes de ESET PROTECT, el valor Válido desde se establece a 2 días antes de la creación del certificado.
Para todos los certificados y las autoridades de certificación que se crean durante la consola web ESET PROTECT, el valor Válido desde se establece a 1 día antes de la creación del certificado. La razón para esto es cubrir todas las posibles discrepancias de tiempo entre los sistemas afectados.
Por ejemplo, una autoridad de certificación y un certificado, que se crean el 12 de enero de 2017 durante la instalación, tendrán un valor predefinido de Válido desde el 10 de enero de 2017 00:00:00, y una autoridad de certificación y un certificado que se crean el 12 de enero de 2017 en la consola web ESET PROTECT tendrá un valor predefinido Válido desde el 11 de enero de 2017 00:0:00.

3. Haga clic en **Guardar** para guardar su nueva Autoridad de certificación. Ahora se encuentra en la lista Autoridad de certificación bajo **Más** > **Autoridad de certificación**, y está lista para ser usada. La autoridad de

certificación se crea en el grupo hogar del usuario que la crea.



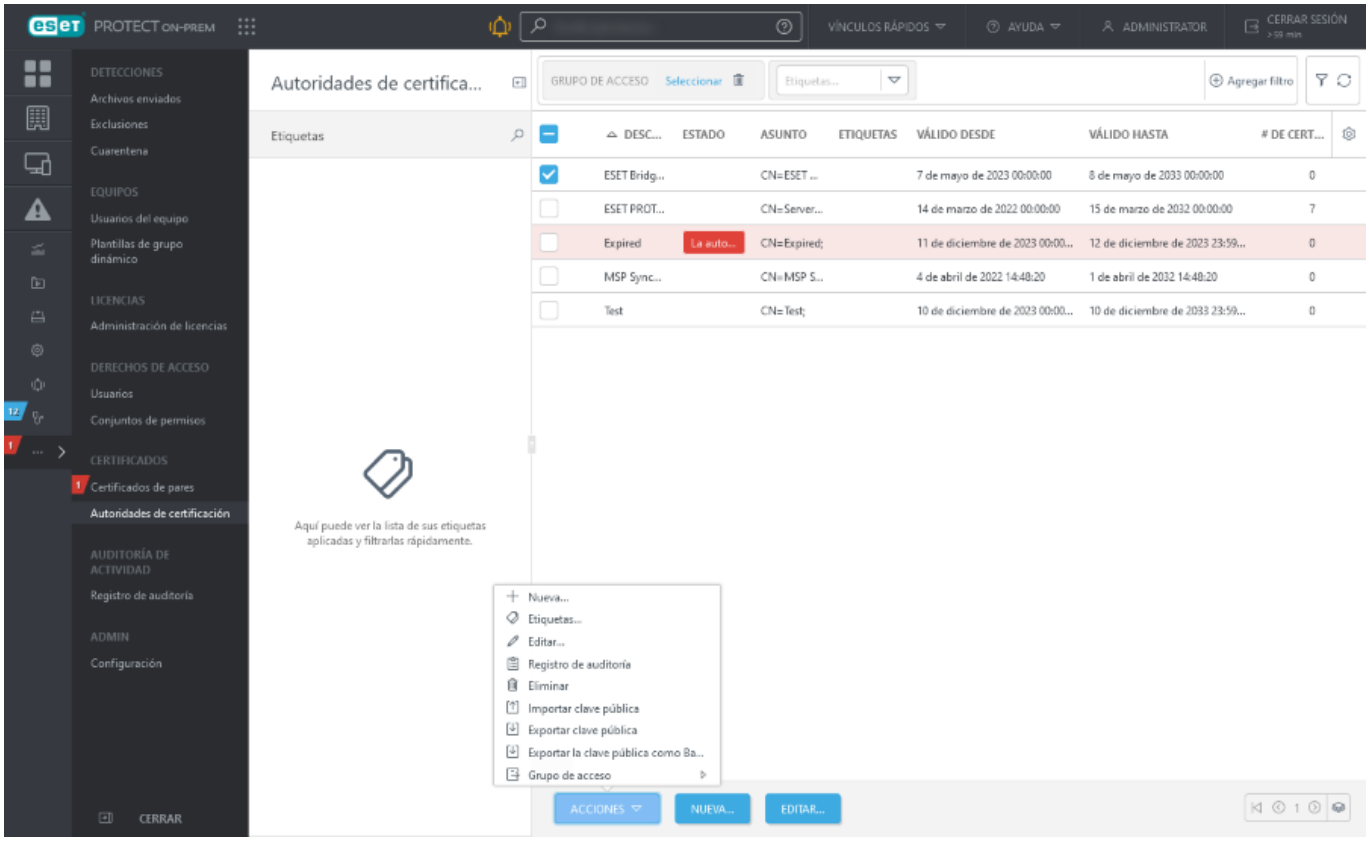
Para gestionar la Autoridad del certificado, seleccione la **casilla de verificación** junto a la Autoridad de certificación de la lista y use el menú contextual (haga clic izquierdo en la Autoridad del certificado) o el botón **Acción** ubicado en la parte inferior de la página. Las opciones disponibles son Importar clave pública y Exportar una clave pública o **Editar** la autoridad de certificación.

Exportar una clave pública

Para exportar una autoridad de certificación, haga clic en **Más** > **Autoridades de certificación**.

> Para exportar una clave pública, el usuario necesita tener derechos de Uso para los Certificados. Consulte la lista completa de derechos de acceso para obtener más información.

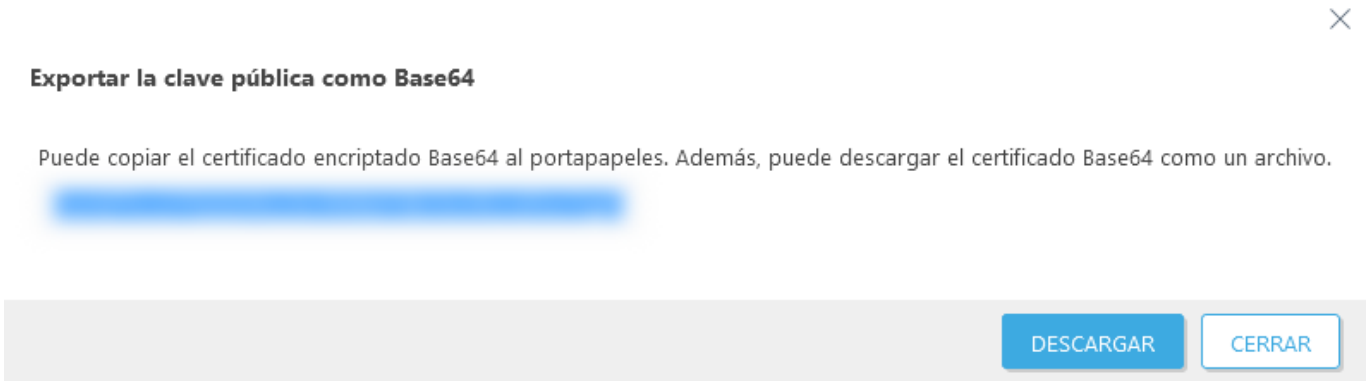
1. Seleccione la Autoridad de certificación que desee usar de la lista y seleccione la casilla de verificación junto a esa autoridad.



2. Seleccione una de las opciones de exportación:

a.Seleccione **Acciones** > **Exportar clave pública**. Seleccione esta opción si desea importar la clave pública a otra instalación de ESET PROTECT On-Prem (migración de un servidor a otro). Escriba un nombre para la clave pública y haga clic en **Guardar**. La clave pública se exportará como un archivo con extensión *.der*.

b.Seleccione **Acciones** > **Exportar clave pública como Base64**. Puede copiar la cadena del certificado codificado Base64 o hacer clic en **Descargar** para descargar el certificado codificado Base64 como archivo.



Si elimina la Autoridad de certificación ESET PROTECT predeterminada y crea una nueva, no va a funcionar. Antes de reemplazar la CA, debe crear y distribuir certificados de pares firmados por la nueva CA. También es necesario cambiar el certificado del servidor en la **Más** > Configuración y luego reiniciar el servicio del servidor ESET PROTECT.

Importar una clave pública

Para importar una autoridad de certificado de terceros, haga clic en **Más** > **Autoridades de certificación**.

1.Haga clic en el botón **Acciones** y, luego, seleccione **Importar clave pública**.

2.**Elegir archivo para cargar**: haga clic en **Examinar** para desplazarse al archivo que desea importar. Solo puede importar un archivo *.der*.

3.Ingrese una **Descripción** para el certificado y haga clic en **Importar**. La Autoridad de certificación se importa con éxito.

Registro de auditoría

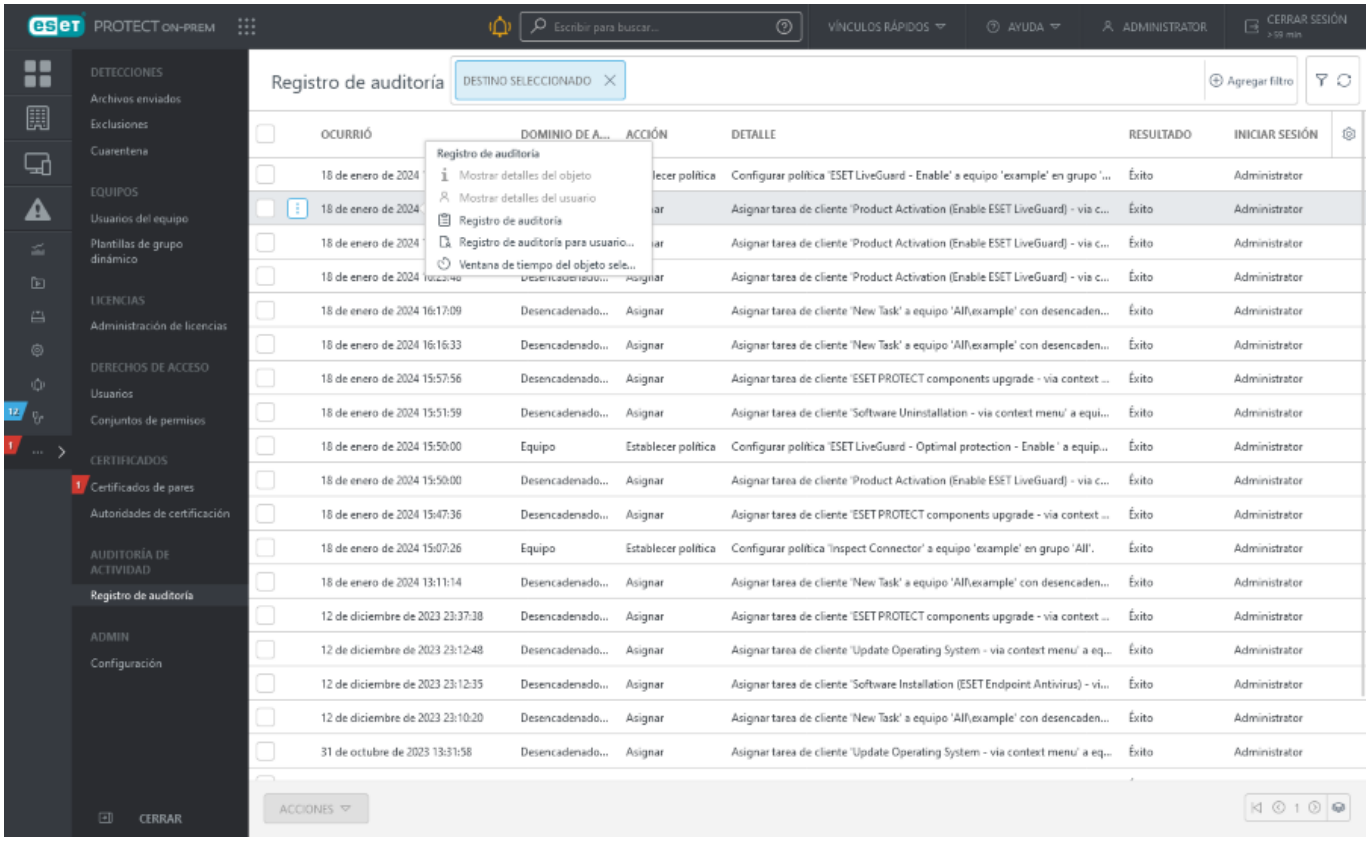
Cuando un usuario realiza una acción en la consola web de ESET PROTECT, la acción se registra. Se crean registros de auditoría si se crea o modifica un objeto de la consola web de ESET PROTECT (por ejemplo, equipo, política, detección, etc.).

El registro de auditoría es una nueva pantalla disponible en ESET PROTECT On-Prem. El registro de auditoría contiene la misma información que el Informe de registro de auditoría, pero permite un filtrado práctico de los datos mostrados. También puede ver directamente el registro de auditoría filtrado para los distintos objetos de la consola web haciendo clic en el objeto de la consola web y seleccionando **Registro de auditoría**.

El registro de auditoría permite que el administrador inspeccione las actividades que se llevan a cabo en la consola web de ESET PROTECT, en particular, si hay más usuarios de la consola web.

Para ver el registro de auditoría, el usuario de la consola web debe tener un conjunto de permisos con la funcionalidad **Registro de auditoría**.

El permiso Registro de auditoría le posibilita al usuario ver las acciones iniciadas por todos los demás usuarios y dominios, incluso las relacionadas con activos para los cuales el usuario no tiene derechos de visualización suficientes.



Haga clic en una línea en el registro de auditoría y podrá realizar las siguientes acciones:

Mostrar detalles del objeto	Muestra los detalles del objeto auditado.
Mostrar detalles del usuario	Muestra los detalles del usuario que realizó la acción respecto del objeto.
Registro de auditoría	Muestra el registro de auditoría para el objeto seleccionado.
Registro de auditoría para usuario seleccionado	Muestra el registro de auditoría para el usuario seleccionado.
Ventana de tiempo del objeto seleccionado	Muestra el registro de auditoría para el objeto seleccionado con un filtro activado de ocurrencia de tiempo.

Haga clic en **Agregar filtro** para filtrar la vista de tabla en función de diversos criterios:

- **<= Ocurrido**: define la fecha y hora antes de los cuales ocurrió la acción.
- **<= Ocurrido**: define la fecha y hora después de los cuales ocurrió la acción.
- **Acción**: selecciona la acción realizada.
- **Dominio de auditoría**: selecciona el objeto de consola web modificado.
- **Usuario de auditoría**: selecciona al usuario de la consola web que realizó la acción.
- **Resultado**: selecciona el resultado de la acción.

Configuración

En esta sección, puede configurar valores específicos para el servidor de ESET PROTECT en sí. Estas configuraciones son similares a las Políticas, pero se aplican directamente en el servidor ESET PROTECT.

Conexión

Puerto de servidor (requiere de un reinicio): es el puerto para la conexión entre ESET PROTECT Server y el agente. La modificación de esta opción requiere que se reinicie el servicio del servidor ESET PROTECT antes de que se efectúe el cambio. Para cambiar el puerto, es preciso implementar cambios en la configuración del firewall.

Puerto de la consola web (requiere que se reinicie): puerto para la conexión entre la consola web de ESET PROTECT y ESET PROTECT Server. Para cambiar el puerto, es preciso implementar cambios en la configuración del firewall.

Seguridad avanzada (requiere reinicio): esta configuración habilita la seguridad avanzada para la comunicación de red de componentes de ESET PROTECT. La seguridad avanzada está habilitada de forma predeterminada.

Certificado (requiere reinicio): aquí, puede administrar certificados de ESET PROTECT Server. Haga clic en Cambiar certificado y seleccione qué certificado de servidor ESET PROTECT debe ser utilizado por su servidor ESET PROTECT. Para obtener más información, consulte el capítulo Certificados de pares.

> Estos cambios requieren del reinicio del servicio de ESET PROTECT Server. Consulte nuestro artículo de la base de conocimiento para acceder a instrucciones.

Actualizaciones

Intervalo de actualización: intervalo en el que se recibirán las actualizaciones. Puede seleccionar un intervalo regular y configurar los valores, o puede usar una expresión CRON.

Servidor de actualización: servidor de actualización desde el cual el servidor de ESET PROTECT recibe las actualizaciones para los productos ESET y los componentes de ESET PROTECT. Para actualizar el ESET PROTECT On-Prem 11.0 desde una replicación (herramienta de replicación), defina la dirección completa de la carpeta de actualización `era6` (de acuerdo con la ubicación de origen del servidor HTTP). Por ejemplo:

```
http://your_server_address/mirror/eset_upd/era6
```

Tipo de actualización: seleccione el tipo de actualizaciones del módulo del servidor ESET PROTECT que desea recibir. Puede encontrar la versión actual de los módulos del servidor ESET PROTECT en **Ayuda** > **Acerca de**.

Actualización regular	Las actualizaciones del módulo del servidor ESET PROTECT se descargarán automáticamente desde el servidor de ESET con el menor tráfico de red. Configuración predeterminada.

Actualización previa al lanzamiento	Estas actualizaciones se han sometido a pruebas internas exhaustivas y pronto estarán disponibles para el público en general. Puede beneficiarse al habilitar actualizaciones previas a la publicación al tener acceso a las actualizaciones más recientes de módulos de servidor ESET PROTECT. Las actualizaciones previas al lanzamiento pueden resolver un problema con el servidor ESET PROTECT en algunos casos. Sin embargo, las actualizaciones previas a su lanzamiento pueden no ser lo suficientemente estables en todo momento y no se deben usar servidores de producción cuando se requieren disponibilidad y estabilidad máximas. Las actualizaciones previas a la publicación solo están disponibles con AUTOSELECT definido en el parámetro **Actualizar servidor**.

Configuración avanzada

Proxy HTTP: puede usar un servidor proxy para facilitar el tráfico de Internet a clientes en su red. Si instala ESET PROTECT On-Prem mediante el instalador todo en uno, se habilita el proxy HTTP de forma predeterminada. La configuración del proxy HTTP no se aplica a la comunicación con servidores de autenticación de dos factores.

Llamada de reactivación: ESET PROTECT Server puede ejecutar una replicación instantánea del agente ESET Management en un equipo cliente a través de EPNS. Esto resulta útil cuando no desea esperar el intervalo regular cuando el agente ESET Management se conecta al servidor ESET PROTECT. Por ejemplo, cuando desea que una Tarea se ejecute de inmediato en los clientes o si desea que se aplique una política rápidamente.

Reactivación en LAN: Configure **Direcciones multidifusión** si quiere enviar llamadas de reactivación en LAN a una o más direcciones IP.

Servidor SMTP: puede usar un servidor SMTP para permitir que ESET PROTECT Server envíe mensajes de correo electrónico (por ejemplo, enviar los informes o las notificaciones por correo electrónico). Especifique los detalles de su servidor SMTP.

Active Directory: puede preestablecer la configuración de AD. ESET PROTECT On-Prem utiliza sus credenciales en forma predeterminada en las tareas de sincronización con Active Directory (sincronización del usuario, sincronización del grupo estático). Cuando los campos relacionados se dejan en blanco en la configuración de la tarea, ESET PROTECT On-Prem utiliza las credenciales preestablecidas. Utilice un usuario de AD de solo lectura, ESET PROTECT On-Prem no realiza cambios en la estructura de AD.

Si ejecuta ESET PROTECT Server en Linux (o Aparato virtual), el archivo de configuración de *Kerberos* debe estar bien configurado. Puede configurar *Kerberos* para sincronizar con varios dominios.

Si ESET PROTECT Server se ejecuta en un equipo de Windows conectado a un dominio, solo se necesita el **host** en archivo. Es posible sincronizar entre más dominios si se ha establecido confianza.

- **Host** - Ingrese el nombre del servidor o la dirección IP de su controlador de dominio.
- **Nombre de usuario**: Ingrese el nombre de usuario para su controlador de dominio con el siguiente formato:
  - Servidor de `DOMAIN\username` (ESET PROTECT ejecutándose en Windows)
  - Servidor de `username@FULL.DOMAIN.NAME` o `username` (ESET PROTECT ejecutándose en Linux).

Asegúrese de escribir el dominio en letras mayúsculas, ya que es el formato requerido para autenticar consultas correctamente en un servidor de Active Directory.

- **Contraseña**: ingrese la contraseña usada para ingresar al controlador de dominio.

- **Contenedor de raíz**: introduzca el identificador completo de un contenedor de AD, por ejemplo: `CN=John,CN=Users,DC=Corp`. Sirve como **Nombre distinguido** preestablecido. Le recomendamos que copie y pegue este valor de una tarea del servidor para asegurarse de que se trata del valor correcto (copie el valor del campo **Nombre distinguido** una vez seleccionado).

El servidor de ESET PROTECT en Windows usa el protocolo de cifrado LDAPS (LDAP por sobre SSL) de manera predeterminada para todas las conexiones de Active Directory (AD). También puede configurar LDAPS en el aparato virtual de ESET PROTECT.
Para realizar correctamente una conexión de AD a través de LDAPS, configure lo siguiente:
1. El controlador de dominio debe tener instalado un certificado de la máquina. Para emitir un certificado para su controlador de dominio, siga los pasos indicados a continuación:
a)Abra el **Administrador de servidores** y haga clic en **Administrar** > **Agregar roles y características**, e instale **Servicios certificados de Active Directory** > **Autoridad de certificación**. Se creará una nueva autoridad de certificación en **Autoridades de certificación raíz de confianza**.
b)Diríjase a **Iniciar** >tipo `certmgr.msc` y presione **Aceptar** para ejecutar la extensión **Certificados** Consola de administración de Microsoft > **Certificados - Equipo local** > **Personal** > haga clic con el botón secundario en el panel vacío > **Todas las tareas** > **Solicitar un nuevo certificado** > rol **Inscribir controlador de dominio**.
c)Compruebe que el certificado emitido contenga la FQDN del controlador de dominio.
d)En su servidor ESET PROTECT, importe la CA que generó a la tienda de cert. (usando la herramienta `certmgr.msc`) a la carpeta CA de confianza.
2. Cuando proporcione la configuración de conexión al servidor de AD, escriba el FQDN del controlador de dominio (como se indica en el certificado del controlador de dominio) en el campo **Servidor** o **Host**. La dirección IP ya no es suficiente para LDAPS.
Para habilitar la reserva al protocolo LDAP, seleccione la casilla de verificación **Usar LDAP en lugar de Active Directory** en la tarea Sincronización de grupos estáticos o Sincronización de usuario.

Servidor Syslog: puede usar ESET PROTECT On-Prem para enviar notificaciones y mensajes de eventos a su Servidor Syslog. Además, exportar los registros de un producto de ESET del cliente y enviarlos al servidor Syslog.

Grupos estáticos: le permite el emparejamiento automático de equipos encontrados con equipos ya presentes en los grupos estáticos. El emparejamiento funciona según el nombre de host informado por el agente ESET Management y, si ya no se puede confiar en él, entonces debe deshabilitarse. Si el emparejamiento falla, el equipo se ubicará en el grupo de Perdidos y Encontrados.

Repositorio: ubicación del repositorio donde se almacenan todos los archivos de instalación.

- El repositorio ESET predeterminado es **AUTOSELECT** (direcciona a: *http://repository.eset.com/v1*). De manera automática, determina el servidor de repositorio con la mejor conexión en función de la ubicación geográfica (dirección IP) de ESET PROTECT Server (al utilizar CDN: Red de Entrega de Contenidos). Por lo tanto, no es necesario que cambie la configuración del repositorio.
- De manera opcional, puede definir un repositorio que utilice únicamente servidores ESET: *http://repositorynocdn.eset.com/v1*
- Jamás utilice una dirección IP para acceder al repositorio de ESET.
- Puede crear y utilizar un repositorio sin conexión.

Participar en el programa de mejora del producto: habilite o deshabilite el envío de 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).

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).

Los últimos archivos de registro del Servidor de ESET PROTECT están disponibles aquí:

- Windows: *C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs*
- Linux: */var/log/eset/RemoteAdministrator/Server/*

Puede configurar la exportación de registros a Syslog aquí.

Limpieza de la base de datos: para evitar una sobrecarga de la base de datos, puede usar esta opción para limpiar regularmente los registros. La limpieza de la base de datos elimina automáticamente estos tipos de registros: Registros de SysInspector, registros de diagnóstico, registros que ya no se recopilan (registros de dispositivos eliminados, registros de plantillas de informes eliminadas). El proceso de limpieza de la base de datos se ejecuta todas la noches a la medianoche de forma predeterminada. Los cambios en esta configuración se harán efectivos a partir de la siguiente limpieza. Puede configurar el intervalo de limpieza para cada uno de estos tipos de registro:

Tipo de registro	Ejemplo de tipo de registro
Registros de detecciones	• Antivirus • Archivos bloqueados • ESET Inspect Alertas • Firewall • HIPS • Protección web (sitios web filtrados)
Registros de administración	• Tareas • Desencadenadores • Configuración exportada • Inscripción
Registros de auditoría	• Registro de auditoría y el informe de registro de auditoría.
Registros de control	• Control del dispositivo • Control Web • Usuarios registrados

Los registros de diagnósticos se limpian a diario. El usuario no puede modificar el intervalo de limpieza.

Durante la limpieza de la base de datos, también se quitan los elementos en Detecciones que corresponden a registros de incidentes desinfectados (independientemente del estado de la detección). De forma predeterminada, el período de limpieza para los registros de incidentes (y Detecciones) se establece en 6 meses. Puede cambiar el intervalo en **Más** > Configuración.

Personalización

Personalizar la interfaz de usuario: puede agregar un logotipo personalizado a la consola webESET PROTECT, a los informes generados a través de una tarea del servidor y a las notificaciones de correo electrónico.

	Consola web	Informes	Notificaciones
Ninguno	Diseño básico, sin logotipo personalizado	El logotipo de ESET PROTECT On-Prem a la izquierda del pie de página.	El logotipo de ESET PROTECT On-Prem a la izquierda del encabezado.

	Consola web	Informes	Notificaciones
Marca compartida	Logotipo personalizado para la consola web	Un logotipo personalizado en el pie de página: el logotipo de ESET PROTECT On-Prem está a la izquierda, y el suyo a la derecha.	Un logotipo personalizado en el encabezado de notificación: el logotipo de ESET PROTECT On-Prem está a la izquierda y el suyo a la derecha.
Marca propia (necesita licencia MSP)	Logotipo personalizado para la consola web	Un logotipo personalizado en el pie de página del informe: no hay logotipo de ESET PROTECT On-Prem, solo su logotipo a la izquierda.	Un logotipo personalizado en el encabezado de notificación: en el lado izquierdo. Junto a él, se lee **Proporcionado por ESET PROTECT On-Prem**.

Logotipo de la empresa

- **Logo con fondo oscuro** (encabezado de la consola web): ese logotipo se mostrará en la esquina superior izquierda de la consola web.

- **Logotipo con fondo claro:** ese logotipo se mostrará en el encabezado (para propietarios de licencias MSP) o el pie de página (configuración de marca compartida) de los informes generados a través de una Tarea del servidor y en el encabezado de las notificaciones de correo electrónico.

Haga clic en  para seleccionar un logotipo. Haga clic en para descargar el logotipo actual. Haga clic en para eliminar el logotipo actual.

Informes y notificaciones

- **Personalizar informes**: habilite esta opción para usar el logotipo seleccionado en los informes o para agregar un texto de pie de página.

- **Texto de pie de página del informe**: escriba el texto que se agregará en el extremo inferior derecho de los informes que se generan en formato PDF.

No se puede usar un logotipo personalizado junto a un texto de pie de página personalizado. El logotipo tiene la posición que el texto de pie de página. Si el logotipo y el pie de página se utilizan de forma simultánea solo se verá el logotipo. Al utilizar la configuración de **marca propia**, el logotipo personalizado aparecerá en el extremo superior izquierdo del informe, se coloca un pequeño logotipo **proporcionado por ESET** en el extremo inferior derecho en lugar del texto de pie de página.

Seguridad avanzada

La seguridad avanzada incluye una comunicación de red segura entre los componentes de ESET PROTECT:

- Los certificados y las autoridades de certificación usarán SHA-256 (en lugar de SHA-1).

- El servidor de ESET PROTECT usa la máxima seguridad posible (TLS 1.3 o 1.2) para la comunicación con agentes, Syslog y comunicación SMTP.

- Usuarios de MDM: El servidor ESET PROTECT usa TLS 1.2 para la comunicación con el servidor MDM. La comunicación entre el servidor MDM y los dispositivos móviles no se ve afectada.

La seguridad avanzada funciona con todos los sistemas operativos compatibles:

- Windows

- Linux – Le recomendamos **usar la versión más reciente de OpenSSL1.1.1**. El agente ESET Management admite OpenSSL 3.x. 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`

- macOS

La seguridad avanzada está habilitada de forma predeterminada.

Servidor SMTP

ESET PROTECT On-Prem puede enviar automáticamente informes y notificaciones por correo electrónico. Habilite **Usar servidor SMTP**, haga clic en **Más** > **Configuración** > **Configuración avanzada** > **Servidor SMTP** y especifique lo siguiente:

- **Host**: nombre de host o dirección de IP de su servidor SMTP.

- **Port**: SMTP usa el puerto 25 como predeterminado, pero lo puede cambiar si su servidor SMTP usa un puerto diferente.

- **Nombre de usuario**: si su servidor SMTP requiere autenticación, especifique el nombre de la cuenta del usuario SMTP (no incluya el dominio ya que no funcionará).

- **Contraseña**: contraseña asociada con la cuenta de usuario SMTP.

- **Tipo de seguridad de conexión**: especifique el tipo de conexión, el predeterminado es **No asegurado**, pero si su servidor SMTP admite conexiones seguras, elija TLS o STARTTLS. Si desea hacer que su conexión sea más segura, use una extensión STARTTLS o SSL/TLS, ya que emplea un puerto independiente para la comunicación cifrada.

- **Tipo de autenticación**: el valor predeterminado está configurado en **Sin autenticación**. Sin embargo, puede seleccionar el tipo de autenticación adecuado de la lista desplegable (por ejemplo, inicio de sesión, CRAM-MD5, CRAM-SHA1, SCRAM-SHA1, NTLM o Automático)

- **Dirección del remitente**: este campo especifica la dirección del remitente que se mostrará en el encabezado de los correos electrónicos de notificación (De:)

- **Servidor de prueba SMTP**: se usa para asegurarse de que la configuración de SMTP sea la correcta. Haga clic en **Enviar correo electrónico de prueba** para abrir una ventana nueva. Ingrese la dirección de correo electrónico del destinatario y el mensaje de correo electrónico de prueba se enviará por el servidor SMTP a esta dirección. Compruebe el buzón de correo del destinatario para verificar que se entregó el correo electrónico de

prueba.

No puede usar una cuenta de correo electrónico de Google como un servidor de SMTP porque Google no permite que aplicaciones de terceros inicien sesión en la cuenta de Google usando solo el nombre de usuario y la contraseña.

Emparejar automáticamente los equipos encontrados

En caso de ocurrencia de instancias múltiples del mismo equipo en ESET PROTECT On-Prem (por ejemplo, si se reinstala el agente ESET Management en un equipo de un cliente ya administrado), la función **Emparejar automáticamente los equipos encontrados** se ocupa de esto y empareja estas instancias en una. Esto debería eliminar la necesidad de verificación manual y clasificación de equipos encontrados.

El emparejamiento se realiza sobre el nombre del host informado por el agente ESET Management y, si no se puede confiar, le recomendamos deshabilitar la función **Emparejar automáticamente los equipos encontrados**. Si el emparejamiento falla, el equipo se ubicará en el grupo de **Perdidos y Encontrados**. La idea es que cada vez que se reinstale el agente ESET Management en un equipo ya administrado, se empareje automáticamente y, por lo tanto, se coloque correctamente en ESET PROTECT On-Prem sin su intervención. Además, el nuevo agente ESET Management obtendrá sus políticas y tareas de inmediato.

- En el modo **deshabilitado**, los equipos que se deben colocar en el grupo **Perdidos y encontrados** se emparejarán con el primer equipo no administrado encontrado (marcador, icono del círculo) ubicado en cualquier lugar del árbol ESET PROTECT On-Prem. Si no hay un marcador con el mismo nombre, el equipo se coloca en el grupo Perdidos y Encontrados.

- En el modo **habilitado (predeterminado)**, los equipos que se deben colocar en el grupo **Perdidos y encontrados** se emparejarán con el primer equipo no administrado encontrado (marcador, icono del círculo) ubicado en cualquier lugar del árbol ESET PROTECT On-Prem. Si no hay un marcador con el mismo nombre, el equipo se emparejará con el primer equipo administrado encontrado (icono de alerta o verificación) ubicado en cualquier lugar del árbol ESET PROTECT On-Prem. Si el emparejamiento falla, el equipo se ubicará en el grupo de Perdidos y encontrados.

Si considera que no desea el emparejamiento automático, lo puede deshabilitar. Siempre podrá verificar y clasificar los equipos de manera manual.

Exportar registros a Syslog

ESET PROTECT On-Prem es capaz de exportar ciertos registros / eventos y enviarlos a su Servidor Syslog. Los eventos en la siguiente categoría de registro se exportan al Servidor Syslog: Detección, Firewall, HIPS, Auditoría e ESET Inspect. Eventos generados en cualquier equipo cliente administrado que ejecute un producto ESET (por ejemplo, ESET Endpoint Security). Estos eventos pueden ser procesados por cualquier solución Seguridad de la información y gestión de eventos (SIEM) capaz de importar eventos desde un Servidor Syslog. Los eventos se escriben en el servidor Syslog por ESET PROTECT On-Prem.

1. Para habilitar el servidor Syslog, haga clic en **Más** > **Configuración** > **Configuraciones avanzadas** > **Servidor Syslog** > **Usar el servidor Syslog**.

2. Para habilitar la exportación, haga clic en **Más** > **Configuración** > **Configuraciones avanzadas** > **Registros** > **Exportar registros a Syslog**.

Sin limitación, todos los registros exportados están disponibles para los usuarios de Syslog. Todos los mensajes del registro de auditoría se exportan a Syslog.

3. Seleccione uno de los siguientes formatos para mensajes de eventos:

- JSON (JavaScript Object Notation)
- LEEF (formato extendido de evento de registro): formato utilizado por la aplicación QRadar de IBM.
- CEF (formato de evento común)

Para filtrar los registros de eventos enviados a Syslog, cree una notificación de categoría de registro con un filtro definido.

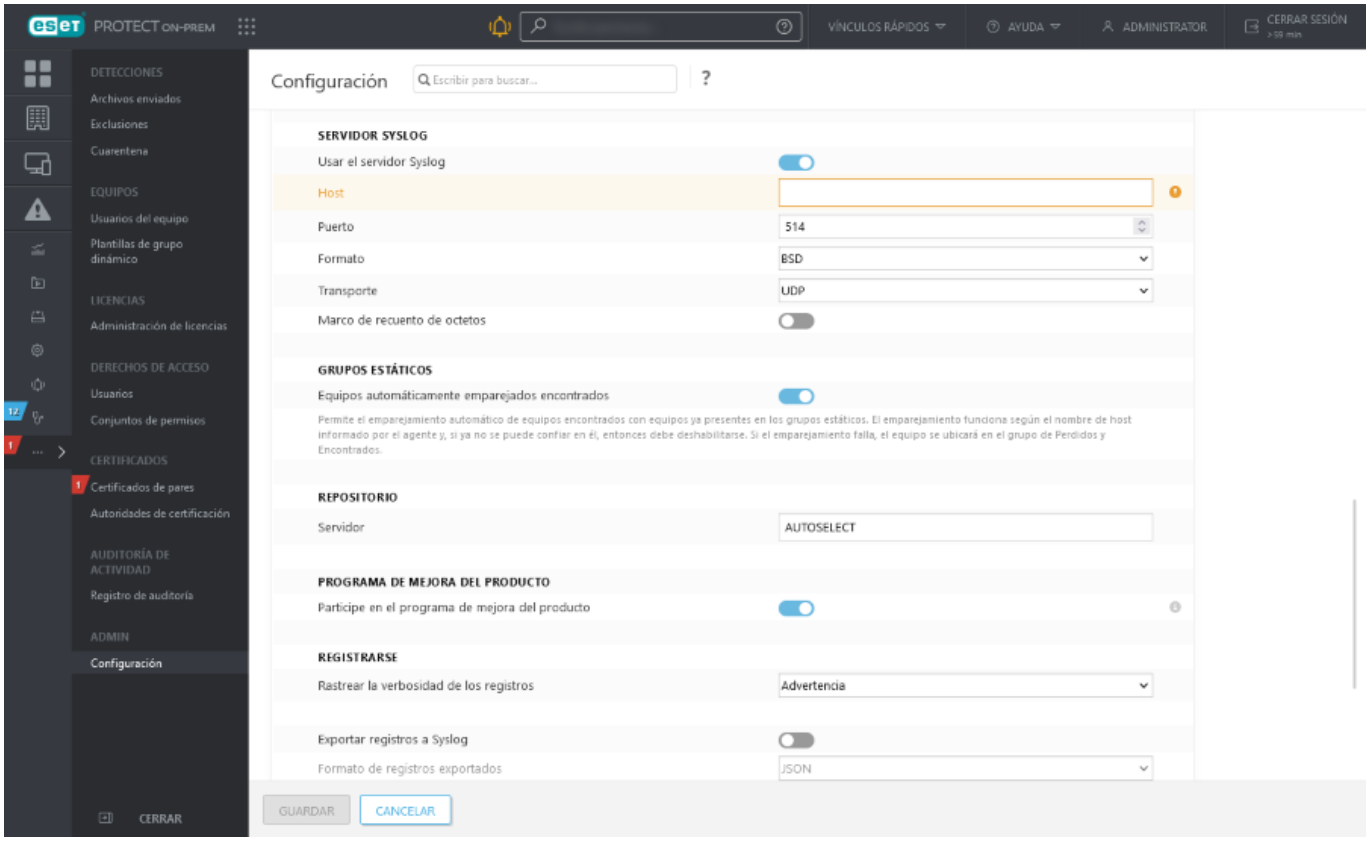
Servidor Syslog

Si tiene un servidor Syslog que se ejecuta en su red, puede Exportar registros a Syslog con el fin de recibir ciertos eventos (Evento de detección, Evento de firewall agregado, Evento de HIPS agregado, etc.) de los equipos de cliente que ejecutan, por ejemplo, ESET Endpoint Security. Puede configurar al servidor ESET PROTECT para enviar Notificaciones a su servidor Syslog.

Para habilitar el servidor Syslog:

1. Vaya a **Más** > **Configuración** > **Configuraciones avanzadas** > **Servidor Syslog** y haga clic en el conmutador junto a **Usar servidor Syslog**.
2. Especifique los siguientes ajustes obligatorios:
   a. **Host** (dirección IP o nombre de host del destino para mensajes Syslog)
   b. Número de **puerto** (el valor predeterminado es 514).
   c. **Formato** del registro: **BSD** (especificación), **Syslog** (especificación)
   d. Protocolo de **transporte** para enviar mensajes a Syslog (**UDP**, **TCP**, **TLS**)
3. Desplácese hacia abajo hasta **Registro** y habilite el conmutador **Exportar registros a Syslog**.

Luego de realizar cambios, haga clic en **Guardar**.



El archivo de registro regular de la aplicación constantemente está siendo escrito. Syslog sirve únicamente como un medio para exportar ciertos eventos asincrónicos como notificaciones o varios eventos del equipo cliente.

Eventos exportados a formato JSON

JSON es un formato liviano para el intercambio de datos. Se forma con una colección de parejas de nombres y valores, y una lista ordenada de valores.

Eventos exportados

Esta sección contiene información sobre el formato y el significado de los atributos de todos los eventos exportados. El mensaje de evento se encuentra en la forma de un objeto JSON con algunas claves obligatorias y otras opcionales. Cada evento exportado contendrá la siguiente clave:

event_type	string		Tipo de eventos exportados: • Threat_Event (**detecciones** antivirus) • FirewallAggregated_Event (**detecciones** de firewall) • HipsAggregated_Event (**detecciones** de HIPS) • Audit_Event (registro de auditoría) • FilteredWebsites_Event (sitios web filtrados: **protección web**) • EnterpriseInspectorAlert_Event (alertas de ESET Inspect) • BlockedFiles_Event (archivos bloqueados)
ipv4	string	opcional	Dirección IPv4 del equipo que genera el evento.
ipv6	string	opcional	Dirección IPv6 del equipo que genera el evento.
hostname	string		Hostname del equipo que genera el evento.

event_type	string		Tipo de eventos exportados: • Threat_Event (**detecciones** antivirus) • FirewallAggregated_Event (**detecciones** de firewall) • HipsAggregated_Event (**detecciones** de HIPS) • Audit_Event (registro de auditoría) • FilteredWebsites_Event (sitios web filtrados: **protección web**) • EnterpriseInspectorAlert_Event (alertas de ESET Inspect) • BlockedFiles_Event (archivos bloqueados)
source_uuid	string		UUID del equipo que genera el evento.
occurred	string		Hora UTC de la ocurrencia del evento. El formato es %d-%b-%Y %H:%M:%S
severity	string		Severidad del evento. Los posibles valores (de menos grave a más grave) son: `Información`, `Aviso`, `Advertencia`, `Error`, `Critical`, `Fatal`
group_name	string		La ruta completa al grupo estático del equipo que genera el evento. Si la ruta tiene más de 255 caracteres, group_name solo contiene el nombre del grupo estático.
group_description	string		Descripción del grupo estático.
os_name	string		Información sobre el sistema operativo del equipo.

Todos los tipos de eventos que se indican a continuación junto con todos los niveles de gravedad se informan al servidor Syslog. Para filtrar los registros de eventos enviados a Syslog, cree una notificación de categoría de registro con un filtro definido.
Los valores notificados dependen del producto de seguridad de ESET (y su versión) instalado en el equipo administrado y solo ESET PROTECT On-Prem informa los datos recibidos. Por lo tanto, ESET no puede proporcionar una lista exhaustiva de todos los valores. Le recomendamos que mida su red y filtre los registros en función de los valores recibidos.

Claves personalizadas en función del event_type:

Threat_Event

Todos los **eventos de detección** antivirus generados por puntos de conexión gestionados se reenviarán a Syslog. Clave específica del evento de detección:

threat_type	string	opcional	Tipo de detección
threat_name	string	opcional	Nombre de la detección
threat_flags	string	opcional	Indicadores relacionados de la detección
scanner_id	string	opcional	ID de exploración
scan_id	string	opcional	ID de exploración
engine_version	string	opcional	Versión del motor de exploración
object_type	string	opcional	Tipo de objeto relacionado con este evento
object_uri	string	opcional	URI del objeto
action_taken	string	opcional	Medidas adoptadas por el punto final
action_error	string	opcional	Mensaje de error si la "acción" no se ha realizado correctamente
threat_handled	bool	opcional	Indica si la detección pudo ser controlada o no
need_restart	bool	opcional	Define si es necesario reiniciar o no
username	string	opcional	Nombre de la cuenta de usuario asociada con el evento

threat_type	string	opcional	Tipo de detección
processname	string	opcional	Nombre del proceso asociado al evento
circumstances	string	opcional	Breve descripción de lo que causó el evento
hash	string	opcional	Hash SHA1 del flujo de datos (de la detección).
firstseen	string	opcional	Hora y fecha cuando la detección se detectó por primera vez en ese equipo. ESET PROTECT On-Prem utiliza diferentes formatos de fecha-hora para el atributo firstseen (y todos los demás atributos fecha-hora) dependiendo del formato de salida del registro (JSON o LEEF): • JSON formato:"%d-%b-%Y %H:%M:%S" • LEEF formato:"%b %d %Y %H:%M:%S"

Ejemplo de registro JSON de Threat_Event:


```
Jun 21 11: 46: 40 030 - MG ERAServer[5648]: {
    "event_type": "Threat_Event",
    "ipv4": "192.168.30.30",
    "hostname": "030-mg",
    "group_name": "All/Lost & found",
    "os_name": "Microsoft Windows 11 Pro",
    "group_description": "Lost & found static group",
    "source_uuid": "1361a9f6-1d45-4561-b33a-b5d6c62c71e0",
    "occured": "21-Jun-2021 09:46:15",
    "severity": "Warning",
    "threat_type": "Virus",
    "threat_name": "XF/Gydhex.A",
    "scanner_id": "Real-time file system protection",
    "scan_id": "virlog.dat",
    "engine_version": "23497 (20210621)",
    "object_type": "file",
    "object_uri": "file:///C:/Users/Administrator/Downloads/xls/YICT080714.xls",
    "action_taken": "Deleted",
    "threat_handled": true,
    "need_restart": false,
    "username": "030-MG\\Administrator",
    "processname": "C:\\Program Files\\WinRAR\\WinRAR.exe",
```

```
    "circumstances": "Event occurred on a newly created file.",
    "firstseen": "21-Jun-2021 09:46:14",
    "hash": "5B97884A45C6C05F93B22C4059F3D9189E88E8B7"
}
```


FirewallAggregated_Event

Los registros de eventos generados por ESET Firewall (**detecciones** de firewall) los agrega el agente de administración de ESET Management para evitar el desperdicio de ancho de banda durante la replicación del agente de ESET Management o del servidor de ESET PROTECT. Clave específica del evento de Firewall:

event	string	opcional	Nombre del evento
source_address	string	opcional	Dirección del origen del evento
source_address_type	string	opcional	Tipo de dirección del origen del evento
source_port	número	opcional	Puerto de la fuente del evento
target_address	string	opcional	Dirección de destino del evento
target_address_type	string	opcional	Tipo de dirección del destino del evento
target_port	número	opcional	Puerto del destino del evento
protocol	string	opcional	Protocolo
account	string	opcional	Nombre de la cuenta de usuario asociada con el evento
process_name	string	opcional	Nombre del proceso asociado al evento
rule_name	string	opcional	Nombre de regla
rule_id	string	opcional	ID de la regla
inbound	bool	opcional	Define si la conexión era de entrada o no
threat_name	string	opcional	Nombre de la detección
aggregate_count	número	opcional	Define cuántos mensajes iguales fueron generados por el punto final entre dos replicaciones consecutivas entre el servidor ESET PROTECT y la gestión del agente ESET Management
action	string	opcional	Medida tomada
handled	string	opcional	Indica si la detección pudo ser controlada o no

Ejemplo de registro JSON de FirewallAggregated_Event:


```
Jun 21 3: 54: 07 030 - MG ERAServer[5648]: {
 "event_type": "FirewallAggregated_Event",
 "ipv4": "192.168.30.30",
 "hostname": "w16test",
     "group_name": "All/Lost & found",
     "os_name": "Microsoft Windows 11 Pro",
```

```
        "group_description": "Lost & found static group",
    "source_uuid": "d9477661-8fa4-4144-b8d4-e37b983bcd69",
    "occured": "21-Jun-2021 13:10:04",
    "severity": ""Warning",
    "event": "Security vulnerability exploitation attempt",
    "source_address": "127.0.0.1",
    "source_address_type": "IPv4",
    "source_port": 54568,
    "target_address": "127.0.0.1",
    "target_address_type": "IPv4",
    "target_port": 80,
    "protocol": "TCP",
    "account": "NT AUTHORITY\\NETWORK SERVICE",
    "process_name": "C:\\Program Files\\Apache Software Foundation\\apache-
  tomcat-9.0.41\\bin\\tomcat9.exe",
    "inbound": true,
    "threat_name": "CVE-2017-5638.Struts2",
    "aggregate_count": 1
  }
```


HIPSAggregated_Event

Los eventos del Sistema de prevención de intrusiones basado en host ( **detecciones** de HIPS) se filtran según la **gravedad** antes de enviarse como mensajes de Syslog. Los atributos específicos de HIPS son los siguientes:

application	string	opcional	Nombre de la aplicación
operation	string	opcional	Operación
target	string	opcional	Destino
action	string	opcional	Medida tomada
action_taken	string	opcional	Medidas adoptadas por el punto final
rule_name	string	opcional	Nombre de regla
rule_id	string	opcional	ID de la regla
aggregate_count	número	opcional	Define cuántos mensajes iguales fueron generados por el punto final entre dos replicaciones consecutivas entre el servidor ESET PROTECT y la gestión del agente ESET Management
handled	string	opcional	Indica si la detección pudo ser controlada o no

Ejemplo de registro JSON de HipsAggregated_Event:


```
Jun 21 13: 54: 07 030 - MG ERAServer[5648]: {
    "event_type": "HipsAggregated_Event",
    "ipv4": "192.168.30.181",
    "hostname": "test-w10-uefi",
    "group_name": "All/Lost & found",
    "os_name": "Microsoft Windows 11 Pro",
    "group_description": "Lost & found static group",
    "source_uuid": "5dbe31ae-4ca7-4e8c-972f-15c197d12474",
    "occured": "21-Jun-2021 11:53:21",
    "severity": "Critical",
    "application": "C:\\Users\\Administrator\\Desktop\\es_pack_to_test\\test\\ja
va.exe",
    "operation": "Attempt to run a suspicious object",
    "target": "C:\\Users\\Administrator\\Desktop\\es_pack_to_test\\test\\trojan.
exe",
    "action": "blocked",
    "handled": true,
    "rule_id": "Suspicious attempt to launch an application",
    "aggregate_count": 2
}
```


Audit_Event

ESET PROTECT On-Prem envía los mensajes de registro de auditoría interna a Syslog. Los atributos específicos son los siguientes:

domain	string	opcional	Dominio de registro de auditoría
action	string	opcional	Acción que se lleva a cabo
target	string	opcional	Acción de destino que está en funcionamiento
detail	string	opcional	Descripción detallada de la acción
user	string	opcional	Usuario de seguridad involucrado
result	string	opcional	Resultado de la acción

Ejemplo de registro de Audit_Event:

```
Jun 21 11: 42: 00 030 - MG ERAServer[5648]: {
    "event_type": "Audit_Event",
    "ipv4": "192.168.30.30",
    "hostname": "030-MG",
    "group_name": "All/Lost & found",
    "os_name": "Microsoft Windows 11 Pro",
    "group_description": "Lost & found static group",
    "source_uuid": "72cdf05f-f9c8-49cc-863d-c6b3059a9e8e",
    "occured": "21-Jun-2021 09:42:00",
    "severity": "Information",
    "domain": "Native user",
    "action": "Login attempt",
    "target": "Administrator",
    "detail": "Authenticating native user 'Administrator'.",
    "user": "",
    "result": "Success"
}
```


FilteredWebsites_Event

ESET PROTECT On-Prem reenvía los sitios web filtrados (detecciones de **protección web**) a Syslog. Los atributos específicos son los siguientes:

processname	string	opcional	Nombre del proceso asociado al evento
username	string	opcional	Nombre de la cuenta de usuario asociada con el evento
hash	string	opcional	Hash SHA1 del objeto filtrado
event	string	opcional	Tipo de evento
rule_id	string	opcional	ID de la regla
action_taken	string	opcional	Medida tomada
scanner_id	string	opcional	ID de exploración
object_uri	string	opcional	URI del objeto
target_address	string	opcional	Dirección de destino del evento
target_address_type	string	opcional	Tipo de dirección del destino del evento (25769803777 = IPv4; 25769803778 = IPv6)
handled	string	opcional	Indica si la detección pudo ser controlada o no

Ejemplo de registro JSON de FilteredWebsites_Event:

```
Jun 21 3: 56: 03 020 - MG ERAServer[5648]: {
 "event_type": "FilteredWebsites_Event",
 "ipv4": "192.168.30.30",
 "hostname": "win-test",
     "group_name": "All/Lost & found",
     "os_name": "Microsoft Windows 11 Pro",
     "group_description": "Lost & found static group",
 "source_uuid": "d9477661-8fa4-4144-b8d4-e37b983bcd69",
 "occured": "21-Jun-2021 03:56:20",
 "severity": "Warning",
 "event": "An attempt to connect to URL",
 "target_address": "192.255.255.255",
 "target_address_type": "IPv4",
 "scanner_id": "HTTP filter",
 "action_taken": "blocked",        "object_uri": "https://test.com",
 "hash": "ABCDAA625E6961037B8904E113FD0C232A7D0EDC",
 "username": "WIN-TEST\\Administrator",
 "processname": "C:\\Program Files\\Web browser\\brwser.exe",
 "rule_id": "Blocked by PUA blacklist"
}
```

EnterpriseInspectorAlert_Event

ESET PROTECT On-Prem reenvía las alarmas de ESET Inspect a Syslog. Los atributos específicos son los siguientes:

processname	string	opcional	Nombre del proceso que causa esta alarma
username	string	opcional	Dueño del proceso
rulename	string	opcional	Nombre de la regla que desencadena esta alarma
count	número	opcional	Cantidad de alertas de este tipo que se han generado desde la última alarma
hash	string	opcional	Hash SHA1 de la alarma
eiconsolelink	string	opcional	Enlace a la alarma en la consola ESET Inspect On-Prem
eialarmid	string	opcional	Subparte del ID del enlace de la alarma ($1 en ^http.*/alarm/([0-9]+)$)
computer_severity_score	número	opcional	Nivel de gravedad del equipo
severity_score	número	opcional	Nivel de gravedad de la regla

Ejemplo de registro JSON de EnterpriseInspectorAlert_Event:


```
Jun 16 16:19:00 Win2016Std ERAServer[2772]: {
 "event_type": "EnterpriseInspectorAlert_Event",
 "ipv4": "192.168.30.30",
 "hostname": "shdsolec.vddjc",
     "group_name": "All/Lost & found",
     "os_name": "Microsoft Windows 11 Pro",
     "group_description": "Lost & found static group",
 "source_uuid": "csd77ad2-2453-42f4-80a4-d86dfa9d0543",
 "occured": "13-Jun-2021 07:45:00",
 "severity": "Warning",
 "processname": "ProcessName",
 "username": "UserName",
 "rulename": "RuleName2",
 "count": 158,
 "eiconsolelink": "http://eiserver.tmp/linkToConsole",
 "computer_severity_score": "1",
 "severity_score": "1"
}
```


BlockedFiles_Event

ESET PROTECT On-Prem reenvía las alarmas de los archivos bloqueados de ESET Inspect On-Prem a Syslog. Los atributos específicos son los siguientes:

processname	string	opcional	Nombre del proceso asociado al evento
username	string	opcional	Nombre de la cuenta de usuario asociada con el evento
hash	string	opcional	Hash SHA1 del archivo bloqueado
object_uri	string	opcional	URI del objeto
action	string	opcional	Medida tomada
firstseen	string	opcional	Hora y fecha cuando la detección se detectó por primera vez en ese equipo (formato de fecha y hora).
cause	string	opcional	
description	string	opcional	Descripción del archivo bloqueado
handled	string	opcional	Indica si la detección pudo ser controlada o no

Eventos exportados a formato LEEF

Para filtrar los registros de eventos enviados a Syslog, cree una notificación de categoría de registro con un filtro definido.

El formato LEEF es un evento de formato personalizado para IBM® Security QRadar®. Los eventos poseen atributos estándar y personalizados:

- ESET PROTECT On-Prem utiliza algunos atributos estándar descritos en la documentación oficial de IBM.
- Los atributos personalizados son los mismos que en el formato JSON. El atributo deviceGroupName contiene la ruta completa al grupo estático del equipo que genera el evento. Si la ruta tiene más de 255 caracteres, deviceGroupName solo contiene el nombre del grupo estático. El atributo deviceOSName contiene información sobre el sistema operativo del equipo y el atributo deviceGroupDescription contiene la descripción del grupo estático.

Categorías de eventos:

- Detecciones de antivirus
- Firewall
- Sitios web filtrados: protección web
- HIPS
- Auditoría
- ESET Inspect Alertas
- Archivos bloqueados

Puede encontrar más información sobre Log Event Extended Format (LEEF) en el sitio web oficial de IBM.

Eventos exportados a formato CEF

Para filtrar los registros de eventos enviados a Syslog, cree una notificación de categoría de registro con un filtro definido.

CEF es un formato de registro basado en texto desarrollado por ArcSight™. El formato CEF incluye un CEF encabezado y una extensión CEF. La extensión contiene una lista de pares clave-valor.

Encabezado CEF

Encabezado	Ejemplo	Descripción
Device Vendor	ESET	
Device Product	Protect	
Device Version	10.0.5.1	ESET PROTECT On-Prem versión

Encabezado	Ejemplo	Descripción
Device Event Class ID (Signature ID):	109	Identificador único de Categoría de evento del dispositivo: • 100:199 casos de amenaza • 200:299 eventos de firewall • 300–399 HIPS evento • 400–499 Evento de auditoría • 500–599 ESET Inspect evento • 600:699 eventos de archivos bloqueados • 700:799 eventos de sitios web filtrados
Event Name	Detected port scanning attack	Una breve descripción de lo que ocurrió en el evento
Severity	5	Severidad • 2 – Información • 3 – Aviso • 5 – Advertencia • 7 – Error • 8 – Crítico • 10 – Fatal

Extensiones CEF comunes para todas las categorías

Nombre de la extensión	Ejemplo	Descripción
cat	ESET Threat Event	Categoría de evento: • ESET Threat Event • ESET Firewall Event • ESET HIPS Event • ESET RA Audit Event • ESET Inspect Event • ESET Blocked File Event • ESET Filtered Website Event
dvc	10.0.12.59	Dirección IPv4 del equipo que genera el evento.
c6a1	2001:0db8:85a3:0000:0000:8a2e:0370:7334	Dirección IPv6 del equipo que genera el evento.
c6a1Label	Device IPv6 Address	
dvchost	COMPUTER02	Nombre de host del equipo con el evento
deviceExternalId	39e0feee-45e2-476a-b17f-169b592c3645	UUID del equipo que genera el evento.
rt	Jun 04 2017 14:10:0	Hora UTC de la ocurrencia del evento. El formato es %b %d %Y %H:%M:%S
ESETProtectDeviceGroupName	All/Lost & found	La ruta completa al grupo estático del equipo que genera el evento. Si la ruta tiene más de 255 caracteres, ESETProtectDeviceGroupName solo contiene el nombre del grupo estático.

Nombre de la extensión	Ejemplo	Descripción
ESETProtectDeviceOsName	Microsoft Windows 11 Pro	Información sobre el sistema operativo del equipo.
ESETProtectDeviceGroupDescription	Lost & found static group	Descripción de grupo estático.

Extensiones CEF por categoría de eventos

Casos de amenaza

Nombre de la extensión	Ejemplo	Descripción
cs1	W97M/Kojer.A	Nombre de la amenaza encontrada
cs1Label	Threat Name	
cs2	25898 (20220909)	Versión del motor de detección
cs2Label	Engine Version	
cs3	Virus	Tipo de detección
cs3Label	Threat Type	
cs4	Real-time file system protection	ID de exploración
cs4Label	Scanner ID	
cs5	virlog.dat	ID de exploración
cs5Label	Scan ID	
cs6	Failed to remove file	Mensaje de error si la "acción" no se ha realizado correctamente
cs6Label	Action Error	
cs7	Event occurred on a newly created file	Breve descripción de lo que causó el evento
cs7Label	Circumstances	
cs8	0000000000000000000000000000000000000000	Hash SHA1 del flujo de datos (de la detección).
cs8Label	Hash	
act	Cleaned by deleting file	El punto de conexión tomó la acción
filePath	file:///C:/Users/Administrator/Downloads/doc/000001_5dc5c46b.DOC	Objeto URI

Nombre de la extensión	Ejemplo	Descripción
fileType	File	Tipo de objeto relacionado con el evento
cn1	1	La detección se gestionó (1) o no se gestionó (0)
cn1Label	Handled	
cn2	0	Es necesario reiniciar (1) o no es necesario (0)
cn2Label	Restart Needed	
suser	172-MG\\Administrator	Nombre de la cuenta de usuario asociada con el evento
sprod	C:\\7-Zip\\7z.exe	El nombre del proceso de origen del evento
deviceCustomDate1	Jun 04 2019 14:10:00	
deviceCustomDate1Label	FirstSeen	La hora y la fecha en las que se encontró la detección por primera vez en la máquina. El formato es %b %d %Y %H:%M:%S

Ejemplo de registro de CEF de casos de amenazas:

```
CEF:O|ESET|Protect|10.0.0.0|183|File scanner cleaned a virus|5|deviceExternalId=e9d26759-fd21-47f1-9751-d2e7194c41a8 ESETProtectDeviceGroupName=All/Lost & found ESETProtectDeviceOsName=Microsoft Windows 11 Pro ESETProtectDeviceGroupDescription=Lost & found static group cat=ESET Threat Event rt=Jun 04 2017 14:10:00 cs1=W97M/Kojer.A cs1Label=Threat Name cs2=25898 (20220909) cs2Label=Engine Version cs3=Virus cs3Label=Threat Type cs4=Real-time file system protection cs4Label=Scanner ID cs5=virlog.dat cs5Label=Scan ID act=Cleaned by deleting fileType=File filePath=file:///C:/Users/Administrator/Downloads/doc/000001_5dc5c46b.DOC cn1=1 cn1Label=Handled suser=172-MG\\Administrator sprod=C:\\7-Zip\\7z.exe cs7=Event occurred on a newly created file. cs7Label=Circumstances eviceCustomDate1=Jun 04 2019 14:10:00 deviceCustomDate1Label=FirstSeen cs8=00000000000000000000000000000000000000000 cs8Label=Hash
```

Eventos de firewall

Nombre de la extensión	Ejemplo	Descripción
msg	TCP Port Scanning attack	Nombre del evento
src	127.0.0.1	Dirección IPv4 de origen del evento
c6a2	2001:0db8:85a3:0000:0000:8a2e:0370:7334	Dirección IPv6 de origen del evento
c6a2Label	Source IPv6 Address	
spt	36324	Puerto de la fuente del evento
dst	127.0.0.2	Dirección IPv4 de destino del evento
c6a3	2001:0db8:85a3:0000:0000:8a2e:0370:7335	Dirección IPv6 de destino del evento
c6a3Label	Destination IPv6 Address	
dpt	24	Puerto de destino del evento
proto	http	Protocolo
act	Blocked	Medida tomada
cn1	1	La detección se gestionó (1) o no se gestionó (0)
cn1Label	Handled	
suser	172-MG\\Administrator	Nombre de la cuenta de usuario asociada con el evento
deviceProcessName	someApp.exe	Nombre del proceso asociado al evento
deviceDirection	1	La conexión era entrante (0) o saliente (1)
cnt	3	El número de los mismos mensajes generados por el punto de conexión entre dos replicaciones consecutivas entre ESET PROTECT On-Prem y el agente de ESET Management
cs1		ID de la regla
cs1Label	Rule ID	
cs2	custom_rule_12	Nombre de regla
cs2Label	Rule Name	
cs3	Win32/Botnet.generic	Nombre de amenaza
cs3Label	Threat Name	

Ejemplo de registro CEF de casos de firewall:

```
CEF:O|ESET|Protect|10.0.0.0|109|Detected port scanning attack|5|deviceExternalId=39e0feee-45e2-476a-b07f-169b592c3645 ESETProtectDeviceGroupName=All/Lost & found ESETProtectDeviceOsName=Microsoft Windows 11 Pro ESETProtectDeviceGroupDescription=Lost & found static group cat=ESET Firewall Event rt=Jun 04 2017 14:10:00 msg=TCP Port Scanning attack src=127.0.0.1 spt=36324 dpt=21 dst=127.0.0.2 proto=http act=Blocked cnt=1 cn1=1 cn1Label=Handled suser=myAccount deviceProcessName=someApp.exe cs2=rule_118882389 cs2Label=Rule Name deviceDirection=0 cs3=Win32/Botnet.generic cs3Label=Threat Name
```

HIPS sucesos

Nombre de la extensión	Ejemplo	Descripción
cs1	Suspicious attempt to launch an application	ID de la regla
cs1Label	Rule ID	
cs2	custom_rule_12	Nombre de regla
cs2Label	Rule Name	
cs3	C:\\someapp.exe	Nombre de la aplicación
cs3Label	Application	
cs4	Attempt to run a suspicious object	Operación
cs4Label	Operation	
cs5	C:\\somevirus.exe	Destino
cs5Label	Target	
act	Blocked	Medida tomada
cs2	custom_rule_12	Nombre de regla
cn1	1	La detección se gestionó (1) o no se gestionó (0)
cn1Label	Handled	
cnt	3	El número de los mismos mensajes generados por el punto de conexión entre dos replicaciones consecutivas entre ESET PROTECT On-Prem y el agente de ESET Management

Ejemplo de registro CEF de casos HIPS:

```
CEF:O|ESET|Protect|10.0.0.0|303|Attempt to run a suspicious object Blocked|5|dvchost=test_bcmcjkbpgp deviceExternalId=82e114a8-9070-4868-8ee2-1e87b7b85ee3 ESETProtectDeviceGroupName=All/Lost & found ESETProtectDeviceOsName=Microsoft Windows 11 Pro ESETProtectDeviceGroupDescription=Lost & found static group cat=ESET HIPS Event rt=Jun 04 2019 14:10:00 cs3=C:\\someapp.exe cs3Label=Application cs4=Attempt to run a suspicious object cs4Label=Operation cs5=C:\\somevirus.exe cs5Label=Target act=Blocked cn1=1 cn1Label=Handled cs1=Suspicious attempt to launch an application cs1Label=Rule ID cnt=1
```

Eventos de auditoría

Nombre de la extensión	Ejemplo	Descripción
act	Login attempt	Acción que se lleva a cabo
suser	Administrator	Usuario de seguridad involucrado
duser	Administrator	Usuario de seguridad dirigido (por ejemplo, para intentos de inicio de sesión)
msg	Authenticating native user 'Administrator'	Una descripción detallada de la acción
cs1	Native user	Dominio de registro de auditoría
cs1Label	Audit Domain	
cs2	Success	Resultado de la acción
cs2Label	Result	

Ejemplo de registro CEF de casos de auditoría:

```
CEF:O|ESET|Protect|10.0.0.0|449|Native user login|2|dvc=10.15.172.133 dvchost=BRNH00006D deviceExternalId=db4a82c0-e1c6-49be-8bac-a436136ed1f4 cat=ESET RA Audit Event rt=Sep 21 2022 13:10:23 cs1=Native user cs1Label=Audit Domain act=Login attempt duser=Administrator msg=Authenticating native user 'Administrator'. cs2=Success cs2Label=Result
```

ESET Inspect sucesos

Nombre de la extensión	Ejemplo	Descripción
deviceProcessName	c:\\imagepath_bin.exe	Nombre del proceso que causa esta alarma
suser	HP\\home	Responsable del proceso
cs2	custom_rule_12	Nombre de la regla que desencadena esta alarma
cs2Label	Rule Name	
cs3	78C136C80FF3F46C2C98F5C6B3B5BB581F8903A9	Hash SHA1 de alarma
cs3Label	Hash	
cs4	https://inspect.eset.com:443/console/alarm/126	Enlace a la alarma en la consola web de ESET Inspect On-Prem
cs4Label	EI Console Link	
cs5	126	Subparte del ID del enlace de la alarma ($1 en ^http.*/alarm/([0-9]+)$)
cs5Label	EI Alarm ID	
cn1	275	Nivel de gravedad del equipo
cn1Label	ComputerSeverityScore	
cn2	60	Nivel de gravedad de la regla
cn2Label	SeverityScore	
cnt	3	El número de alertas del mismo tipo generadas desde la última alarma

Ejemplo del registro de CEF de casos ESET Inspect:

```
CEF:O|ESET|Protect|10.0.0.0|500|ESET Inspect Alert|5|dvchost=test_lrghlbjyoa deviceExternalId=432a30af-6ac7-4b61-ae5c-5141bfc5d878 ESETProtectDeviceGroupName=All/Lost & found ESETProtectDeviceOsName=Microsoft Windows 11 Pro ESETProtectDeviceGroupDescription=Lost & found static group cat=ESET Inspect Alert rt=Sep 21 2022 07:31:55 deviceProcessName=c:\\mother_process_info_imagepath_dir\\mother_process_info_imagepath_bin.exe suser=HP\\home cs2=9_1_0addd4e8baf8e87d4bc4ed77fadc cs2Label=Rule Name cs3=78C136C80FF3F46C2C98F5C6B3B5BB581F8903A9 cs3Label=Hash cs4=https://dev-inspect.eset.com:443/console/alarm/126 cs4Label=EI Console Link cs5=126 cs5Label=EI Alarm ID cn1=275 cn1Label=ComputerSeverityScore cn2=60 cn2Label=SeverityScore
```

Eventos de archivos bloqueados

Nombre de la extensión	Ejemplo	Descripción
act	Execution blocked	Medida tomada
cn1	1	La detección se gestionó (1) o no se gestionó (0)
cn1Label	Handled	
suser	HP\\home	Nombre de la cuenta de usuario asociada con el evento
deviceProcessName	C:\\Windows\\explorer.exe	Nombre del proceso asociado al evento
cs1	78C136C80FF3F46C2C98F5C6B3B5BB581F8903A9	Hash SHA1 del archivo bloqueado
cs1Label	Hash	
filePath	C:\\totalcmd\\TOTALCMD.EXE	Objeto URI
msg	ESET Inspect	Descripción del archivo bloqueado
deviceCustomDate1	Jun 04 2019 14:10:00	
deviceCustomDate1Label	FirstSeen	La hora y la fecha en las que se encontró la detección por primera vez en la máquina. El formato es %b %d %Y %H:%M:%S
cs2	Blocked by Administrator	Causa
cs2Label	Cause	

Ejemplo de registro CEF de casos de archivos bloqueados:

```
CEF:O|ESET|Protect|10.0.0.0|600|Blocked File Event|5|dvchost=test_lrghlbjyoa deviceExternalId=432a30af-6ac7-4b61-ae5c-5141bfc5d878 ESETProtectDeviceGroupName=All/Lost & found ESETProtectDeviceOsName=Microsoft Windows 11 Pro ESETProtectDeviceGroupDescription=Lost & found static group cat=ESET Blocked File Event rt=Sep 21 2022 07:31:55 act=Execution blocked cn1=1 cn1Label=Handled suser=HP\\home deviceProcessName=C:\\Windows\\explorer.exe cs1=78C136C80FF3F46C2C98F5C6B3B5BB581F8903A9 cs1Label=Hash filePath=C:\\totalcmd\\TOTALCMD.EXE deviceCustomDate1=Sep 21 2022 07:31:55 deviceCustomDate1Label=FirstSeen cs2=Blocked by Administrator cs2Label=Cause msg=ESET Inspect
```

Eventos de sitios web filtrados

Nombre de la extensión	Ejemplo	Descripción
msg	An attempt to connect to URL	Tipo de evento
act	Blocked	Medida tomada
cn1	1	La detección se gestionó (1) o no se gestionó (0)
cn1Label	Handled	
suser	Peter	Nombre de la cuenta de usuario asociada con el evento
deviceProcessName	Firefox	Nombre del proceso asociado al evento

Nombre de la extensión	Ejemplo	Descripción
cs1	Blocked by PUA blacklist	ID de la regla
cs1Label	Rule ID	
requestUrl	https://kenmmal.com/	URL de solicitud bloqueada
dst	172.17.9.224	Dirección IPv4 de destino del evento
c6a3	2001:0db8:85a3:0000:0000:8a2e:0370:7335	Dirección IPv6 de destino del evento
c6a3Label	Destination IPv6 Address	
cs2	HTTP filter	ID de exploración
cs2Label	Scanner ID	
cs3	8EECCDD290BE2E99183290FDBE4172EBE3DC7EC5	Hash SHA1 del objeto filtrado
cs3Label	Hash	

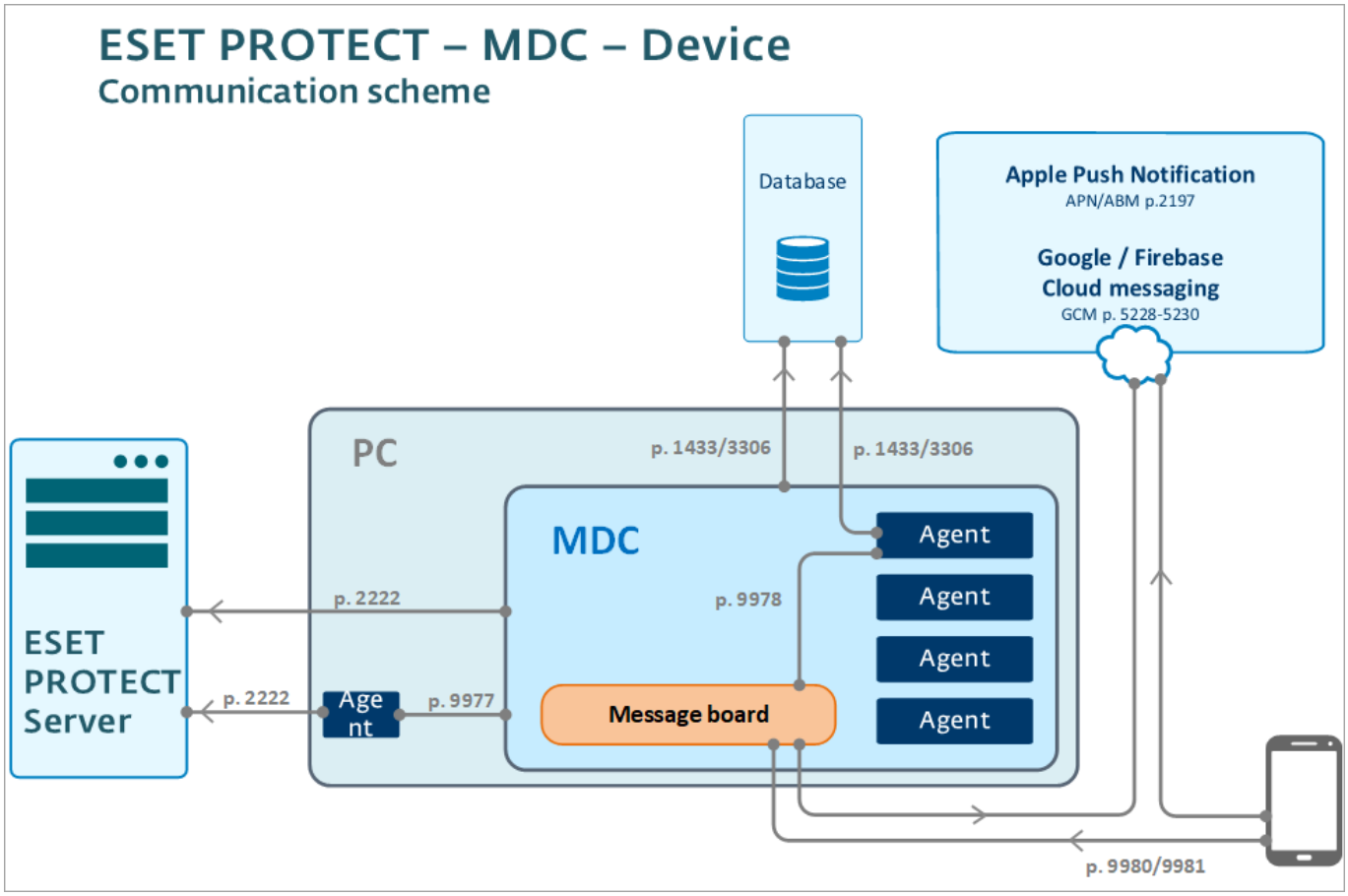
Ejemplo de registro CEF de casos de sitios web filtrados:

```
CEF:O|ESET|Protect|10.0.0.0|716|Filtered Website Event|5|dvchost=test_lrghlbjyoa deviceExternalId=432a30af-6ac7-4b61-ae5c-5141bfc5d878 ESETProtectDeviceGroupName=All/Lost & found ESETProtectDeviceOsName=Microsoft Windows 11 Pro ESETProtectDeviceGroupDescription=Lost & found static group cat=ESET Filtered Website Event rt=Sep 21 2022 07:31:55 msg=An attempt to connect to URL dst=172.17.9.224 cs2=HTTP filter cs2Label=Scanner ID act=Blocked cn1=1 cn1Label=Handled requestUrl=https://kenmmal.com cs3=8EECCDD290BE2E99183290FDBE4172EBE3DC7EC5 cs3Label=Hash suser=Peter deviceProcessName=Firefox cs1=Blocked by PUA blacklist cs1Label=Rule ID
```

Administración de dispositivos móviles

El componente de conector/administración de dispositivos móviles (MDM/MDC) de ESET PROTECT (solo on-prem) llega al fin de ciclo de vida en enero de 2024. Leer más. Le recomendamos migrar a Cloud MDM.

El siguiente diagrama demuestra la comunicación entre los componentes de ESET PROTECT y un dispositivo móvil:



Haga clic para agrandar la imagen.

> Recomendación de seguridad para MDM: El dispositivo host de MDM requiere acceso a Internet. Recomendamos que el dispositivo host de MDM esté detrás de un firewall y que sólo estén abiertos los puertos necesarios para el MDM. También puede implementar un IDS/IPS para supervisar la red en busca de anomalías.

El conector de dispositivo móvil (MDC) es un componente ESET PROTECT que permite el Administrador de dispositivos móviles con ESET PROTECT On-Prem, que le permite administrar dispositivos móviles Android e iOS y la administración de seguridad móvil.

MDC ofrece una solución sin agentes donde los agentes no se ejecutan directamente en dispositivos móviles (para ahorrar batería y rendimiento del dispositivo móvil). MDC actúa como host de estos agentes virtuales. MDC almacena datos para/desde dispositivos móviles en su base de datos SQL dedicada.

Se requiere un certificado HTTPS para autenticar la comunicación entre el dispositivo móvil y MDC. Para autenticar la comunicación entre el Servidor ESET PROTECT y MDC, se utiliza un certificado Proxy.

Para administrar dispositivos Apple, hay una serie de requisitos adicionales. El uso de MDC de ESET PROTECT para administra dispositivos iOS requiere el certificado de servicio de notificaciones Push de Apple. El servicio de APN habilita el ESET MDC para comunicarse de forma seguro con los dispositivos móviles de Apple. Este certificado debe estar firmado directamente por Apple (utilizando el Portal de Certificados Push de Apple) y debe entregarse a MDC a través de la política. Más adelante, es posible que los dispositivos iOS se inscriban al MDC ESET PROTECT.

En ciertos países, Apple Business Manager (ABM) está disponible. ABM es un nuevo método poderoso para la inscripción de dispositivos empresariales iOS. Con ABM puede inscribir los dispositivos a MDC automáticamente

sin contacto directo con el dispositivo y con mínima interacción por parte del usuario. ABM amplía las capacidades del MDM de iOS drásticamente y permite la personalización completa de la configuración del dispositivo.

Después de una instalación y configuración correcta del Conector de dispositivo móvil, los dispositivos móviles pueden inscribirse. Después de una inscripción correcta, el dispositivo móvil puede administrarse desde la Consola web ESET PROTECT.

Instalación y configuración de MDM

El componente de conector/administración de dispositivos móviles (MDM/MDC) de ESET PROTECT (solo on-prem) llega al fin de ciclo de vida en enero de 2024. Leer más. Le recomendamos migrar a Cloud MDM.

Con el fin de aprovechar el componente de Administración de dispositivos móviles en ESET PROTECT On-Prem, realice los siguientes pasos después de la instalación de MDM para poder inscribir y administrar dispositivos móviles.

1. Instale el **Conector de dispositivo móvil** (MDC) mediante el Instalador todo en uno o realice la instalación de componentes para Windows o Linux. También puede implementar MDM como un aparato virtual. Asegúrese de haber cumplido con los requisitos previos antes de la instalación.

Si está instalando MDC con el instalador todo en uno, el certificado HTTPS firmado por la autoridad de certificación de ESET PROTECT On-Prem se genera automáticamente durante el proceso de instalación. El certificado está protegido por contraseña (con una contraseña generada de forma aleatoria) y el certificado no está visible en **Más** > **Certificados de iguales**.
Si desea instalar ESET PROTECT On-Prem con el Instalador todo en uno y usar un certificado HTTPS de terceros, instale ESET PROTECT On-Prem primero, y luego modifique el certificado HTTPS usando directivas (en la sección **Política del conector de dispositivos móviles ESET General** > **Cambiar certificado** > **Certificado personalizado**).
Si está instalando el componente MDC por sí solo, puede usar:
a) un certificado firmado por la AC de ESET PROTECT On-Prem (**Básico** > **Producto**: Conector de dispositivo móvil, **Host**: Nombre de host/Dirección IP de MDC; **Firmar** > **Método de firma**: Autoridad de certificado; **Autoridad de certificado**: ESET PROTECT Autoridad de certificación
b) una cadena de certificado HTTPS de tercero firmado por una CA aprobada por Apple (lista de AC aprobadas por Apple).

2. Active MDC de ESET PROTECT usando una tarea de cliente de activación de producto. El procedimiento es el mismo que cuando activa cualquier producto de seguridad de ESET en un equipo cliente (no se usará una unidad de licencia).

3. Ejecute una Tarea de servidor de Sincronización de usuario (recomendado). Esto le permite sincronizar usuarios automáticamente con Active Directory o LDAP para propósitos de los Usuarios de equipo.

Si planea administrar dispositivos con **Android** solamente (no se administrarán dispositivos con iOS), puede omitir el paso 7.

4. Crear un certificado APN/ABM. Este certificado es usado por MDM ESET PROTECT para la inscripción de dispositivo iOS. Los certificados que se agregarán a su perfil de inscripción también se deben agregar a su perfil ABM.

5. Crear una nueva política para el Conector de dispositivo móvil ESET con el fin de activar APNS.

Siga estas instrucciones para realizar la inscripción de un dispositivo iOS con Apple Business Manager (ABM).

6. Inscriba dispositivos móviles mediante una tarea de Inscripción de dispositivos. Configure la tarea para inscribir dispositivos Android o iOS. También lo puede hacer desde la pestaña **Equipos** o **Grupo** al hacer clic en **Agregar nuevo** > **Dispositivos móviles** mientras tiene seleccionado un **Grupo estático** (no puede usar la función **Agregar** en grupos dinámicos).

7. Si no proporcionó una licencia durante la inscripción del dispositivo, active los dispositivos móviles mediante una Tarea de cliente de activación del producto; elija una licencia de ESET Endpoint Security. Se usará una unidad de licencia por cada dispositivo móvil.

La tarea de **Activación del producto** puede ejecutarse en dispositivos móviles ESET Endpoint para Android con una licencia sin conexión.
La tarea de activación no puede activar los productos de ESET de las versiones 4 y 5 con la licencia sin conexión. Debe activar el producto manualmente o usar una versión del producto compatible (se recomienda usar la versión más reciente).

8. Puede editar usuarios para configurar atributos personalizados y asignar dispositivos móviles si no asignó usuarios durante la inscripción de dispositivos.

9. Ahora podrá comenzar a aplicar políticas y a gestionar dispositivos móviles. Por ejemplo, Crear una política para iOS MDM - Cuenta Exchange ActiveSync que configurará automáticamente la cuenta de correo, los contactos y el calendario en los dispositivos iOS. También podrá aplicar restricciones en un dispositivo iOS o agregar una conexión wifi.

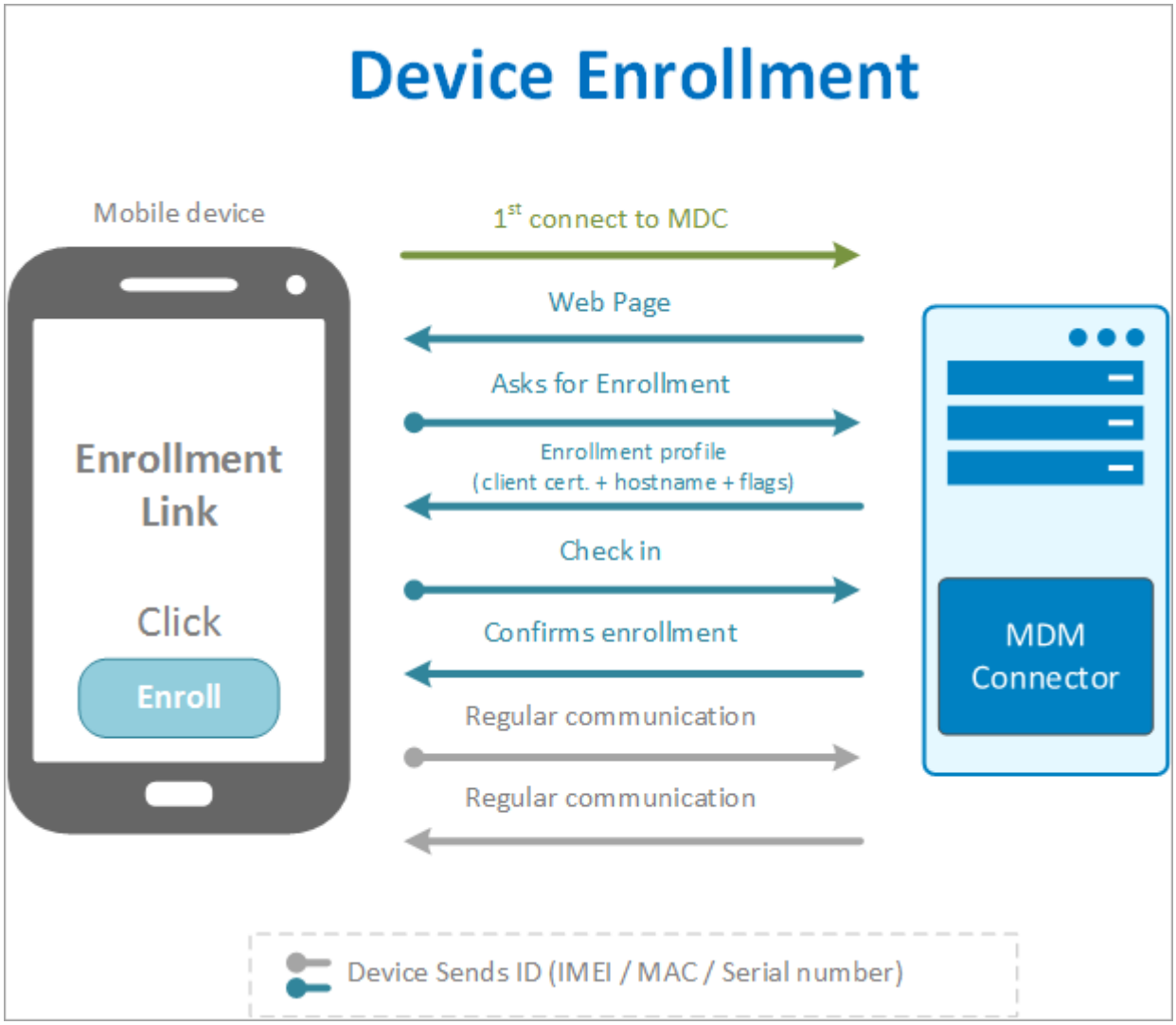
Solución de problemas

- Puede usar la función **Volver a inscribir** en un dispositivo móvil corrupto o limpio. El vínculo para volver a inscribir se enviará por correo electrónico.
- La tarea Detener administración (Desinstalar el agente ESET Management) cancelará la inscripción de MDM de un dispositivo móvil y lo quitará de ESET PROTECT On-Prem.
- Para actualizar MDC, use la tarea Actualización de componentes de ESET PROTECT.
- Consulte también Resolución de problemas de MDM

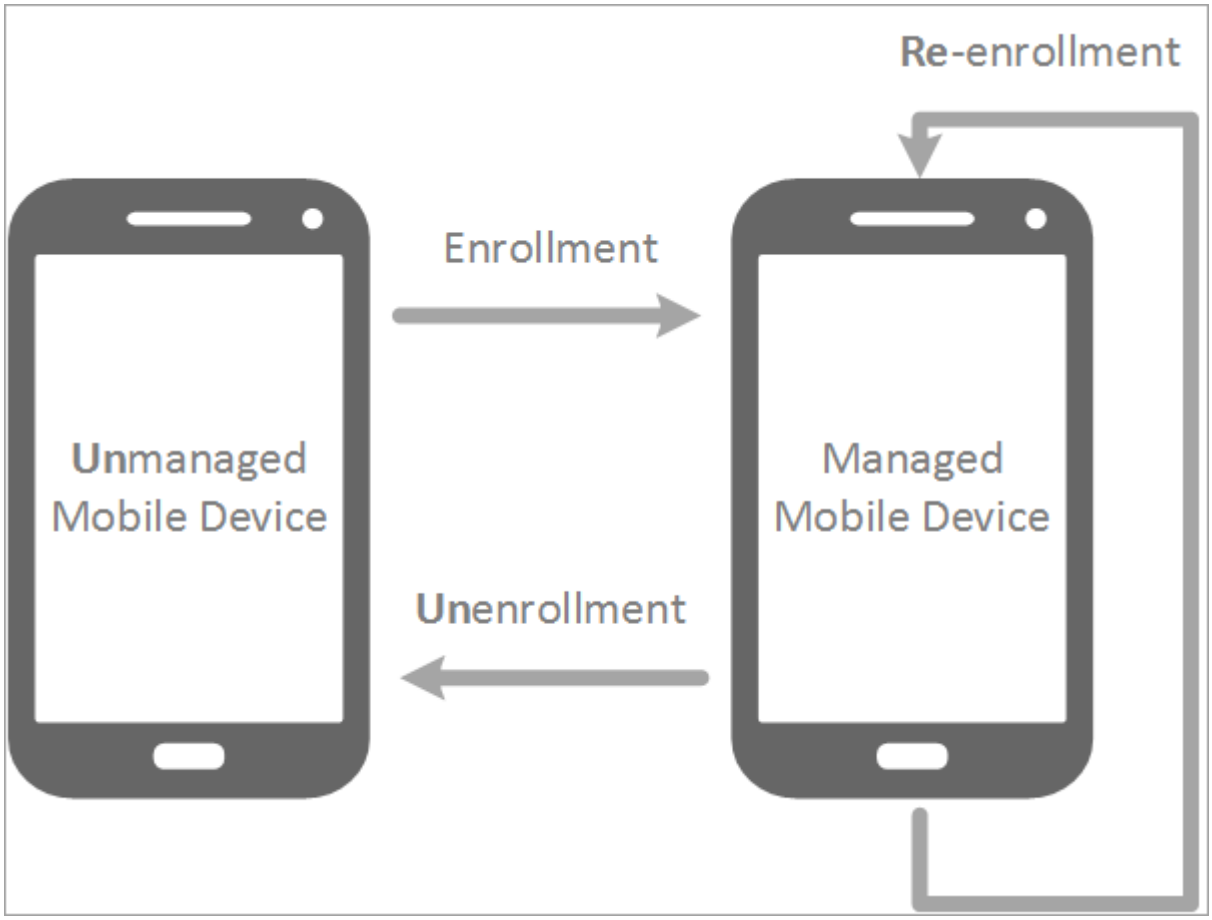
Inscripción de dispositivos

Los dispositivos móviles se pueden administrar mediante ESET PROTECT On-Prem y un producto de seguridad ESET que se ejecute en el dispositivo móvil. Para comenzar a administrar dispositivos móviles, los debe inscribir en ESET PROTECT On-Prem (ya no es necesario introducir el IMEI ni otros números de identificación en el dispositivo móvil).

El siguiente diagrama ilustra la manera en que el Dispositivo móvil se comunica con el Conector de dispositivo móvil durante el proceso de Inscripción:



Este diagrama explica cuándo se puede usar la inscripción, la reinscripción y la cancelación de la inscripción, y explica la diferencia entre dispositivos administrados y no administrados.



- **Inscripción**: la inscripción solo se puede utilizar cuando el dispositivo no es gestionado por MDM. En este caso, el dispositivo no existe en la sección **Equipos**. Eliminar un dispositivo de la consola web no significa que deje de ser administrado y el dispositivo aparecerá en la Consola web luego de una replicación exitosa. Solo el proceso de cancelación de inscripción puede quitar un dispositivo del estado administrado. Cada token de inscripción es único y de una única vez, por lo que se lo puede utilizar una sola vez. Una vez utilizado el token, no es posible volver a usarlo.

- **Reinscripción**: La reinscripción solo se puede usar si el dispositivo está administrado. El token de reinscripción es siempre diferente del token de inscripción, y también solo se lo puede usar una vez.
Para reinscribir un dispositivo, abra la sección **Equipos** y seleccione el dispositivo móvil que desea reinscribir. Abra el menú **Equipo** y seleccione **Móvil > Reinscribir**.

- **Cancelación de inscripción**: La cancelación de inscripción es la forma correcta de detener la administración de un dispositivo. La cancelación de inscripción se realiza mediante una Tarea de cliente de detener la administración. Si un dispositivo no responde, puede tomar hasta tres días que el dispositivo se elimine. Si desea quitar el dispositivo para volver a inscribirlo, utilice la reinscripción.

> Siga estas instrucciones para realizar la inscripción de un dispositivo iOS con Apple Business Manager (ABM).

Puede inscribir dispositivos móviles en la sección **Equipos** o en Más > Grupos. Seleccione el **Grupo estático** al que desea agregar dispositivos móviles, haga clic en **Agregar dispositivo** > **Dispositivos móviles** y, luego, seleccione uno de los siguientes métodos de inscripción:

- **Android o iOS/iPadOS** - Hay dos métodos de inscripción:

  - Enviar correo electrónico – Inscripción masiva de dispositivos móviles por correo electrónico. Esta opción

es más adecuada si necesita inscribir una gran cantidad de dispositivos móviles o si tiene dispositivos móviles existentes a los cuales no tiene acceso físico. Para usar esta opción, debe haber una participación activa del usuario/propietario del dispositivo móvil.

- Escanear código QR: inscripción de un solo dispositivo móvil. Podrá inscribir un dispositivo móvil a la vez y deberá repetir el mismo proceso para cada dispositivo. Le recomendamos usar esta opción solo si tiene una menor cantidad de dispositivos móviles para inscribir. Esta opción es adecuada si no desea que los propietarios de dispositivos móviles o usuarios no hagan nada y usted deba realizar todas las tareas de inscripción por sí mismo. Además, puede usar esta opción si tiene dispositivos móviles nuevos que se entregarán a los usuarios después de configurar todos los dispositivos.

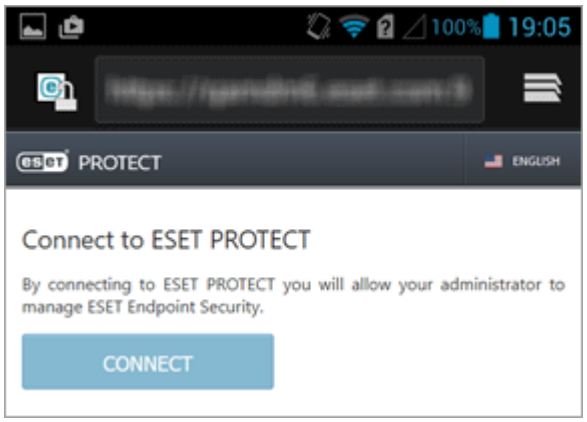
- **Inscripción individual como Propietario de dispositivos (únicamente en Android 7 y superior)**: dispositivo móvil único solamente para dispositivos Android. Podrá inscribir un dispositivo móvil a la vez y deberá repetir el mismo proceso para cada dispositivo. Este proceso de inscripción solo es posible en dispositivos nuevos (recién salidos de la caja) o después de un restablecimiento completo/de fábrica. Este proceso de inscripción proporcionará derechos de administración superiores al administrador sobre los derechos de administración del usuario del dispositivo móvil.

Inscripción de dispositivo Android

Existen dos escenarios para la inscripción cuando se activa ESET Endpoint Security para Android (EESA) en el dispositivo móvil. Podrá activar EESA en el dispositivo móvil a través de una tarea de cliente de activación del producto ERA (recomendada). El otro escenario es para dispositivos móviles con la aplicación ESET Endpoint Security para Android ya activada.

EESA ya activado: siga los siguientes pasos para inscribir su dispositivo:

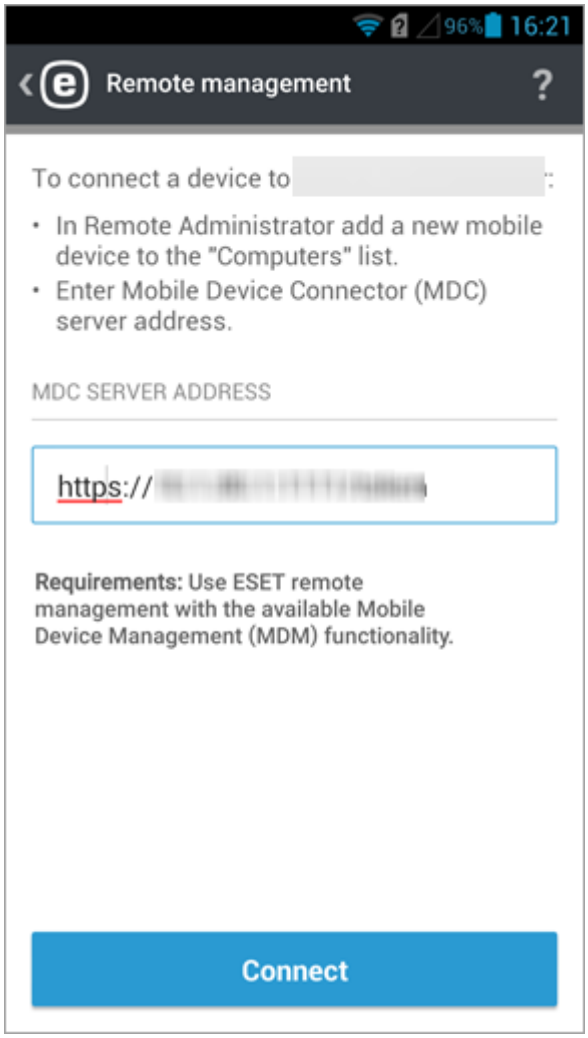
1. Toque el enlace de inscripción recibido por correo electrónico (incluyendo el número de puerto), o ingréselo de forma manual en el navegador (por ejemplo, *https://eramdm:9980/<token>*). Es posible que se le solicite que acepte un certificado SSL, haga clic en **Aceptar** si está de acuerdo y luego haga clic en **Conectar**.



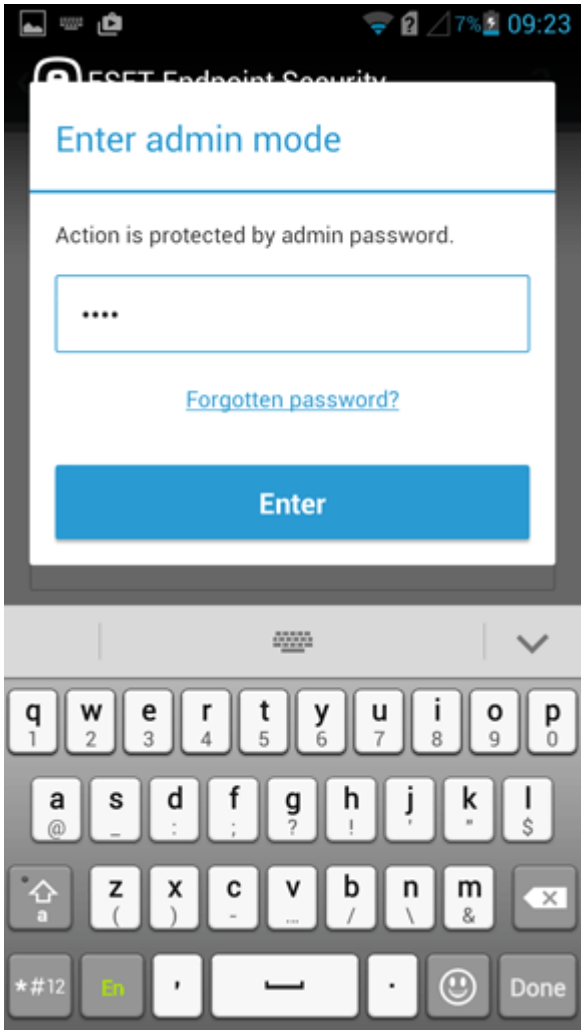
Si no cuenta con ESET Endpoint Security instalado en su dispositivo móvil, se lo redirigirá automáticamente a la Google Play Store, donde puede descargar la aplicación.

Si recibe la notificación **No se encontró aplicación que pueda abrir este enlace**, intente abrir el enlace de registro en el navegador web de Android predeterminado.

2. Consulte sus detalles de conexión (la dirección y el puerto del servidor del Conector de dispositivo móvil) y haga clic en **Conectar**.



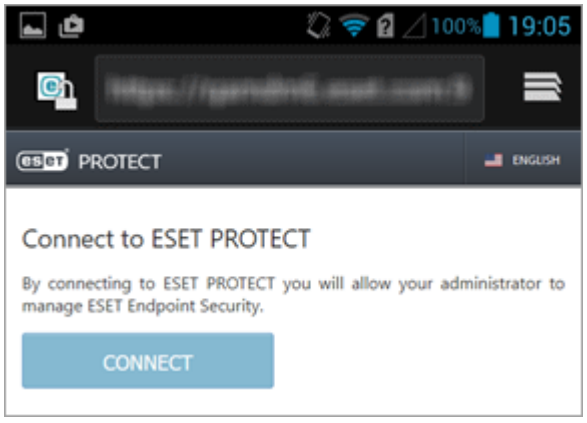
3. Ingrese la contraseña de modo admin de ESET Endpoint Security en el espacio en blanco y toque **Ingresar**.



4. Este dispositivo móvil es ahora administrado por ESET PROTECT On-Prem, toque **Finalizar**.

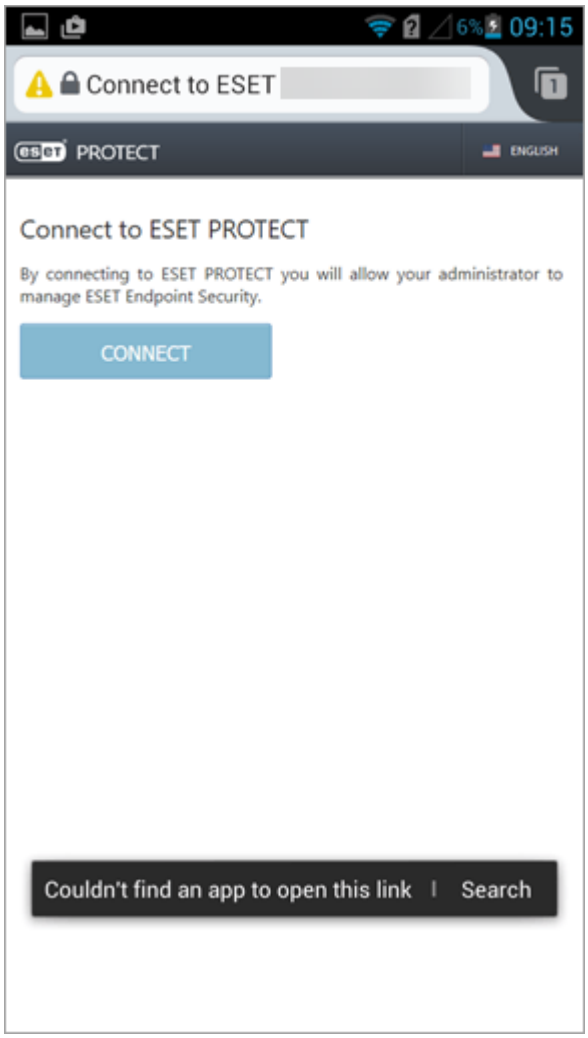
EESA no activado aún: siga los siguientes pasos para activar el producto e inscribir su dispositivo:

1. Toque el enlace de inscripción recibido por correo electrónico (incluido el número de puerto) e ingréselo de forma manual en el navegador (por ejemplo, *https://esmcmdm:9980/<token>*) o puede usar el **Código QR**. Es posible que se le solicite que acepte un certificado SSL, haga clic en **Aceptar** si está de acuerdo y luego haga clic en **Conectar**.

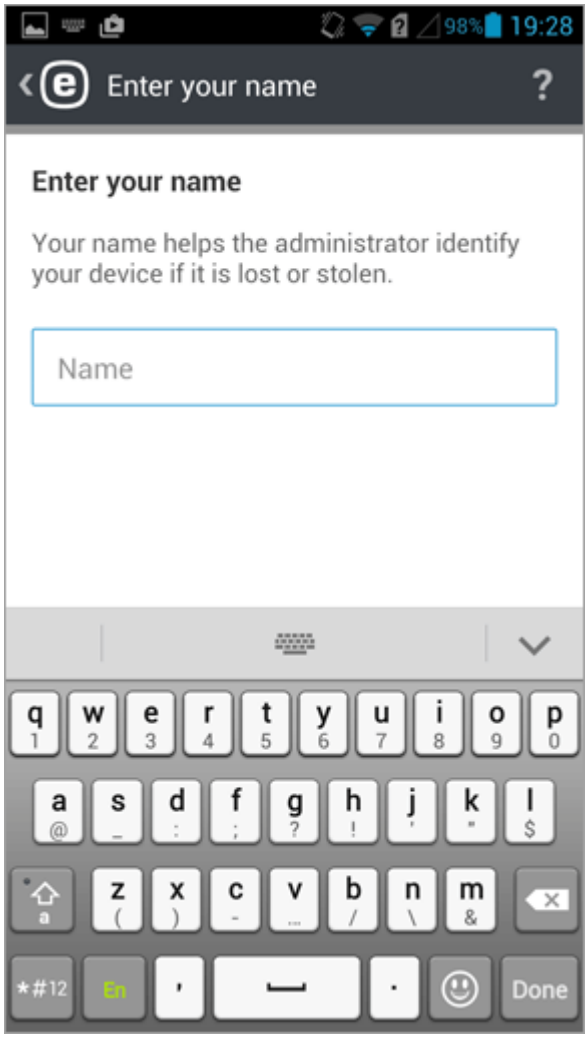


Si no cuenta con ESET Endpoint Security instalado en su dispositivo móvil, se lo redirigirá automáticamente a la Google Play Store, donde puede descargar la aplicación.

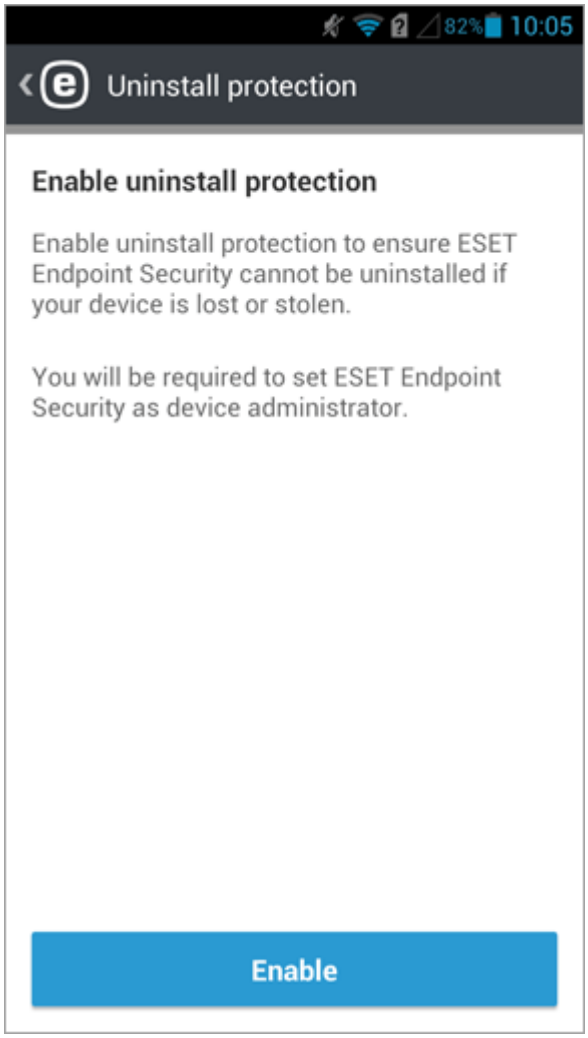
Si recibe la notificación **No se encontró aplicación que pueda abrir este enlace**, intente abrir el enlace de registro en el navegador web de Android predeterminado.



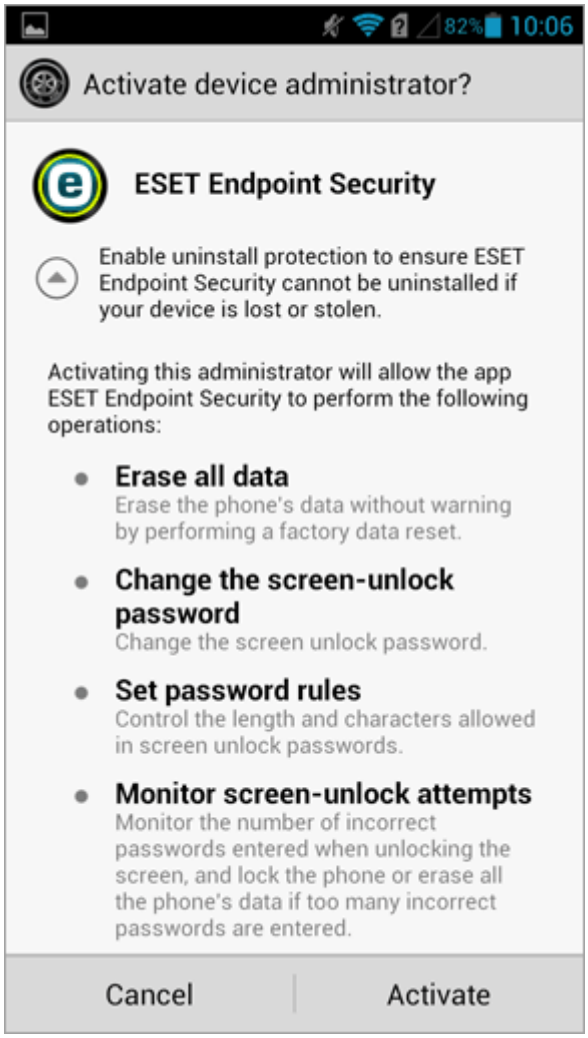
2. Ingrese el nombre del dispositivo móvil. (Este nombre no está visible en ESET PROTECT On-Prem. Solo es relevante para Anti-Theft y para registros de diagnóstico.)



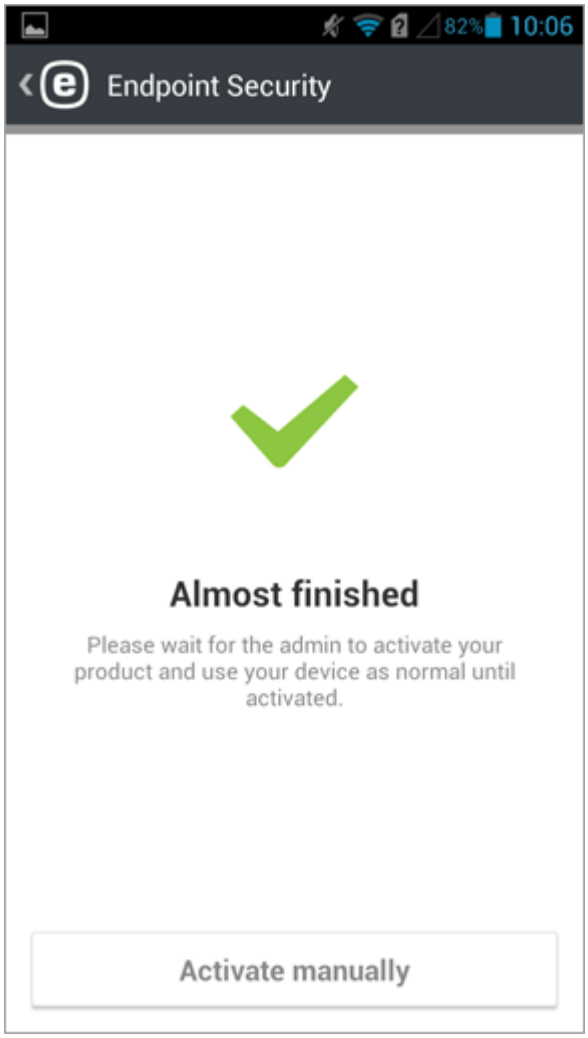
3. Toque **Habilitar** para habilitar la protección contra desinstalaciones.



4. Toque **Activar** para activar el administrador de dispositivos.



5. En este punto, puede salir de la aplicación ESET Endpoint Security para Android del dispositivo móvil y abrir la consola web ESET PROTECT.



6. Dentro de la Consola web ESET PROTECT, ingrese en **Tareas de cliente** > **Móvil** > Activación del producto y haga clic en **Nueva**.

Es posible que el cliente de Activación del producto tarde en ejecutarse en el dispositivo móvil. Una vez ejecutada la tarea con éxito, se activará la aplicación ESET Endpoint Security para Android y el dispositivo móvil podrá ser administrado por ESET PROTECT On-Prem. Ahora el usuario será capaz de usar la aplicación ESET Endpoint Security para Android. Al abrir la aplicación ESET Endpoint Security para Android, se mostrará el menú principal:

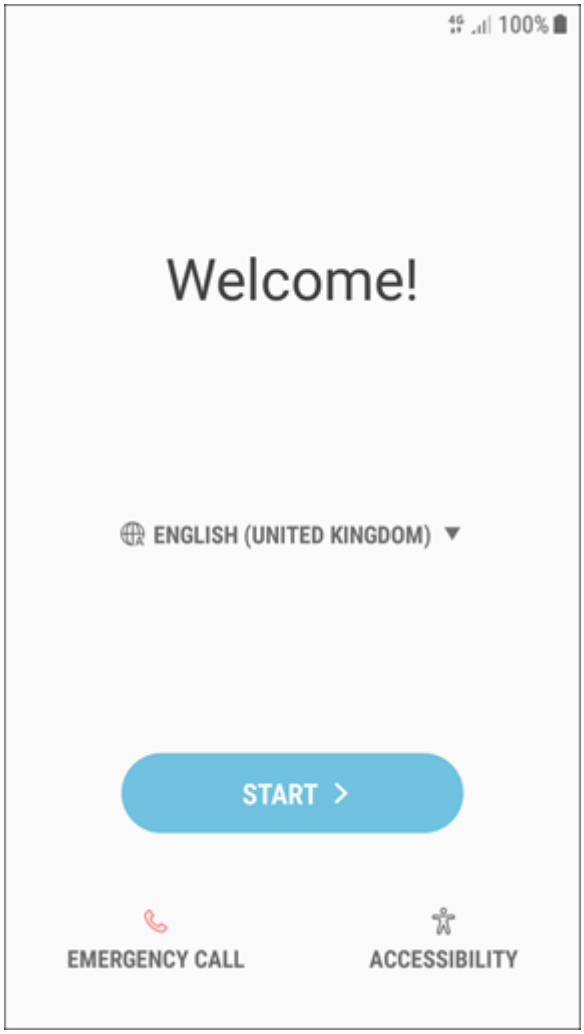
Inscripción de dispositivo Android como Propietario de dispositivos

Este tipo de inscripción está disponible únicamente para dispositivos Android v7 y superiores.
El dispositivo Android debe haber sido restablecido de fábrica o estar recién salido de la caja para poder realizar los siguientes pasos de inscripción.

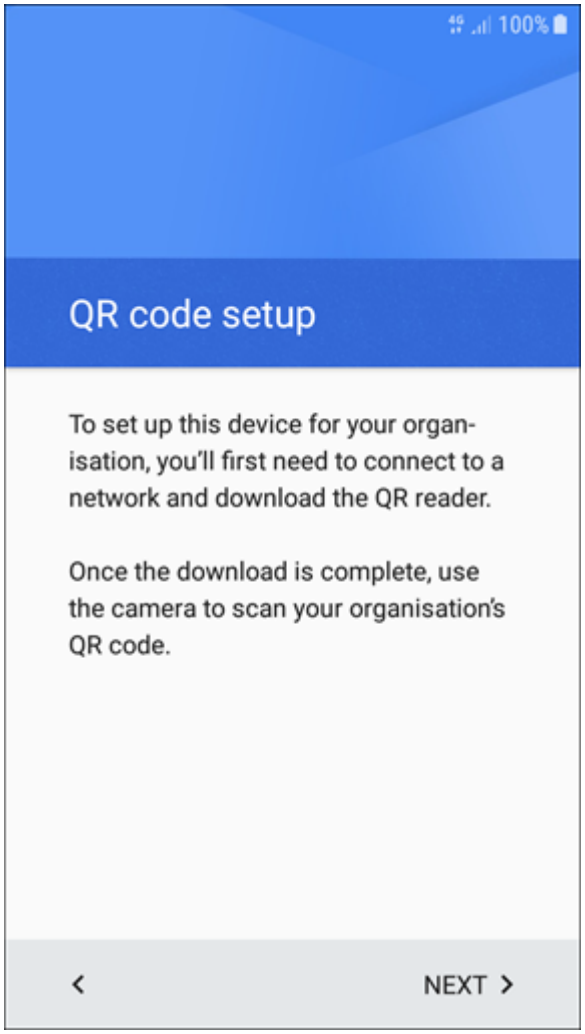
1. Encienda el dispositivo móvil.

2. Ingrese en pin de la tarjeta SIM.

3. En la pantalla de bienvenida, seleccione el idioma preferido y toque la pantalla seis (6) veces cerca del texto «Bienvenido» para iniciar la configuración del código QR.

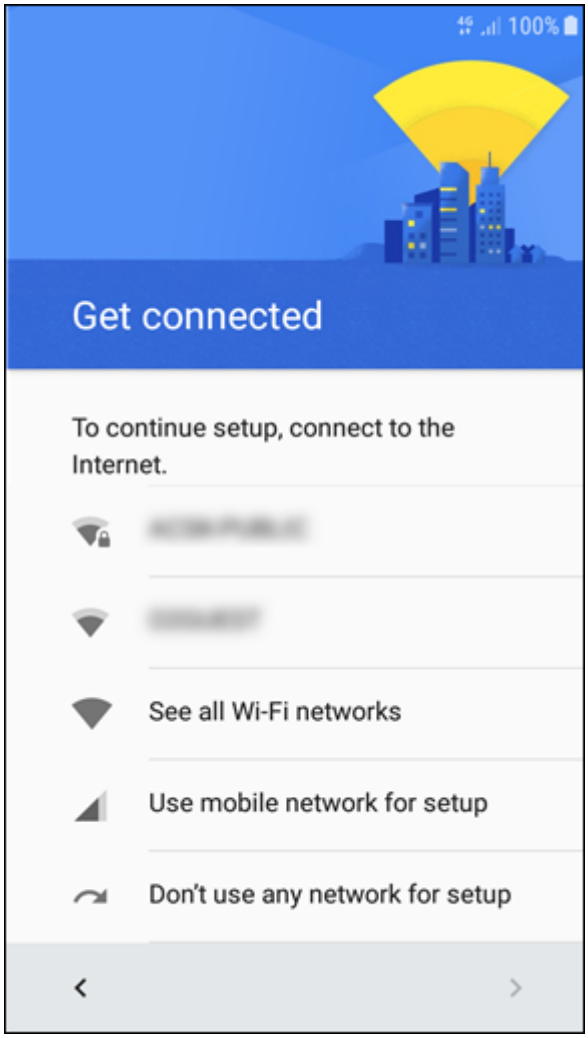


4. Si realizó correctamente el paso anterior, aparecerá en la pantalla una **Configuración de código QR**. Toque **Siguiente** para continuar.



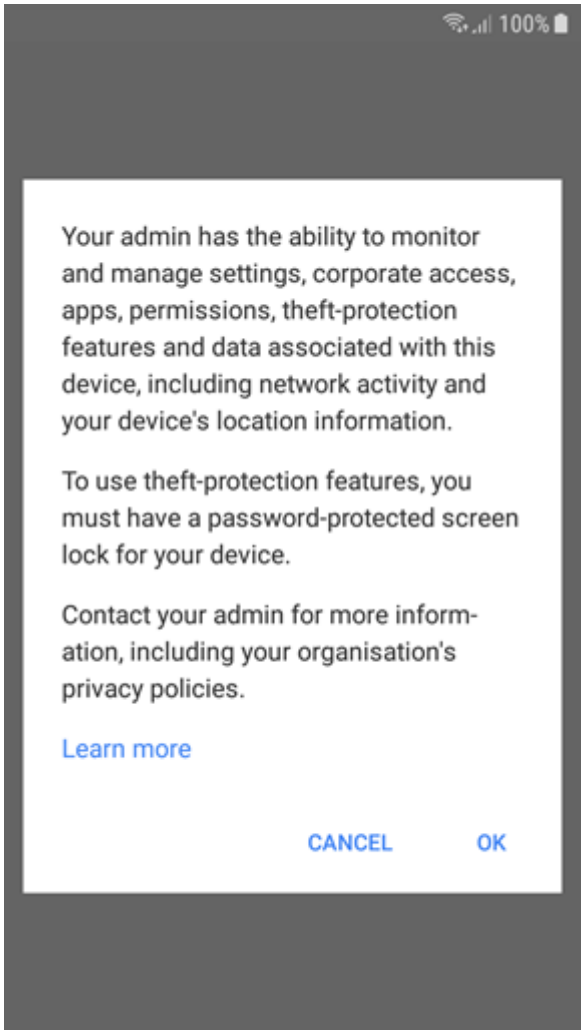
Algunos dispositivos pueden requerir que cifre el almacenamiento del dispositivo (a veces también es necesario conectar el cargador). Seleccione el tipo de cifrado que desea y proceda según las instrucciones en la pantalla.

5. Seleccione una conexión a Internet. Esto se usará para descargar el lector de códigos QR necesario para el siguiente paso.

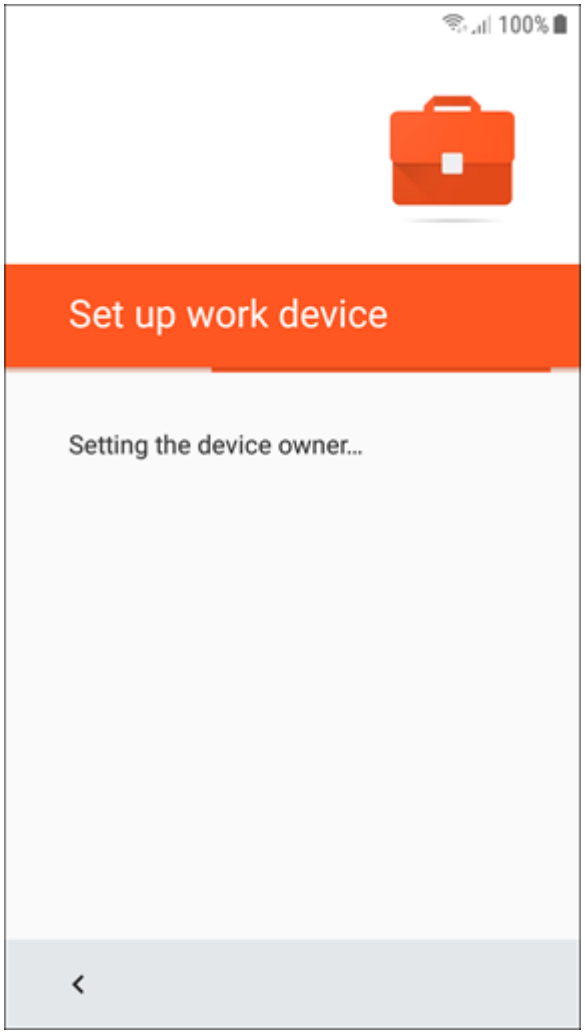


6. Ahora se instalará el lector de códigos QR. Después de terminar la instalación, lea el código QR que se generó en la Consola Web de ESET PROTECT.

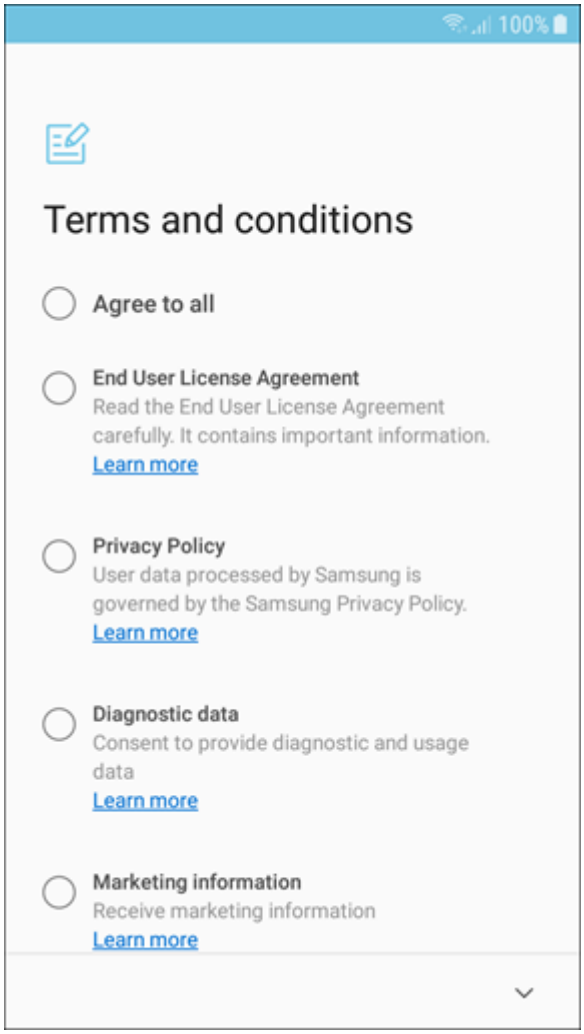
7. Se le pedirá que confirme que entiende que está otorgando derechos superiores de Propietario del dispositivo al Administrador. Toque **OK** para continuar.



8. La aplicación de ESET Endpoint Security para Android se habrá instalado y se aplicará los permisos necesarios.



9. Toque en **Aceptar todo** para aceptar el EULA, la Política de privacidad y la transferencia de datos de diagnóstico y mercadeo.



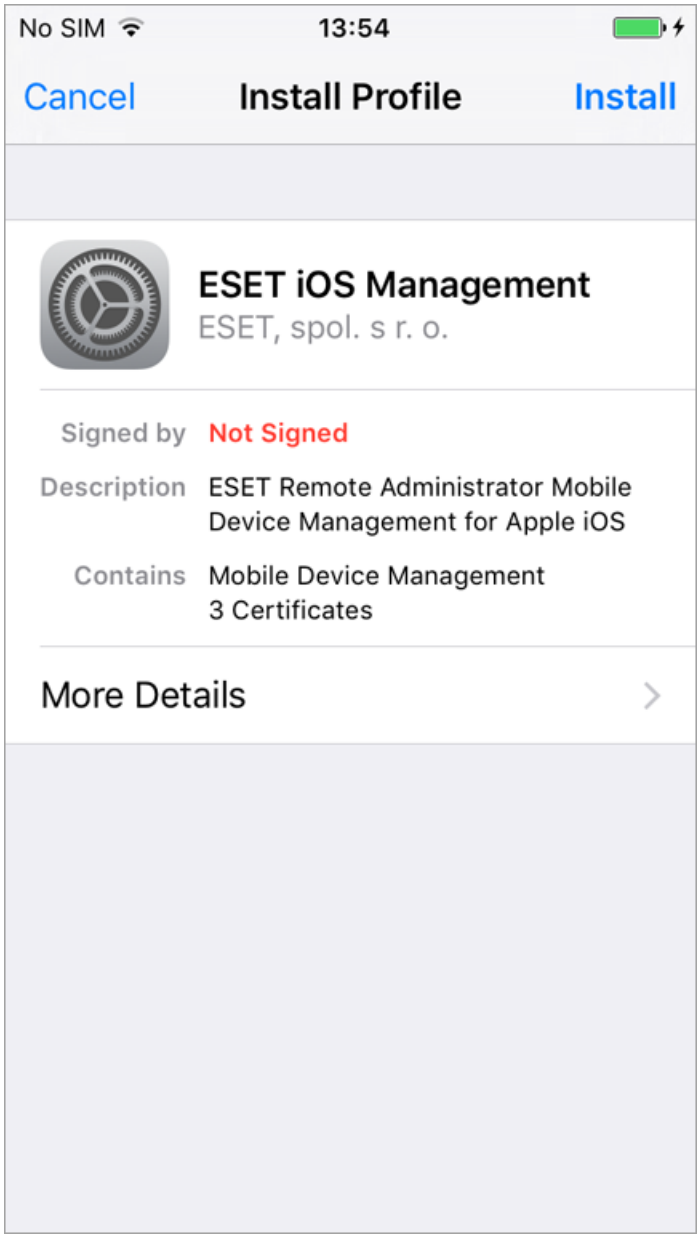
10. Ahora el dispositivo está inscrito en el modo Propietario del Dispositivo.

Inscripción de dispositivo iOS

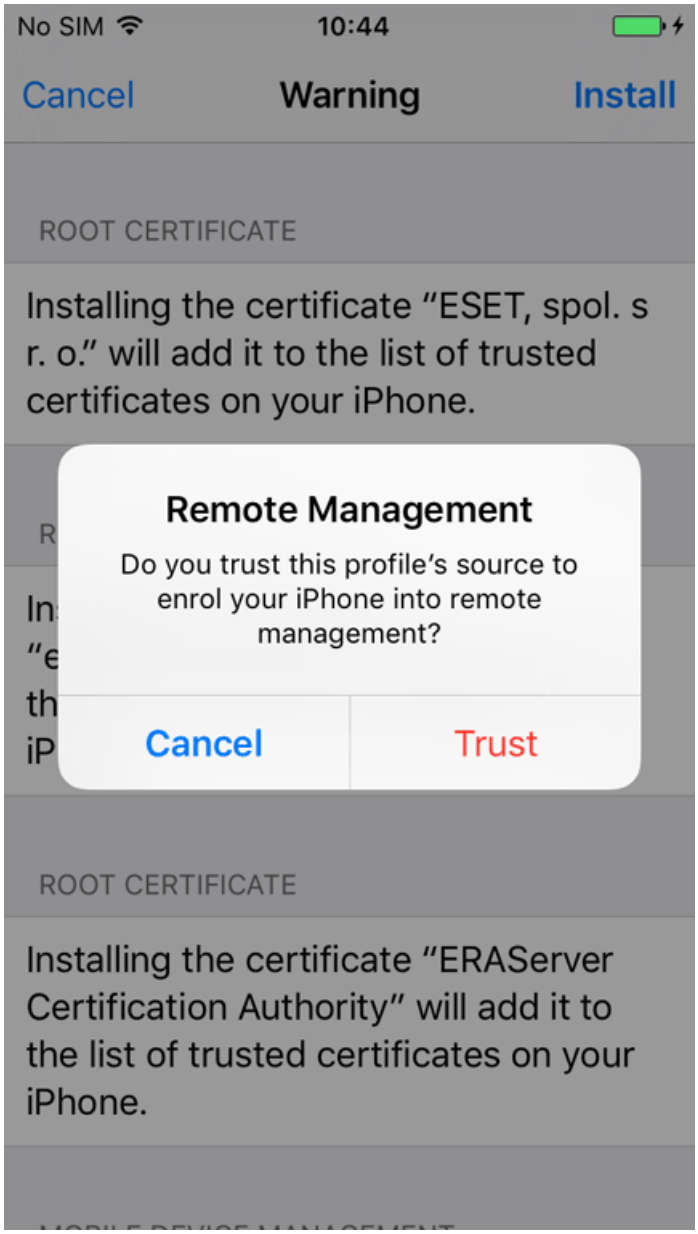
> Siga estas instrucciones para realizar la inscripción de un dispositivo iOS con Apple Business Manager (ABM).

1. Toque el enlace de inscripción recibido por correo electrónico (incluido el número de puerto) e ingréselo de forma manual en el navegador (por ejemplo, *https://eramdm:9980/<token>*) o puede usar el **Código QR**.

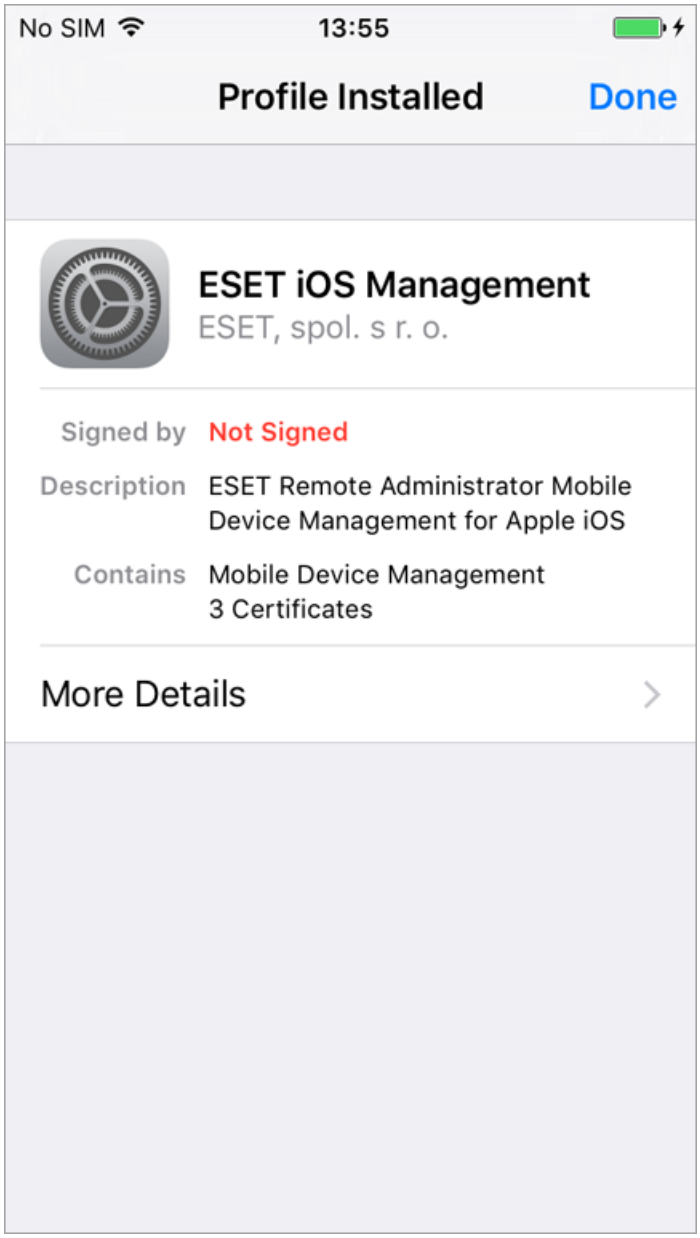
2. Toque en **instalar** para continuar en la pantalla de inscripción MDM **instalar perfil**.



3. Toque en **confiar** para permitir la instalación del nuevo perfil.

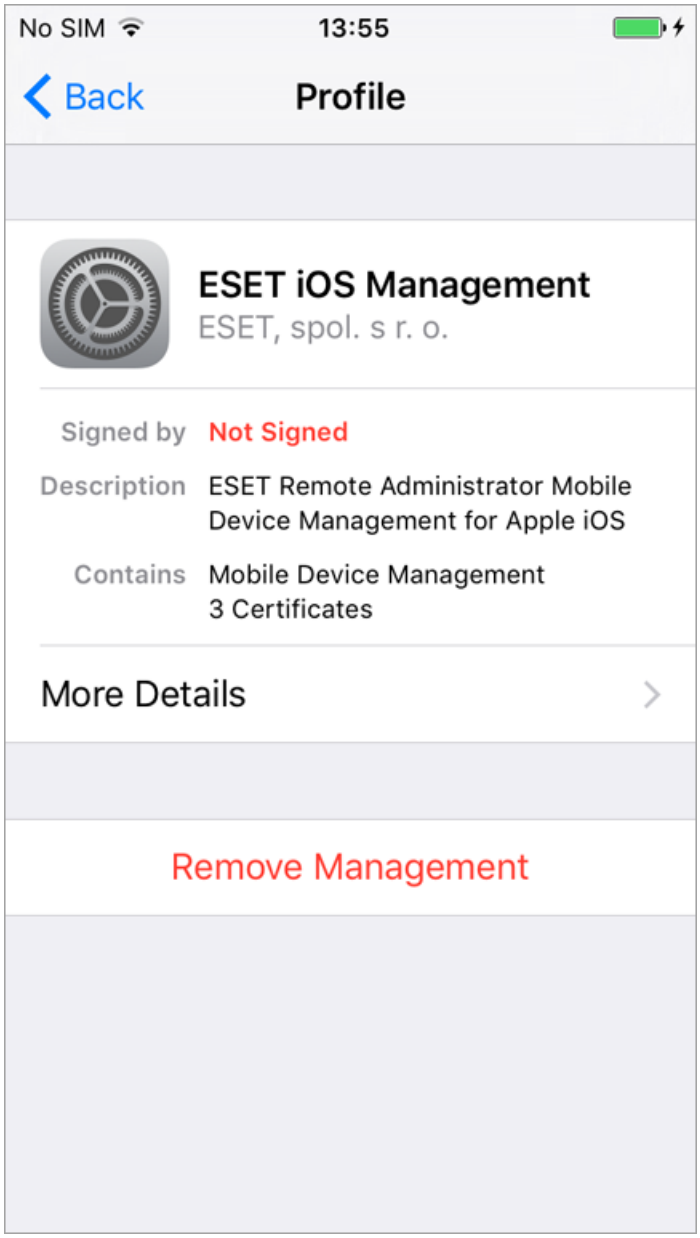


4. Después de instalar el nuevo perfil, el campo **Firmado por**, mostrará que el perfil **No firmado**. Esto se debe a que iOS no reconoce el certificado. Para tener un perfil de inscripción firmado, use un certificado HTTPS firmado por un CA de confianza de Apple. O puede usar su propio certificado de inscripción HTTPS para firmar la inscripción.



5. Este perfil de inscripción le permite configurar dispositivos y establecer políticas de seguridad para los usuarios o grupos.

La eliminación de este perfil de inscripción elimina todos los valores de la empresa (Correo, Calendario, Contactos, etc.) y el dispositivo móvil iOS no será administrado. Si un usuario elimina el perfil de inscripción, ESET PROTECT On-Prem no será consciente de ello y el estado del dispositivo cambiará a y luego a pasados 14 días porque el dispositivo no se conecta. No se dará otra indicación de que el perfil de inscripción se ha eliminado.



Inscripción de dispositivo iOS con ABM

Apple Business Manager (ABM) es el nuevo método de Apple para inscribir dispositivos iOS corporativos. Con ABM puede inscribir los dispositivos iOS sin contacto directo con el dispositivo y con mínima interacción por parte del usuario. La inscripción ABM de Apple le otorga a los administradores la opción de personalizar el proceso completo de configuración de dispositivos. También brinda la opción para evitar que los usuarios eliminen el perfil MDM del dispositivo. Puede inscribir sus dispositivos iOS existentes (si cumplen con los requisitos ABM de dispositivos iOS) y todos los dispositivos iOS que compre en el futuro. Para más información sobre ABM de Apple, consulte la guía de ABM de Apple y la documentación de ABM de Apple.

Sincronice su MDM de ESET PROTECT con el servidor Apple ABM:

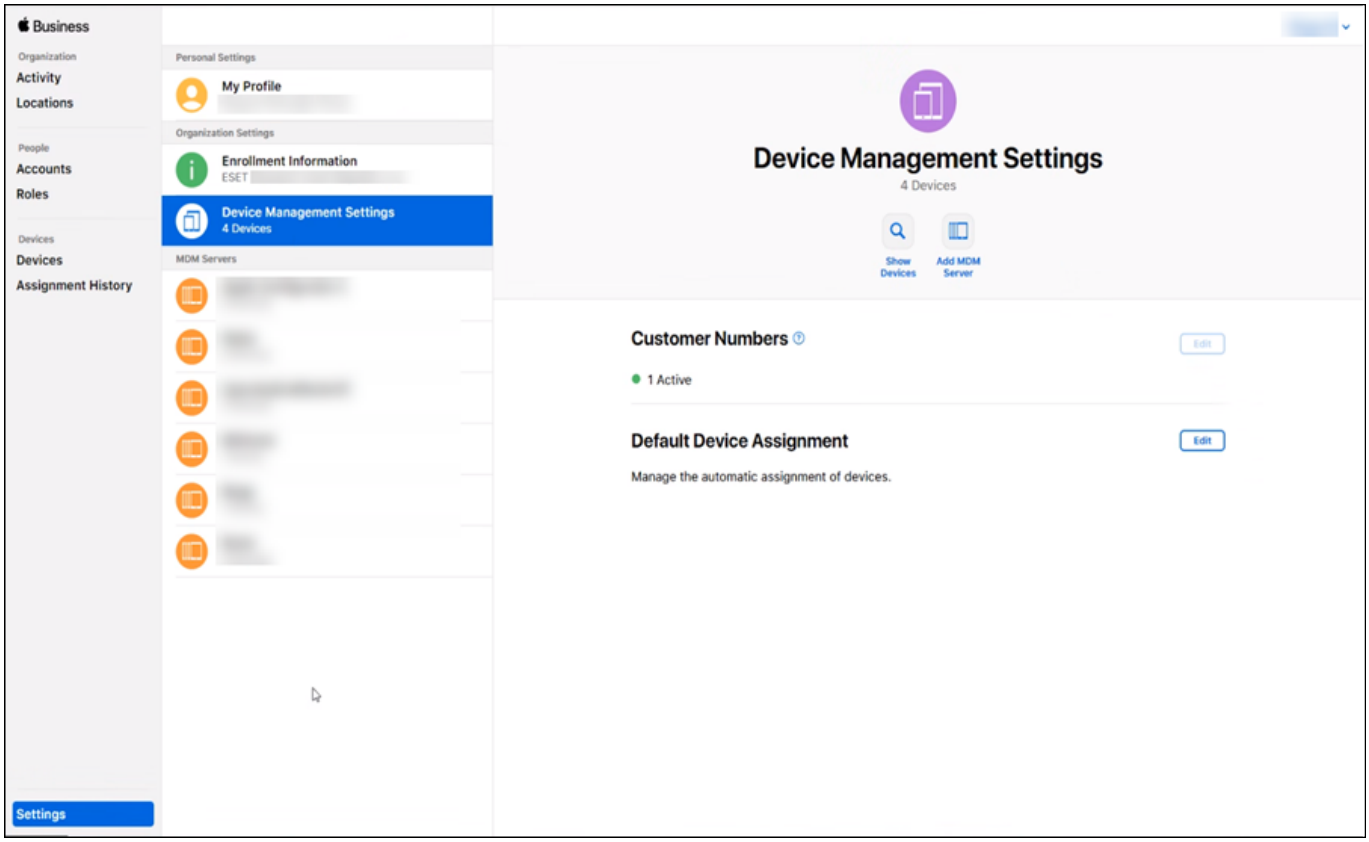
1. Verifique que se cumplan todos los requisitos de ABM de Apple en términos de requisitos de cuenta y requisitos de dispositivo.

Cuenta ABM:

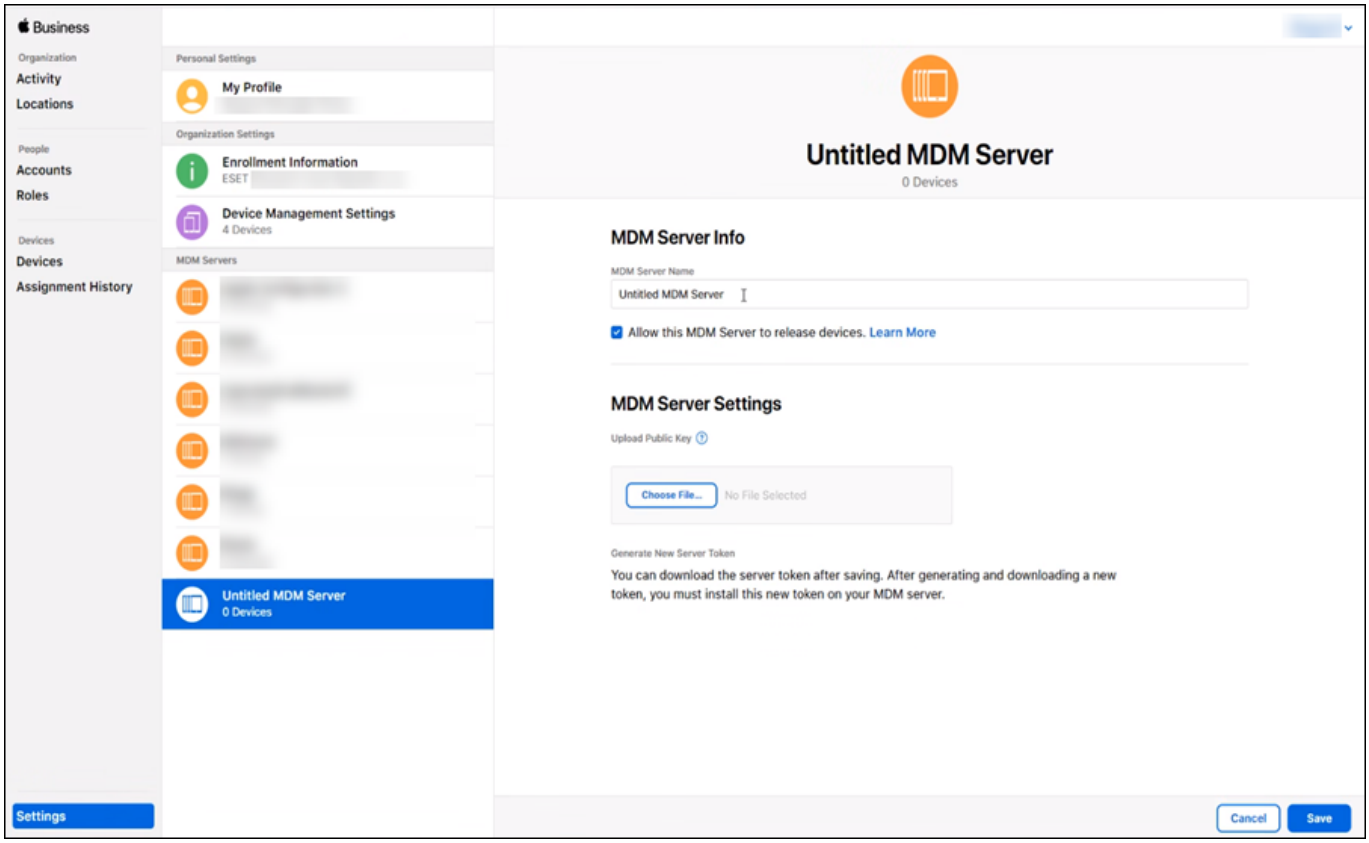
- El programa solo se encuentra disponible en ciertos países. Visite el sitio web de ABM de Apple para consultar si ABM se encuentra disponible en su país.
- Puede encontrar los requisitos de la cuenta ABM de Apple en estos sitios web: Requisitos del programa de implementación de Apple y Requisitos del programa de inscripción de dispositivos Apple
- Consulte los requisitos detallados del dispositivo de ABM.

2. Inicie sesión en su cuenta ABM de Apple (si no tiene una cuenta ABM de Apple, puede crear una).

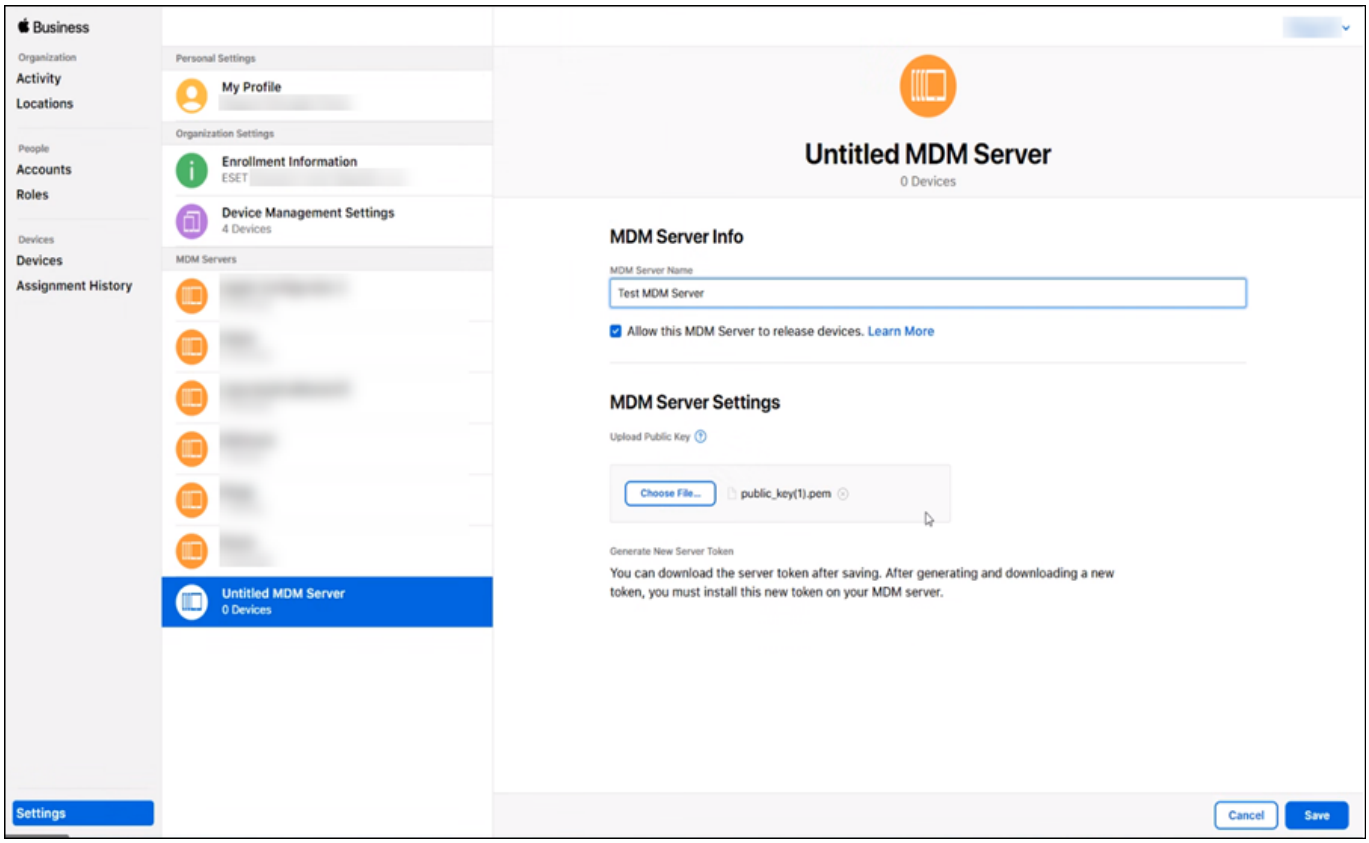
3. En la sección **Configuración de administración de dispositivos**, seleccione **Agregar servidor MDM**.



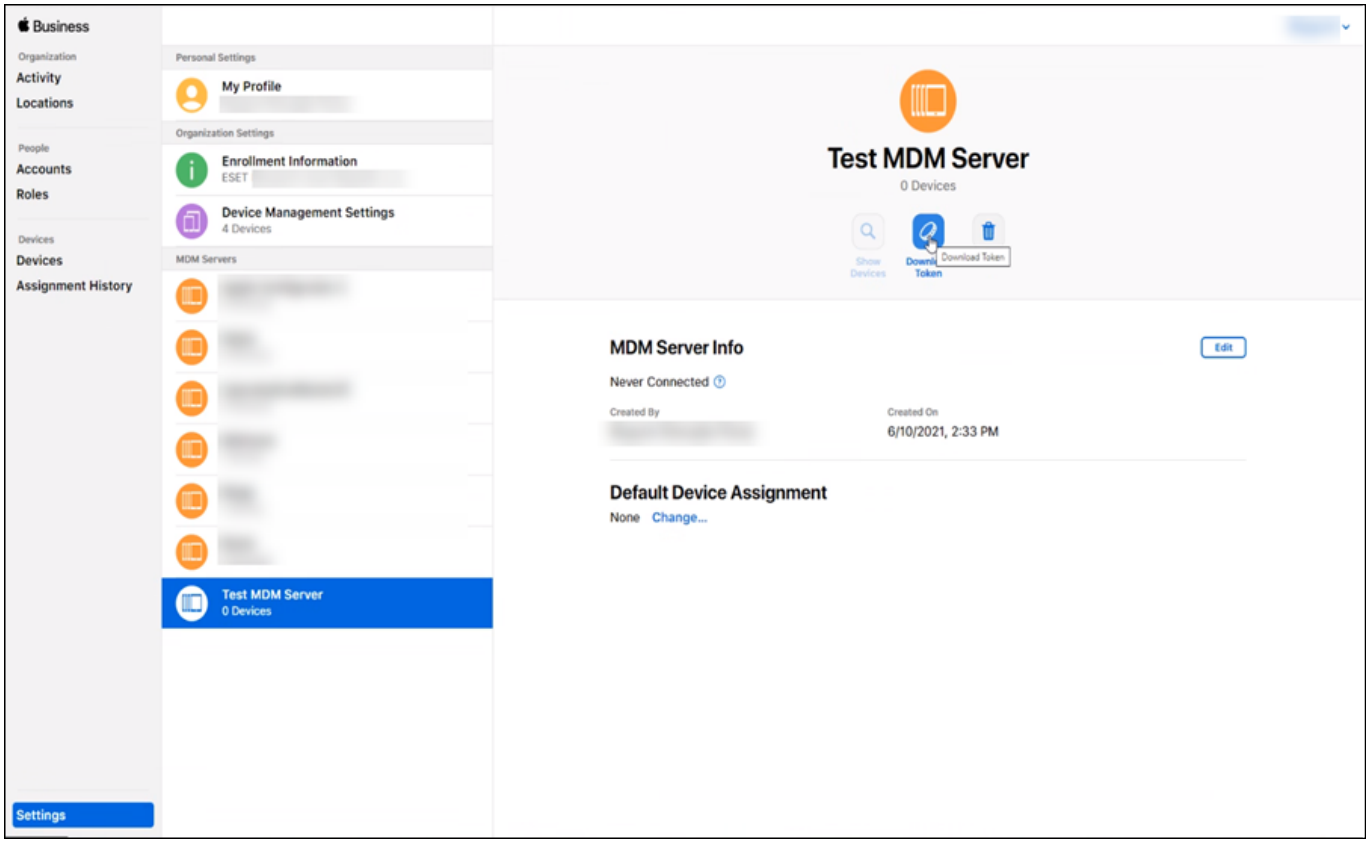
4. En la pantalla sin título del servidor MDM, escriba el **Nombre del servidor MDM**, por ejemplo: "MDM_Server,".



5. Cargue su clave pública en el portal ABM. Haga clic en **Seleccionar archivo** y seleccione el archivo de clave pública (este es el certificado APNS que descargó del portal de certificados push de Apple) y haga clic en **Guardar**.



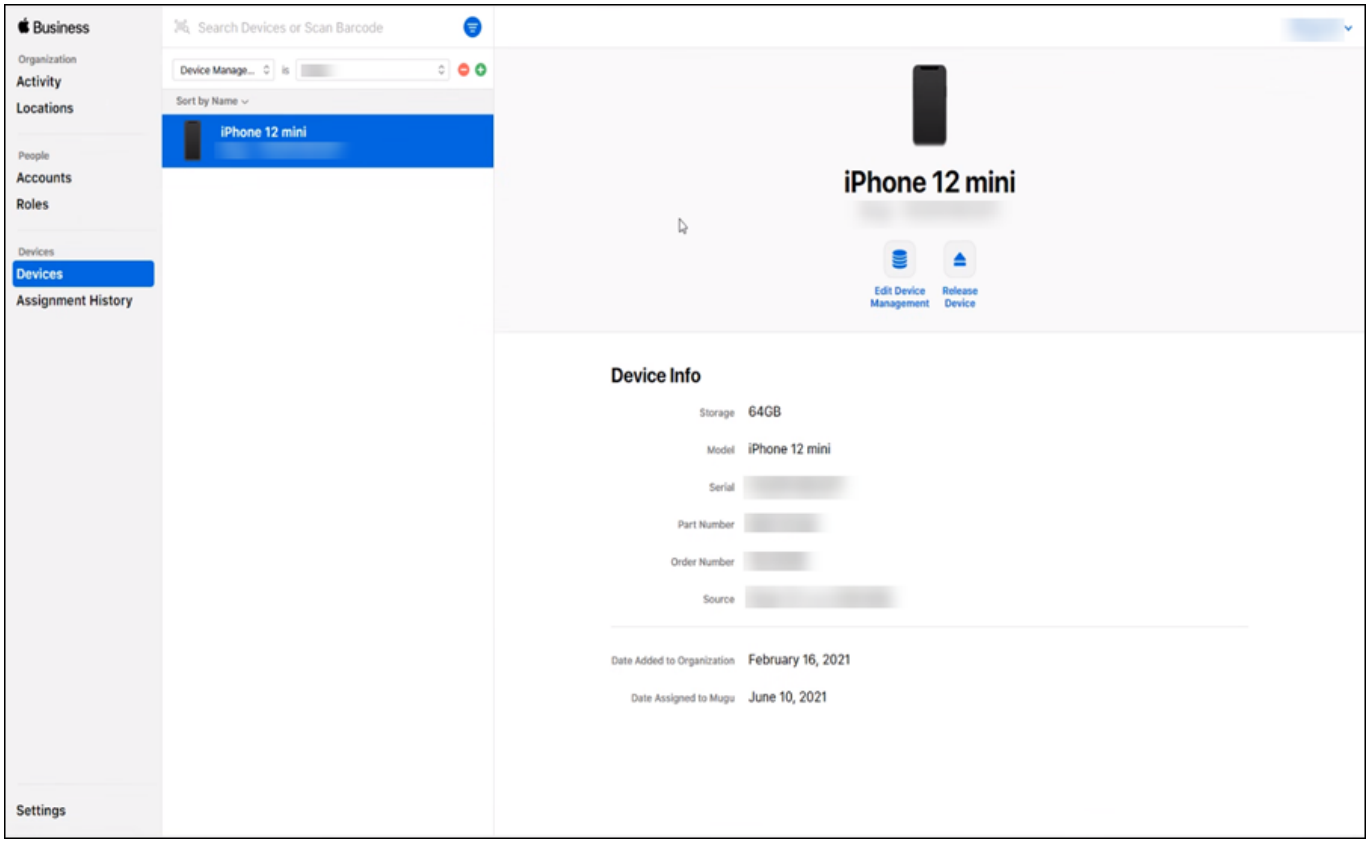
6. Haga clic en **Descargar token** para descargar su token de Apple ABM. Este archivo se cargará en la política MDC de ESET PROTECT en **Apple Business Manager (ABM)** > **Cargar token de autorización**.



Agregar dispositivo iOS a ABM de Apple

El siguiente paso es asignar dispositivos iOS a su servidor MDM virtual dentro del portal ABM de Apple. Puede asignar sus dispositivos iOS por número de serie, número de orden o cargando una lista de números de serie para dispositivo objetivo en formato CSV. En cualquier caso necesita asignar el dispositivo iOS al servidor MDM virtual (el que creó en los pasos anteriores).

1. Diríjase a la sección **Dispositivos** del portal de ABM, seleccione el dispositivo que desea asignar y haga clic en **Editar administración de dispositivos**.



2. Luego de seleccionar el servidor MDM de la lista, confirme su selección y el dispositivo móvil se asignará a su servidor MDM.

⚠ Una vez que se elimina un dispositivo del portal ABM se lo hace de forma permanente, no es posible volver a agregarlo.

Luego, puede salir del portal ABM de Apple y continuar en la consola web de ESET PROTECT.

⚠ Si está inscribiendo dispositivos iOS actualmente en uso (y que cumplen con los requisitos de dispositivo) se aplicarán las nuevas configuraciones de directivas luego de realizar un reseteo a fábrica del dispositivo objetivo.

Para completar el proceso de inscripción necesita cargar el certificado APNS a la directiva MDC que se asignará al servidor MDM. (Esta directiva MDC cumplirá el rol de configuración del servidor MDM.)

ℹ Si su dispositivo iOS muestra un mensaje de que no es posible descargar el perfil de ESET durante la inscripción, verifique que el servidor MDM dentro de ABM esté configurado correctamente (cuente con los certificados adecuados) y que asignó el dispositivo iOS correcto a su servidor MDM de ESET PROTECT seleccionado dentro de ABM de Apple.

Resolución de problemas: vuelva a agregar un dispositivo ABM eliminado

Si eliminó un dispositivo ABM de la lista de dispositivos de la ESET PROTECT Web Console, siga los pasos que se indican a continuación para volver a agregar el dispositivo a la ESET PROTECT Web Console:

1. Anule la asignación del dispositivo del servidor de administración de dispositivos móviles en ABM. No suelte el dispositivo en el portal ABM.

2. Espere 30 minutos.

3. Vuelva a asignar el dispositivo al servidor MDM.

Inscripción vía correo electrónico

Este método es ideal para la inscripción masiva de dispositivos móviles. Puede enviar un enlace de inscripción a un número de dispositivos por correo electrónico. Cada dispositivo móvil recibirá un token único por única vez basado en la dirección de correo electrónico.

Es obligatorio configurar el servidor SMTP para la inscripción masiva por correo electrónico. Vaya a **Más** > Configuración, amplíe la sección **Configuración avanzada** y especifique los detalles del servidor SMTP.

1.Para agregar nuevos dispositivos móviles, vaya a la sección **Equipos**. Seleccione el **Grupo estático** al que desea agregar dispositivos móviles y haga clic en **Agregar dispositivo** > **Dispositivos móviles**.

2.Vaya a la sección **Básica**.

3.**Seleccionar tipo**: seleccione **Android o iOS/iPadOS**.

4.**Distribución**: seleccione **Enviar correo electrónico**.

5.**Grupo principal**: si no tiene un grupo estático específico para dispositivos móviles, le recomendamos crear un **Grupo estático nuevo** (llamado **dispositivos móviles**, por ejemplo). Si ya tiene un grupo existente, haga clic en **Todos**, se abrirá una ventana donde podrá elegir el grupo estático.

6.**Personalizar más ajustes**

- **Mobile Device Connector**: se seleccionará automáticamente. Si tiene más de un MDC, seleccione el FQDN del MDC que desea usar. Si todavía no instaló el Conector de dispositivo móvil, consulte los capítulos Instalación del conector de dispositivo móvil: Windows o Linux para leer las instrucciones de instalación.
- **Licencia**: haga clic en **Seleccionar** y elija la licencia que se usará para la activación. Se creará una tarea de cliente de Activación del producto para el dispositivo móvil. Se tomará una unidad de licencia (una para cada dispositivo móvil).
- **Etiquetas:** seleccione o agregue etiquetas adecuadas para identificar el dispositivo móvil.

7.Vaya a **Configuración del producto**.

8. Seleccione la casilla de verificación **Acepto el Acuerdo de licencia de usuario final y confirmo estar de acuerdo con la Política de privacidad**. Consulte el Acuerdo de licencia de usuario final (EULA), los Términos de uso y la Política de privacidad de los productos ESET.

9.Vaya a **Lista**.

10. **Lista de dispositivos**: especifique los dispositivos móviles para inscripción, puede usar las siguientes funciones para agregar dispositivos móviles:

- **Agregar**: entrada única; necesita escribir manualmente una dirección de correo electrónico asociada

con el dispositivo móvil al cual se enviará el correo electrónico de inscripción. Si asigna un usuario al dispositivo móvil haciendo clic en **Alinear con usuario existente** y seleccionando al usuario, la dirección de correo electrónico se sobrescribirá y se reemplazará por la dirección especificada en la pantalla **Más** > Usuarios de equipos. Si desea agregar otro dispositivo móvil, haga clic en **Agregar** nuevamente y envíe la información necesaria.

- **Agregar usuario**: para agregar dispositivos, puede seleccionar las casillas de verificación enumeradas en **Más** > Usuarios de equipos. Haga clic en **Desemparejar** para corregir la lista de dispositivos móviles para inscripción. Una vez que desempareja un usuario asignado, dicho usuario aparecerá como no emparejado. Haga clic en **Emparejar** para seleccionar el usuario deseado para un dispositivo no emparejado. Haga clic en el ícono de la **Papelera** para eliminar una entrada.

- **Importar CSV** : un método que facilita agregar una gran cantidad de dispositivos móviles. Cargue un archivo *.csv* que contenga la lista de dispositivos para agregar, consulte Importar CSV para obtener más información.

- **Pegar del portapapeles:** Importar una lista personalizada de direcciones separadas con delimitadores personalizados (esta característica funciona de manera similar a una importación CSV).

> Le recomendamos asignar al menos un usuario a un dispositivo móvil. Si quiere usar las políticas personalizadas en iOS debe haber un usuario asignado a un dispositivo.
> Le recomendamos especificar el **Nombre del dispositivo** en cada entrada cuando use el método Importar CSV. Este nombre de dispositivo se muestra en la sección **Equipos**. Si deja vacío el campo **Nombre del dispositivo**, se usará la dirección de correo electrónico y aparecerá como nombre del dispositivo en **Equipos** y **Grupos**. Ello podría generar confusión, en especial si usa la misma dirección de correo electrónico para inscribir varios dispositivos. La dirección de correo electrónico aparecerá varias veces y le evitará poder distinguir entre los dispositivos.

11. Vaya a **Inscripción**.

12. **Vista previa de correo electrónico:** una plantilla de mensaje predefinida contiene los detalles necesarios para la inscripción del usuario. Las **Instrucciones** se muestran debajo del **Contenido** en el mensaje de correo electrónico de inscripción y contienen un **Nombre de dispositivo** (o una dirección de correo electrónico) con un enlace de inscripción (URL). Si usa una dirección de correo electrónico para inscribir varios dispositivos móviles, se mostrará una lista de dispositivos y cada una con su propio vínculo de inscripción (URL) asignado. También hay instrucciones que debe seguir el usuario del dispositivo móvil (iOS y Android) para completar la inscripción.

13. Cuando haga clic en **Enviar**, se enviará un correo electrónico a cada dirección de correo electrónico con los enlaces de inscripción adecuados e instrucciones.

14. Para finalizar la inscripción de dispositivos móviles, siga estos pasos o permita a los usuarios/propietarios de los dispositivos móviles realizar los pasos ellos mismos:

- Inscripción de dispositivo Android

- Inscripción de dispositivo iOS

Inscripción individual mediante vínculo o código QR

Si va a inscribir un dispositivo móvil mediante un vínculo de inscripción o un código QR, necesitará acceso físico al dispositivo. Además, para usar el código QR, deberá tener la aplicación de lector/explorador de código QR instalada en el dispositivo móvil.

> Para grandes cantidades de dispositivos móviles, le recomendamos usar la Inscripción por correo electrónico.

1.Para agregar nuevos dispositivos móviles, vaya a la sección **Equipos**. Seleccione el **Grupo estático al que desea agregar dispositivos móviles y** haga clic en **Agregar dispositivo** > **Dispositivos móviles**.

2.Vaya a la sección **Básica**.

3.**Seleccionar tipo**: seleccione **Android o iOS/iPadOS**.

4.**Distribución**: seleccione **Explorar código QR**.

5.**Grupo principal**: si no tiene un grupo estático específico para dispositivos móviles, le recomendamos crear un **Grupo estático nuevo** (llamado **dispositivos móviles**, por ejemplo). Si ya tiene un grupo existente, haga clic en **Todos**, se abrirá una ventana donde podrá elegir el grupo estático.

6.**Personalizar más ajustes**

- **Mobile Device Connector**: se seleccionará automáticamente. Si tiene más de un MDC, seleccione el FQDN del MDC que desea usar. Si todavía no instaló el Conector de dispositivo móvil, consulte los capítulos Instalación del conector de dispositivo móvil: Windows o Linux para leer las instrucciones de instalación.

- **Licencia**: haga clic en **Seleccionar** y elija la licencia que se usará para la activación. Se creará una tarea de cliente de Activación del producto para el dispositivo móvil. Se tomará una unidad de licencia (una para cada dispositivo móvil).

- **Etiquetas:** seleccione o agregue etiquetas adecuadas para identificar el dispositivo móvil.

7.Vaya a **Configuración del producto**.

8. Seleccione la casilla de verificación **Acepto el Acuerdo de licencia de usuario final y confirmo estar de acuerdo con la Política de privacidad**. Consulte el Acuerdo de licencia de usuario final (EULA), los Términos de uso y la Política de privacidad de los productos ESET.

9.Vaya a **Lista**.

10. **Lista de dispositivos**: especifique los dispositivos móviles para inscripción, puede usar las siguientes funciones para agregar dispositivos móviles:

- **Agregar**: entrada única; necesita escribir manualmente una dirección de correo electrónico asociada con el dispositivo móvil al cual se enviará el correo electrónico de inscripción. Si asigna un usuario al dispositivo móvil haciendo clic en **Alinear con usuario existente** y seleccionando al usuario, la dirección de correo electrónico se sobrescribirá y se reemplazará por la dirección especificada en la pantalla **Más** > Usuarios de equipos. Si desea agregar otro dispositivo móvil, haga clic en **Agregar** nuevamente y envíe

la información necesaria.

• **Agregar usuario**: para agregar dispositivos, puede seleccionar las casillas de verificación enumeradas en **Más** > Usuarios de equipos. Haga clic en **Desemparejar** para corregir la lista de dispositivos móviles para inscripción. Una vez que desempareja un usuario asignado, dicho usuario aparecerá como no emparejado. Haga clic en **Emparejar** para seleccionar el usuario deseado para un dispositivo no emparejado. Haga clic en el ícono de la **Papelera** para eliminar una entrada.

• **Importar CSV** : un método que facilita agregar una gran cantidad de dispositivos móviles. Cargue un archivo *.csv* que contenga la lista de dispositivos para agregar, consulte Importar CSV para obtener más información.

• **Pegar del portapapeles:** Importar una lista personalizada de direcciones separadas con delimitadores personalizados (esta característica funciona de manera similar a una importación CSV).

11. Después de hacer clic en **Continuar**, se mostrará una lista de dispositivos con el **Enlace** de inscripción (URL) y el **código QR** correspondientes. Escriba la URL completa en el navegador web del dispositivo manualmente (por ejemplo *https://eramdm:9980/token*, el token será diferente para cada dispositivo móvil) o envíe esta URL al dispositivo móvil por otros medios. Como alternativa, puede usar un **Código QR**, que sería más conveniente que escribir la URL, pero requiere un lector/explorador de código QR en el dispositivo móvil.

12. Una vez que haya completado la inscripción de todos los dispositivos seleccionados, haga clic en **Finalizar**.

13. Para realizar la inscripción real de los dispositivos móviles, siga estas instrucciones detalladas:

- Inscripción de dispositivo Android
- Inscripción de dispositivo iOS

Propietario del dispositivo Android (solo Android 7 y posteriores)

Si va a inscribir un dispositivo móvil Android mediante un código de inscripción QR, necesitará acceso físico al dispositivo. Además, esta inscripción solo es posible en un dispositivo después de que haya sido borrado o restablecido al ajuste de fábrica o que esté listo para usarse.

> No es posible usar la Inscripción vía correo electrónico para la inscripción masiva de dispositivos Android como un Propietario de dispositivos.

1.Para agregar nuevos dispositivos móviles, vaya a la sección **Equipos**. Seleccione el **Grupo estático al que desea agregar dispositivos móviles y** haga clic en **Agregar dispositivo** > **Dispositivos móviles**.

2.Vaya a la sección **Básica**.

3.**Seleccionar tipo**: Seleccione **Propietario del dispositivo Android (solo Android 7 y posteriores)**.

4.**Distribución**: seleccione **Explorar código QR**.

5.**Grupo principal**: si no tiene un grupo estático específico para dispositivos móviles, le recomendamos crear un **Grupo estático nuevo** (llamado **dispositivos móviles**, por ejemplo). Si ya tiene un grupo existente, haga clic en **Todos**, se abrirá una ventana donde podrá elegir el grupo estático.

6.**Personalizar más ajustes**

- **Mobile Device Connector**: se seleccionará automáticamente. Si tiene más de un MDC, seleccione el FQDN del MDC que desea usar. Si todavía no instaló el Conector de dispositivo móvil, consulte los capítulos Instalación del conector de dispositivo móvil: Windows o Linux para leer las instrucciones de instalación.

- **Licencia**: haga clic en **Seleccionar** y elija la licencia que se usará para la activación. Se creará una tarea de cliente de Activación del producto para el dispositivo móvil. Se tomará una unidad de licencia (una para cada dispositivo móvil).

- **Etiquetas:** seleccione o agregue etiquetas adecuadas para identificar el dispositivo móvil.

7.Vaya a **Configuración del producto**.

8. Seleccione la casilla de verificación **Acepto el Acuerdo de licencia de usuario final y confirmo estar de acuerdo con la Política de privacidad**. Consulte el Acuerdo de licencia de usuario final (EULA), los Términos de uso y la Política de privacidad de los productos ESET.

9.Vaya a **Lista**.

10. **Lista de dispositivos**: especifique los dispositivos móviles para inscripción, puede usar las siguientes funciones para agregar dispositivos móviles:

- **Agregar**: entrada única; necesita escribir manualmente una dirección de correo electrónico asociada con el dispositivo móvil al cual se enviará el correo electrónico de inscripción. Si asigna un usuario al dispositivo móvil haciendo clic en **Alinear con usuario existente** y seleccionando al usuario, la dirección de correo electrónico se sobrescribirá y se reemplazará por la dirección especificada en la pantalla **Más** > Usuarios de equipos. Si desea agregar otro dispositivo móvil, haga clic en **Agregar** nuevamente y envíe la información necesaria.

- **Agregar usuario**: para agregar dispositivos, puede seleccionar las casillas de verificación enumeradas en **Más** > Usuarios de equipos. Haga clic en **Desemparejar** para corregir la lista de dispositivos móviles para inscripción. Una vez que desempareja un usuario asignado, dicho usuario aparecerá como no emparejado. Haga clic en **Emparejar** para seleccionar el usuario deseado para un dispositivo no emparejado. Haga clic en el ícono de la **Papelera** para eliminar una entrada.

- **Importar CSV** : un método que facilita agregar una gran cantidad de dispositivos móviles. Cargue un archivo *.csv* que contenga la lista de dispositivos para agregar, consulte Importar CSV para obtener más información.

- **Pegar del portapapeles:** Importar una lista personalizada de direcciones separadas con delimitadores personalizados (esta característica funciona de manera similar a una importación CSV).

11. Después de hacer clic en **Continuar**, se mostrará una lista de dispositivos con el **Enlace** de inscripción (URL) y el **código QR** correspondientes. Escriba la URL completa en el navegador web del dispositivo manualmente (por ejemplo *https://eramdm:9980/token*, el token será diferente para cada dispositivo móvil) o envíe esta URL al dispositivo móvil por otros medios. Como alternativa, puede usar un **Código QR**,

que sería más conveniente que escribir la URL, pero requiere un lector/explorador de código QR en el dispositivo móvil.

12. Una vez que haya completado la inscripción de todos los dispositivos seleccionados, haga clic en **Finalizar**.

13. Siga estos pasos en el dispositivo Android para realizar el proceso de inscripción.

Crear una política para iOS MDM - Cuenta de Exchange ActiveSync

Esta política rige todas las configuraciones para dispositivos iOS. Esta configuración se aplica a dispositivos iOS ABM y no ABM.

- La configuración solo para ABM se marca con un ícono de ABM 

. Esta configuración solo se aplica a dispositivos iOS inscritos en el portal ABM de Apple. Recomendamos que no personalice esta configuración solo de ABM al crear una política para dispositivos iOS no ABM.

- Algunas configuraciones solo se pueden aplicar a un dispositivo iOS con cierta versión de iOS. Estos ajustes están marcados por un icono que representa la versión de iOS, por ejemplo, iOS versión 11.0 y posteriores 

.

- Si ambos íconos (el ícono ABM y el de versión de iOS) se muestran junto a una configuración específica, el dispositivo debe cumplir ambos requisitos o la administración de la configuración fallará.

Consulte el escenario de ejemplo a continuación que explica cómo utilizar una política MDM de iOS cuando desea configurar una cuenta de correo electrónico de Microsoft Exchange:

Puede usar esta directiva para configurar una cuenta de correo de Microsoft Exchange, los contactos y el calendario en usuarios de dispositivos móviles con iOS. La ventaja de usar esta política es que sólo necesita crear una directiva que luego podrá aplicar a muchos dispositivos móviles iOS sin necesidad de configurar cada uno por separado. Esto es posible usando los atributos de usuario de Active Directory. Debe especificar una variable, por ejemplo, `${exchange_login/exchange}` que se reemplazará con un valor de AD para un usuario particular.

Si no usa Microsoft Exchange o Exchange ActiveSync, puede configurar manualmente cada servicio (**Cuentas de correo**, **Cuentas de contactos**, **Cuentas de LDAP**, **Cuentas de calendario** y **Cuentas de calendario suscritas**).

El siguiente es un ejemplo de cómo crear y aplicar una nueva política para configurar automáticamente el correo, los contactos y el calendario para cada usuario en un dispositivo móvil iOS, usando el protocolo Exchange ActiveSync (EAS) para sincronizar estos servicios.

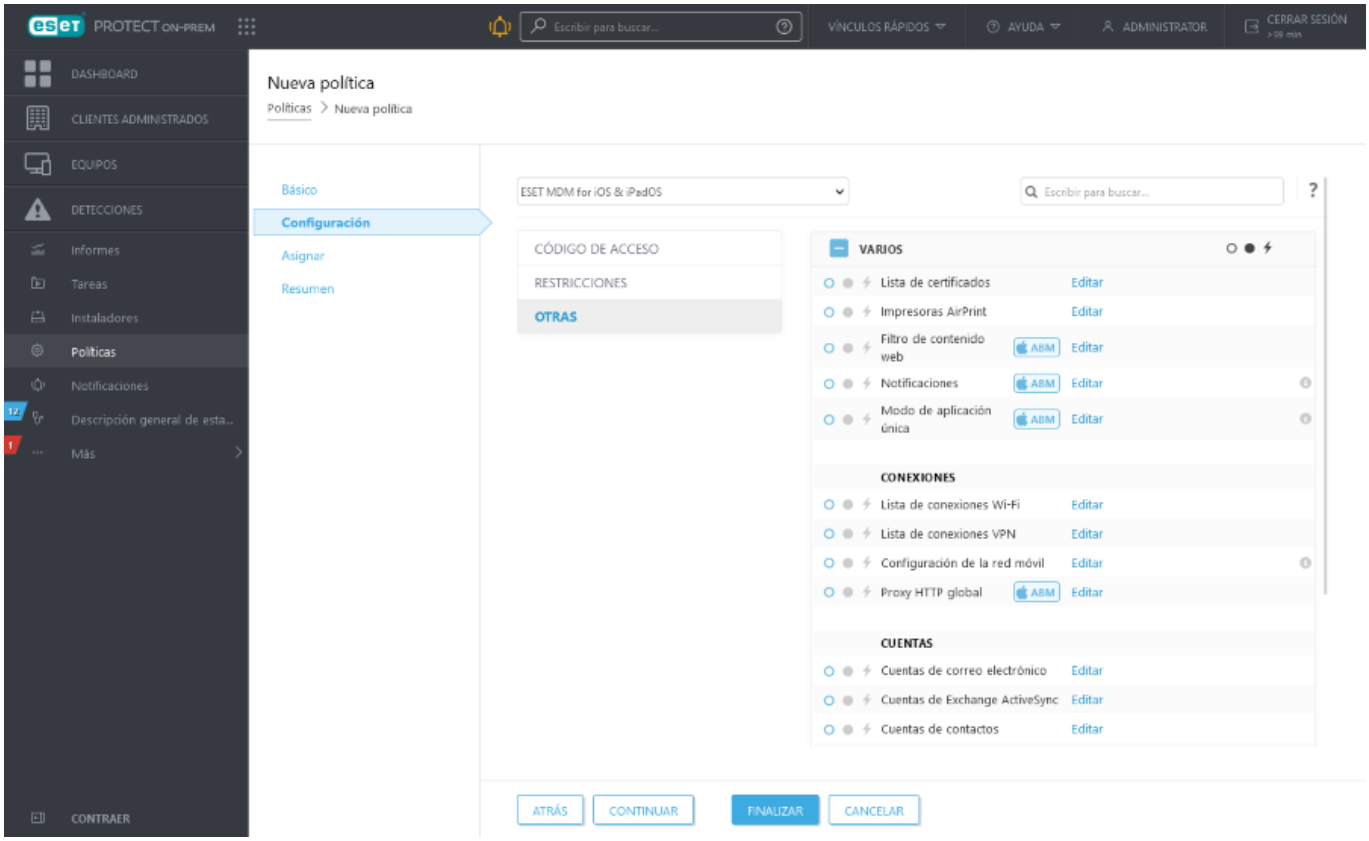
> Antes de comenzar a configurar esta política, asegúrese de haber realizado los pasos descritos en Administración de dispositivos móviles.

Básica

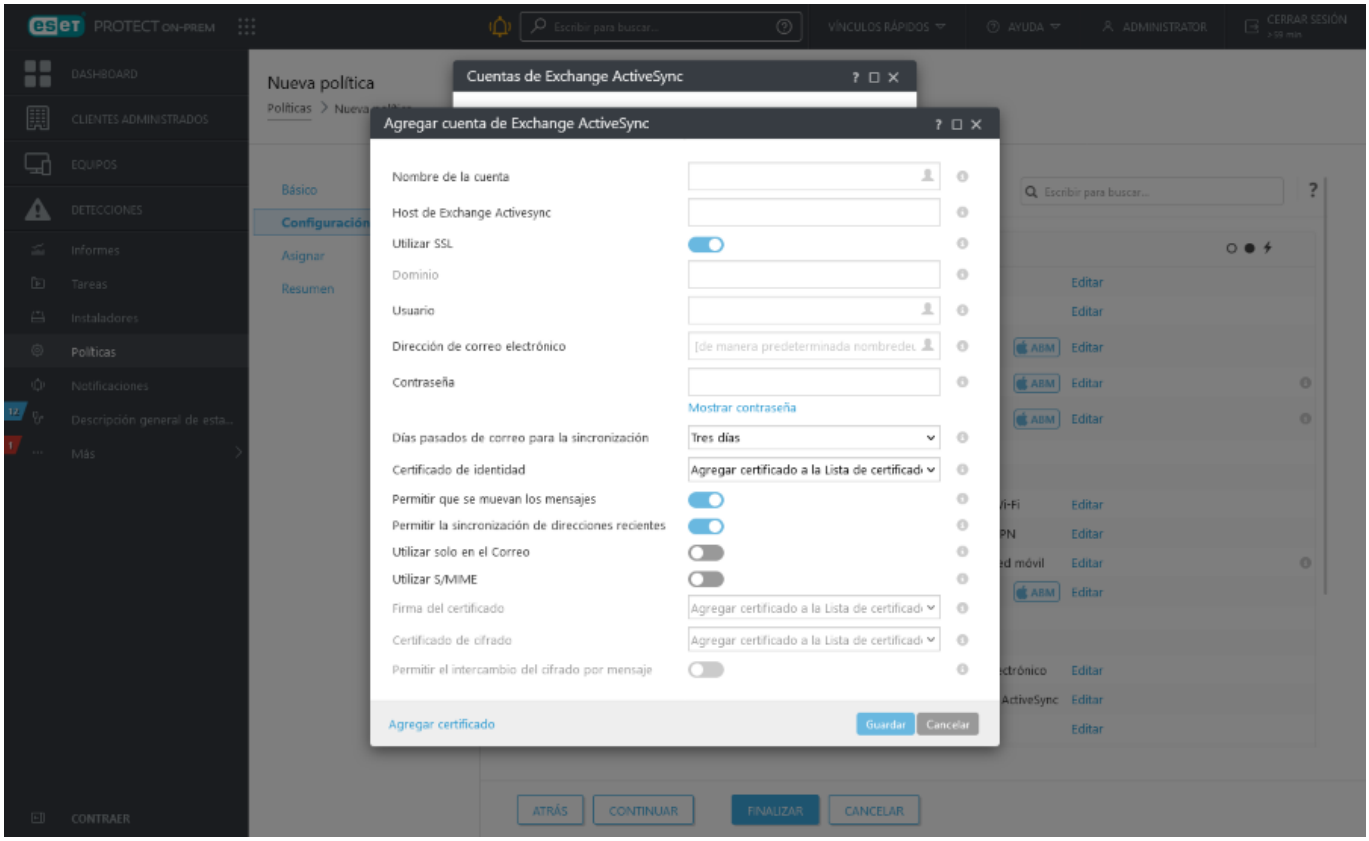
Ingrese un **Nombre** para esta política. El campo **Descripción** es opcional.

Configuración

Seleccione **MDM de ESET para iOS/iPadOS** desde el menú desplegable, haga clic en **Otros** para expandir las categorías y haga clic en **Editar** junto a **Cuentas de Exchange ActiveSync**.



Haga clic en **Agregar** y especifique los detalles de su cuenta de Exchange ActiveSync. Podrá usar variables para ciertos campos (seleccionando de la lista desplegable), como Usuario o Dirección de correo electrónico. Estas variables serán reemplazadas por los valores reales de Usuarios de equipos cuando se aplica una política.



• **Nombre de la cuenta**: ingrese el nombre de la cuenta de Exchange.

• **Host de Exchange ActiveSync**: especifica el nombre de host de Exchange Server o su dirección IP.

• **Usar SSL**: esta opción se encuentra habilitada de forma predeterminada. Especifica si Exchange Server usa la Capa de sockets seguros (SSL) para la autenticación.

• **Dominio**: este campo es opcional. Puede ingresar el dominio al que pertenece esta.

• **Usuario**: nombre de usuario de Exchange. Seleccione la variable correspondiente desde la lista desplegable para usar el atributo de Active Directory para cada usuario.

• **Dirección de correo electrónico**: seleccione la variable correspondiente desde la lista desplegable para usar un atributo de Active Directory para cada usuario.

• **Contraseña**: opcional. Le recomendamos que deje este campo vacío. Si se deja en blanco, se les pedirá a los usuarios que creen sus propias contraseñas.

• **Días pasados de correo para la sincronización**: seleccione el número de días pasados de correo electrónico que desea sincronizar desde la lista desplegable.

• **Identificar certificado**: credenciales para conectarse con ActiveSync.

• **Permitir que se muevan los mensajes**: si se activa esta opción, se podrán mover los mensajes desde esta cuenta a otra.

• **Permitir la sincronización de direcciones recientes**: si se habilita esta opción, se le permitirá al usuario sincronizar direcciones usadas recientemente entre dispositivos.

• **Usar solo en el Correo**: habilite esta opción si desea permitir solamente a la aplicación de correo para

enviar mensajes de correo electrónico salientes desde esta cuenta.

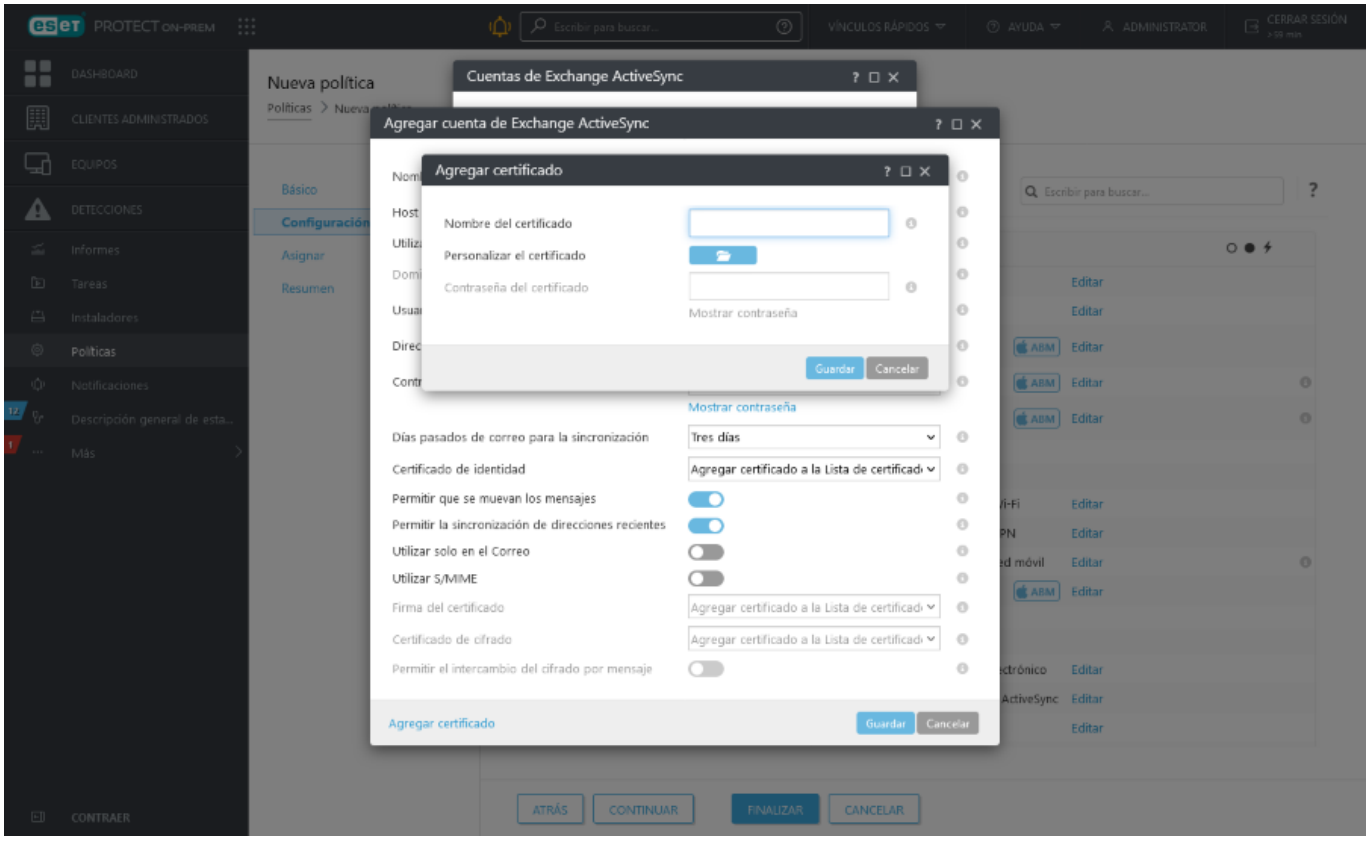
• **Usar S/MIME**: habilite esta opción para usar el cifrado S/MIME en los mensajes de correo electrónico salientes.

• **Firma del certificado**: credenciales para firmar los datos MIME.

• **Certificado de cifrado**: credenciales para el cifrado de los datos MIME.

• **Activar el conmutador del cifrado por mensaje**: permite al usuario seleccionar si desea cifrar cada mensaje.

Si no especifica un valor y dejar el campo en blanco, a los usuarios de dispositivos móviles se les pedirá que ingresen este valor. Por ejemplo una **Contraseña**.

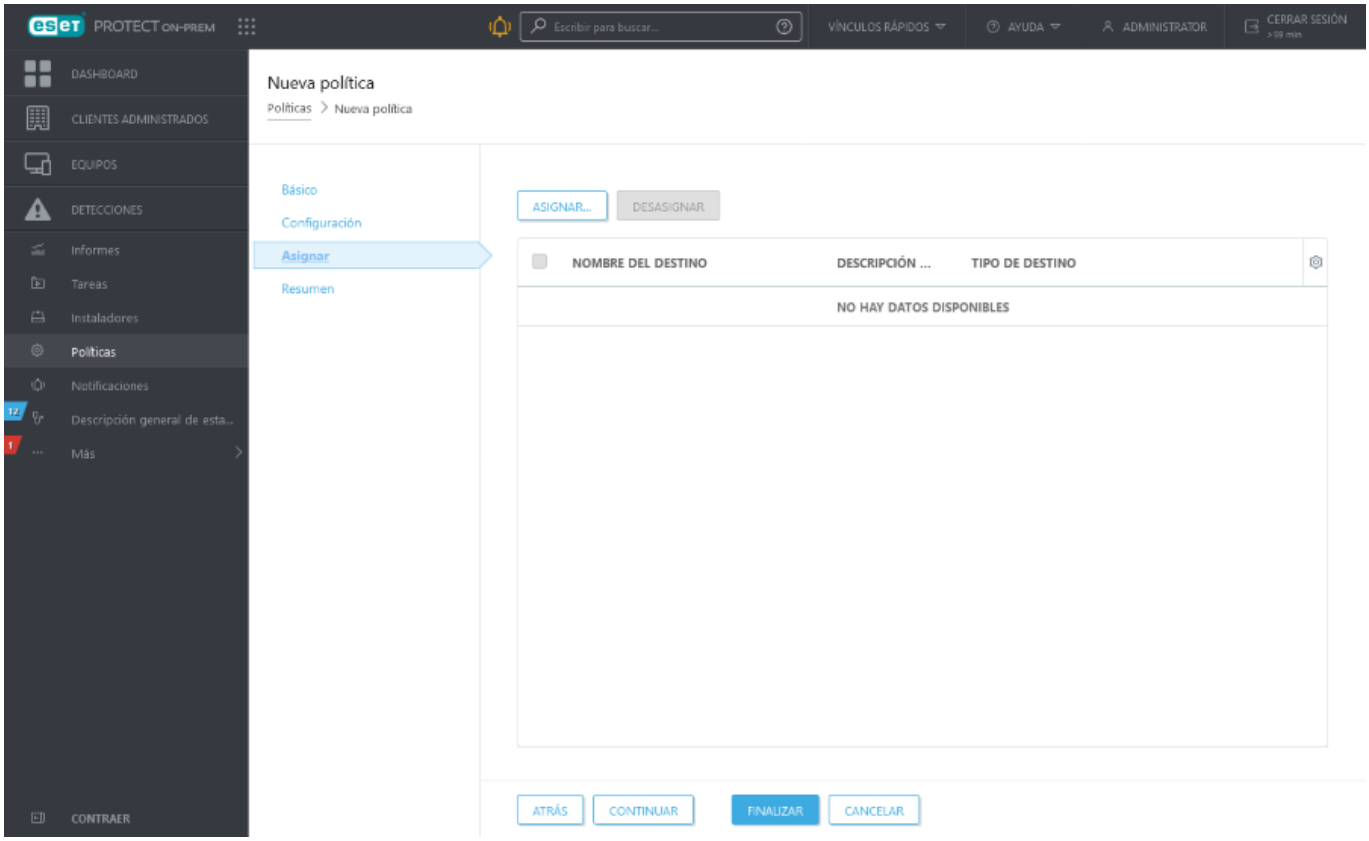


• **Agregar certificado** : puede agregar certificados de Exchange específicos (identidad del usuario, firma digital o certificado de cifrado) si es requerido.

Siguiendo los pasos anteriores, podrá agregar varias cuentas de Exchange ActiveSync, si así lo desea. De esta manera, habrá más cuentas configuradas en un dispositivo móvil. También podrá editar las cuentas existentes si fuera necesario.

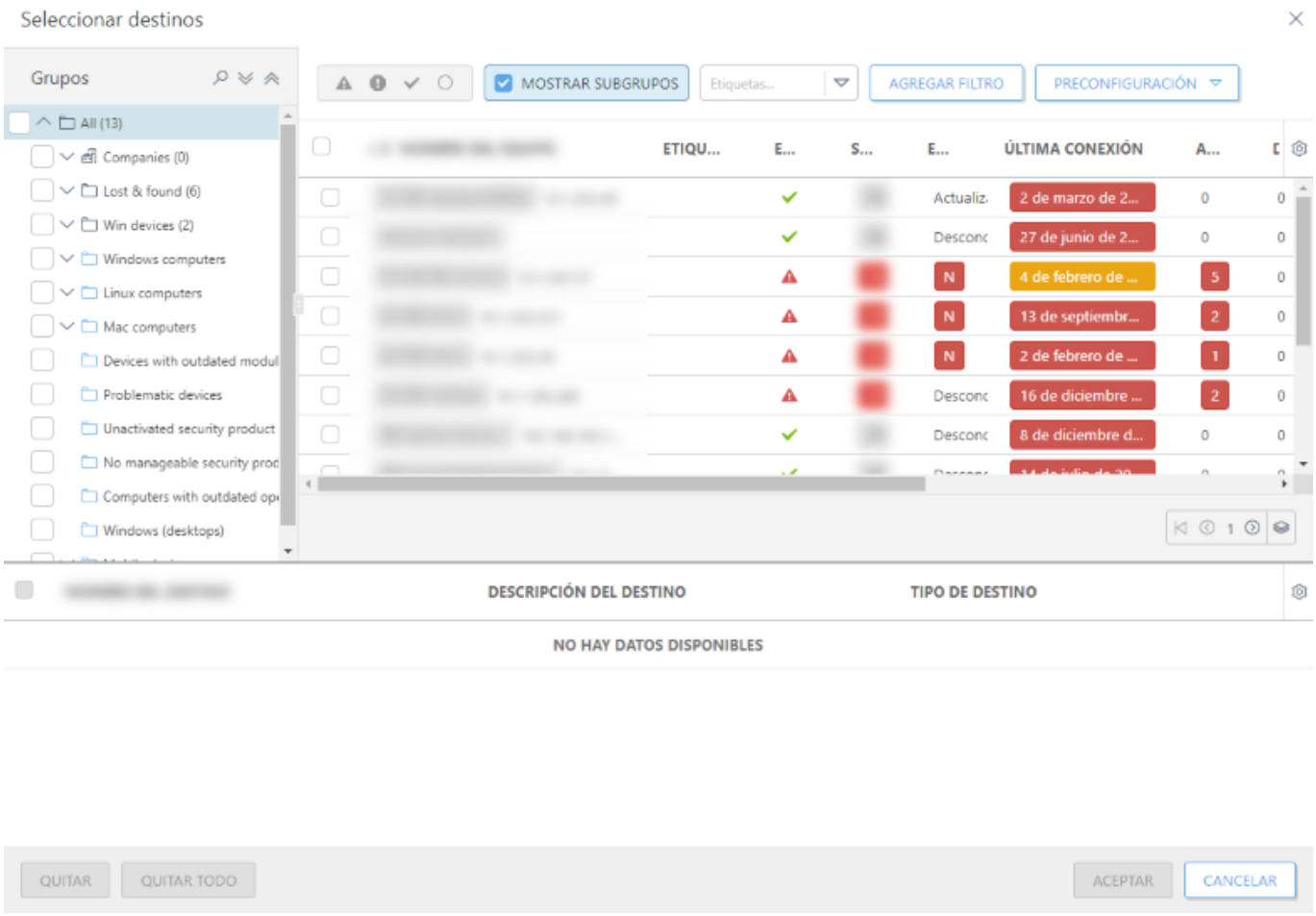
Asignar

Especifique los clientes (equipos/dispositivos móviles individuales o grupos completos) que serán los destinatarios de esta directiva.



Haga clic en **Asignar** para visualizar todos los Grupos estáticos y dinámicos y a sus miembros. Seleccione los equipos o grupos que desee y haga clic en **Aceptar**.

Para asignar todos los equipos de un grupo, asigne el grupo en lugar de los equipos individuales para evitar que la consola web se ralentice.
Si selecciona una gran cantidad de equipos, la consola web muestra una advertencia.



Resumen

Revise la configuración de esta política y haga clic en **Finalizar**. La política se aplica a los destinos después de su próxima conexión con el servidor de ESET PROTECT (en función del intervalo de conexión del agente).

Crear una política para que MDC active APN/ABM para la inscripción de iOS

Al cambiar e certificado https usado en su política para MDC, siga estos pasos para evitar desconectar dispositivos móviles de su MDM:
1. Cree y aplique la nueva política que use el certificado https.
2. Permita a los dispositivos registrarse en el servidor MDM y recibir la nueva política.
3 Verifique que los dispositivos estén usando el nuevo certificado https (el intercambio del certificado https está completo).
4. Deje pasar por lo menos 72 horas para que sus dispositivos reciban la nueva política. Después de que todos los dispositivos hayan recibido la nueva política (ya no se muestra la Alerta MDM Core "El cambio del certificado HTTPS sigue en progreso. Se sigue usando el antiguo certificado" en la pestaña de Alertas), puede quitar la política anterior.

Este es un ejemplo de cómo crear una nueva política para que el Conector de dispositivo móvil ESET active APNS (Servicios de notificaciones push de Apple) y la función del Programa de registro de dispositivos iOS. Esto es necesario para la Inscripción de dispositivos iOS. Antes de configurar esta política, cree un nuevo certificado APN y hágalo firmar por Apple en el Portal de certificados push de Apple de manera que se convierta en un certificado

firmado o en un **Certificado APNS**. Para obtener instrucciones paso a paso vea la sección Certificado APN.

Básica

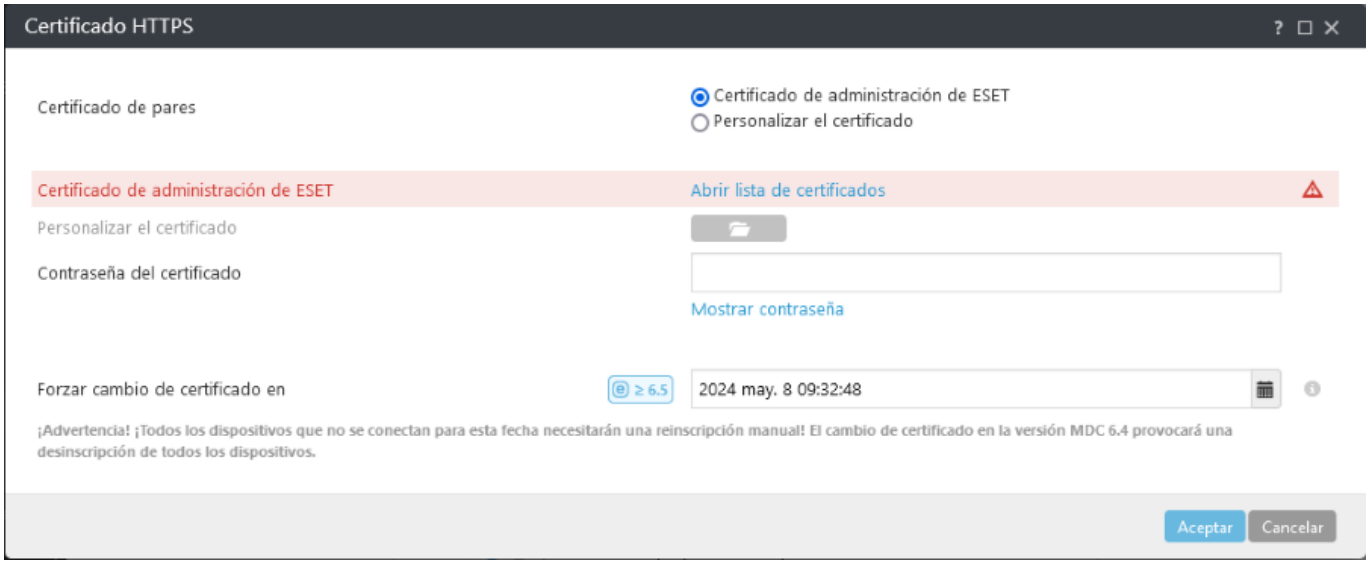
Ingrese un **Nombre** para esta política. El campo **Descripción** es opcional.

Configuración

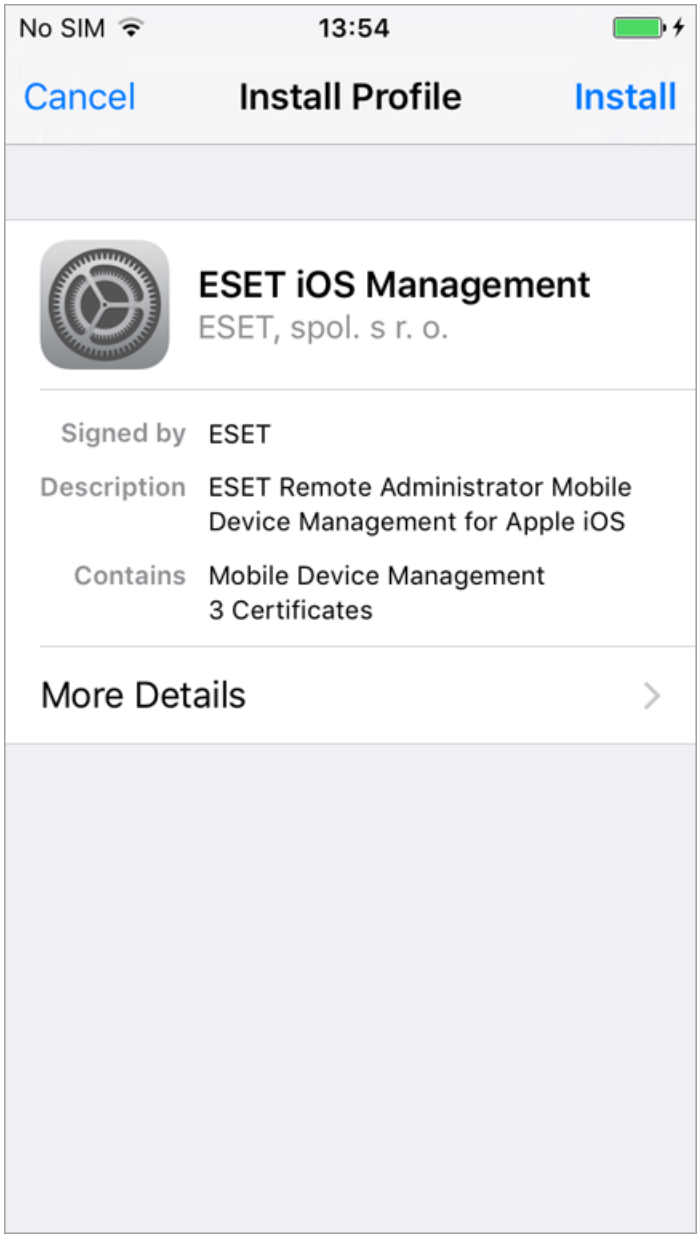
Seleccione **Conector de dispositivo móvil con ESET** de la lista desplegable.

Si instaló un servidor MDM con un instalador todo en uno (no como independiente ni como componente) el certificado HTTPS se generó automáticamente durante la instalación. Para los demás casos deberá aplicar un certificado HTTPS personalizado. Puede encontrar más información comentada luego del paso uno del tema de administración de dispositivo móvil.
Puede usar el certificado ESET PROTECT (firmado por la AC ESET PROTECT On-Prem) o su certificado personalizado. También puede especificar la fecha para el **Cambio forzado de certificado**. Haga clic en el símbolo de herramienta junto a esta configuración para obtener más información.

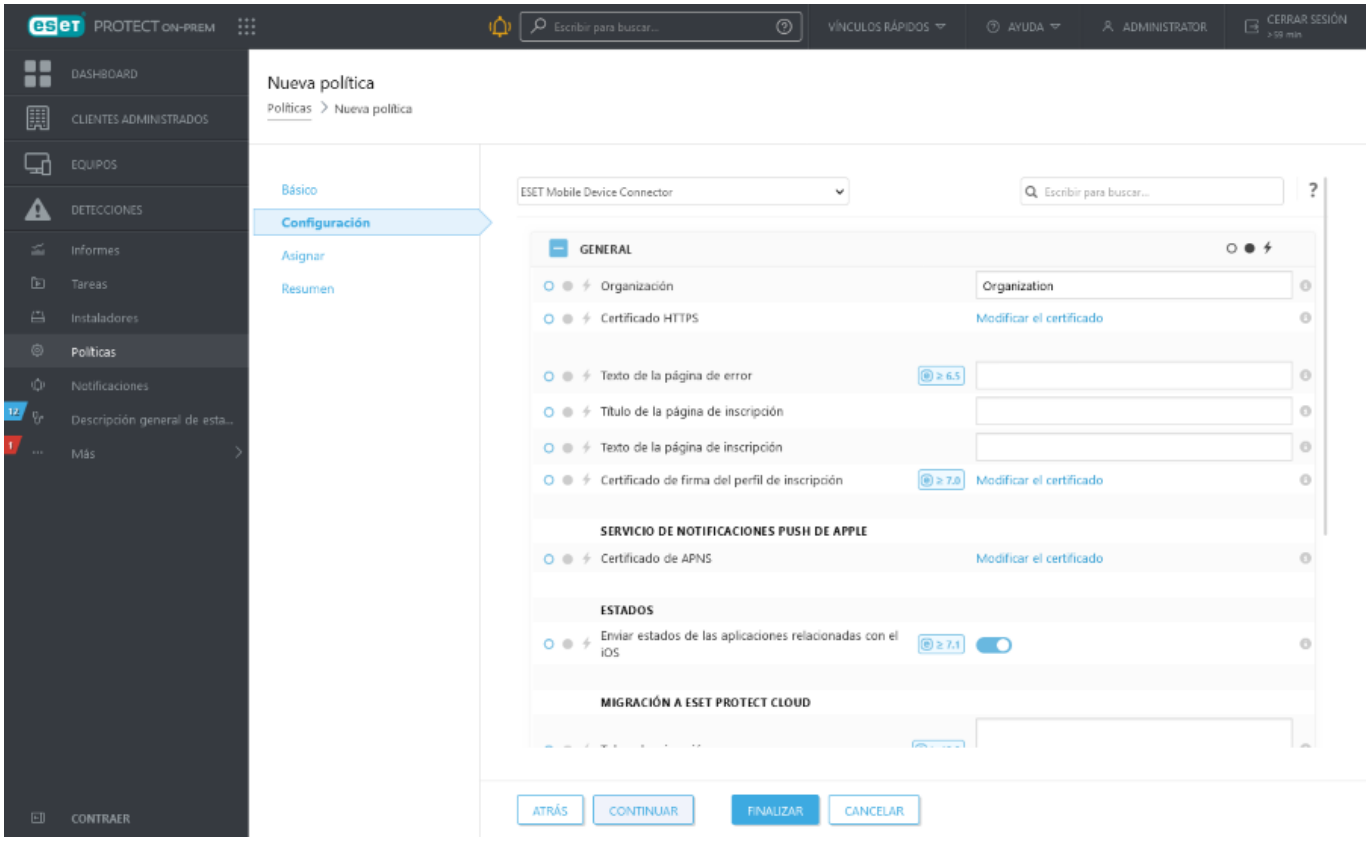
Escriba el nombre exacto de su organización sobre la cadena **Organización**. Esto será usado por el generador de perfil de inscripción para incluir esta información en el perfil.



En **General**, puede cargar de manera opcional su certificado HTTPS para el registro en el **Certificado de firma del perfil de inscripción** (esto solo afecta el registro que no sea ABM). Esto permitirá que la página de registro para dispositivos iOS que visiten durante el proceso de registro quede firmada que sean visibles en el archivo **Firmado por** ubicado en el certificado.

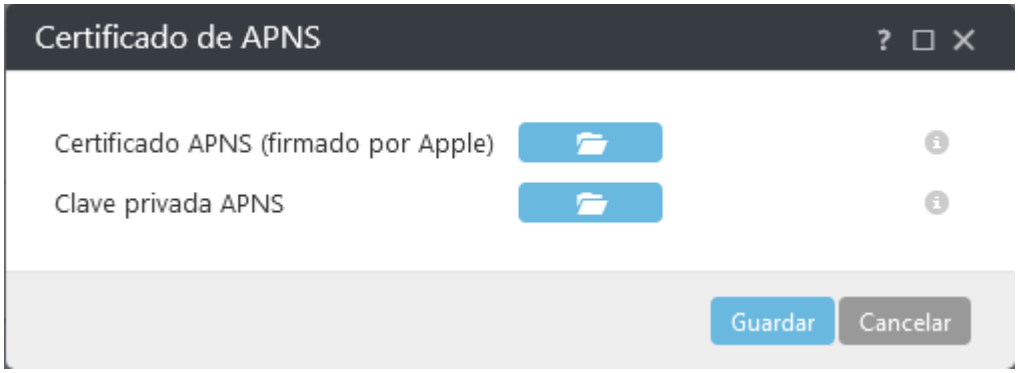


Cargar los certificados de Apple para registro en iOS: Navegue hasta el Servicio de notificaciones Push de Apple y cargue el Certificado de APNS y una Clave privada de APNS.



Certificado APNS (firmado por Apple): haga clic en la carpeta y busque el Certificado APNS para cargarlo. El Certificado de APNS es el archivo que descargó del Portal de certificados push de Apple.

Clave privada de APNS: haga clic en la carpeta y busque la Clave privada de APNS para cargarla. La clave privada de APNS es el archivo que descargó durante la creación del certificado APN/ABM.



Programa de mejora del producto: Habilite o deshabilite la transmisión de informes de fallas y datos anónimos de telemetría a ESET.

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).

Si está creando esta política para la inscripción de iOS con ABM de Apple, vaya a **Apple Business Manager (ABM)**.

Apple Business Manager (ABM): estas configuraciones son solo para ABM. ABM

Luego de la configuración inicial, si se modifica cualquiera de estos ajustes, para aplicar los cambios, necesitará realizar un reinicio a estado de fábrica y volver a inscribir todos los dispositivos iOS afectados.

Cargar token de autorización: haga clic en el ícono de la carpeta y busque el token del servidor ABM. El token del servidor ABM es el archivo que descargó cuando creó el servidor MDM virtual en el portal ABM de Apple.

Instalación obligatoria: el usuario no podrá usar el dispositivo sin la instalación de un perfil MDM.

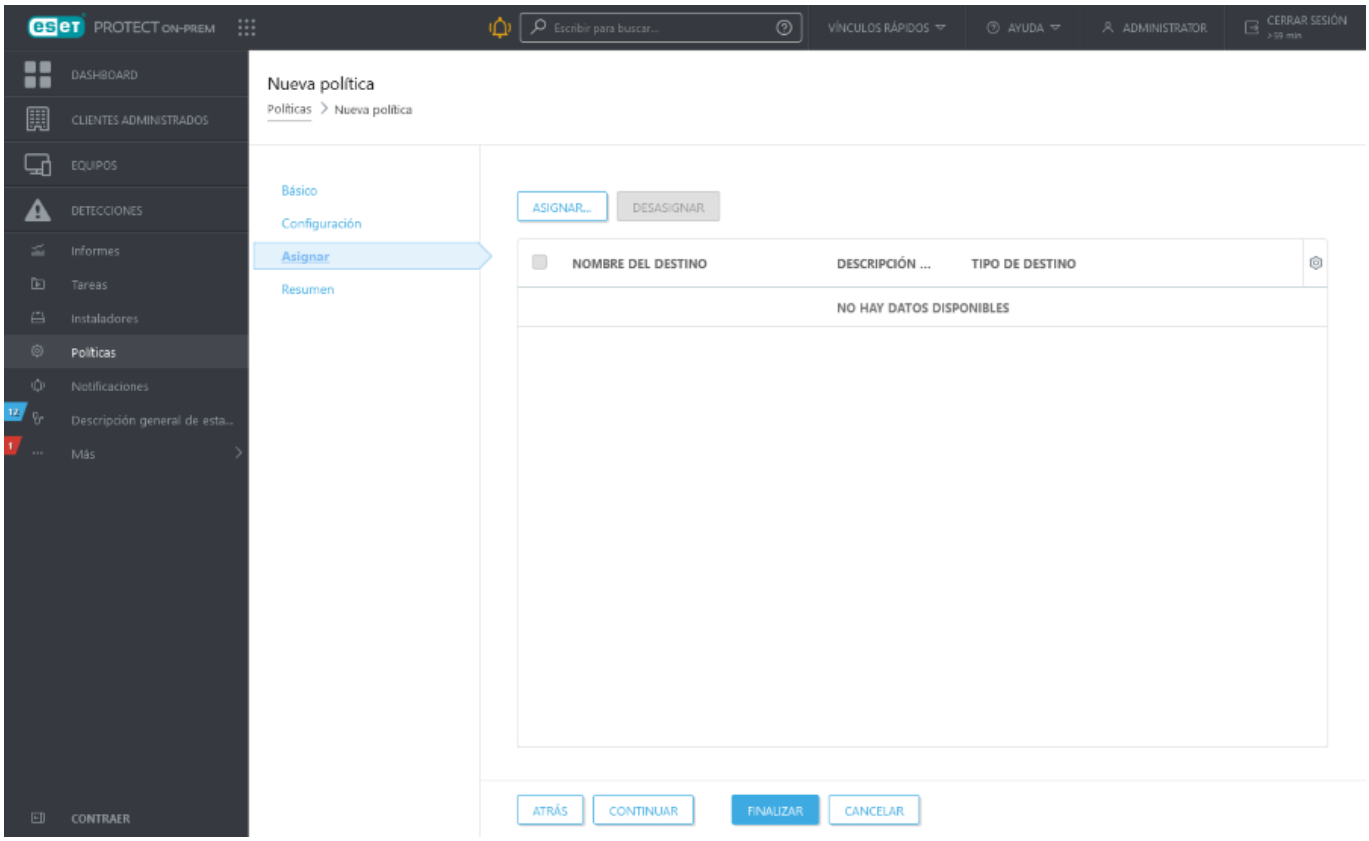
Permitir al usuario quitar el perfil MDM: el dispositivo debe estar en modo supervisado para no permitir que el usuario elimine el perfil MDM.

Solicitar ingreso al dominio: Se le solicitará al usuario ingresar credenciales de dominio válidas en el asistente de configuración del dispositivo.

Omitir elementos de configuración: esta configuración le permite elegir qué paso de la configuración inicial de iOS se omitirán. Puede obtener más información sobre cada uno de estos pasos en el articulo de la base de conocimiento de Apple.

Asignar

Seleccione el dispositivo que hospeda el servidor MDM que la política tiene como objetivo.



Haga clic en **Asignar** para visualizar todos los Grupos estáticos y dinámicos y a sus miembros. Seleccione la instancia del Conector de dispositivo móvil en la que desea aplicar la política y haga clic en **OK**.

Resumen

Revise la configuración de esta política y haga clic en **Finalizar**.

Crear una política para hacer cumplir las restricciones en iOS y añadir conexión wifi

Puede crear una política para dispositivos móviles iOS para hacer cumplir ciertas restricciones. También puede definir múltiples conexiones wifi de manera que, por ejemplo, los usuarios se conecten automáticamente a la red wifi en diferentes ubicaciones de la oficina. Lo mismo se aplica a las conexiones VPN.

Las restricciones que se pueden aplicar en los dispositivos móviles iOS se enumeran en categorías. Por ejemplo, puede desactivar FaceTime y el uso de la cámara, desactivar ciertas características de iCloud, ajustar opciones de seguridad y privacidad o deshabilitar aplicaciones seleccionadas.

> Las restricciones que se pueden aplicar o no dependen de la versión de iOS usado por los dispositivos cliente. Las versiones iOS 8.x y posteriores son compatibles.

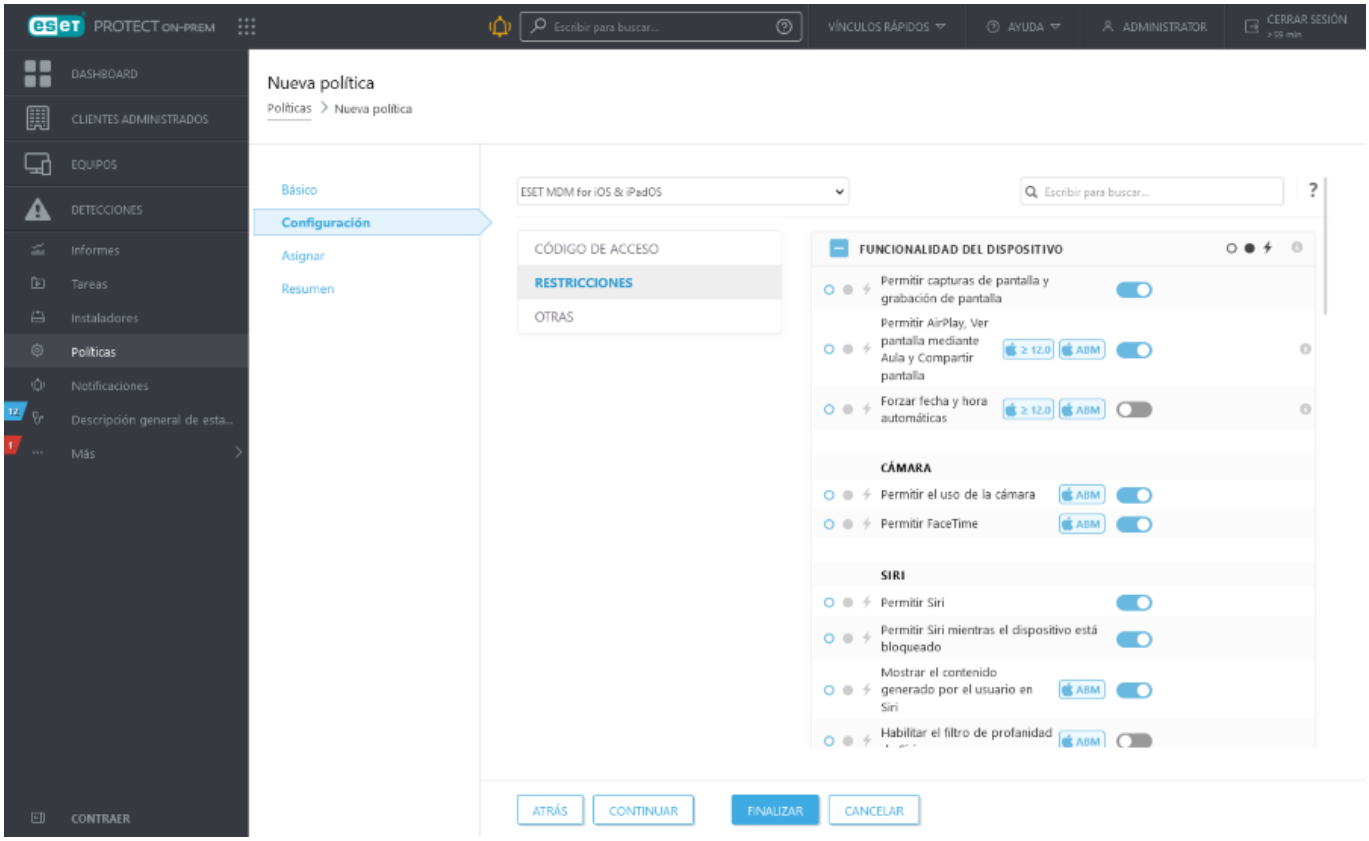
A continuación se muestra un ejemplo de cómo desactivar las aplicaciones **cámara** y **FaceTime** y agregar detalles de conexión wifi a la lista con el fin de conectar el dispositivo móvil iOS a una red wifi siempre que se detecte la red. Si usa la opción Unirse automáticamente, los dispositivos móviles iOS se conectarán a esta red por defecto. La configuración de directiva anulará la selección manual de un usuario de una red wifi.

Básica

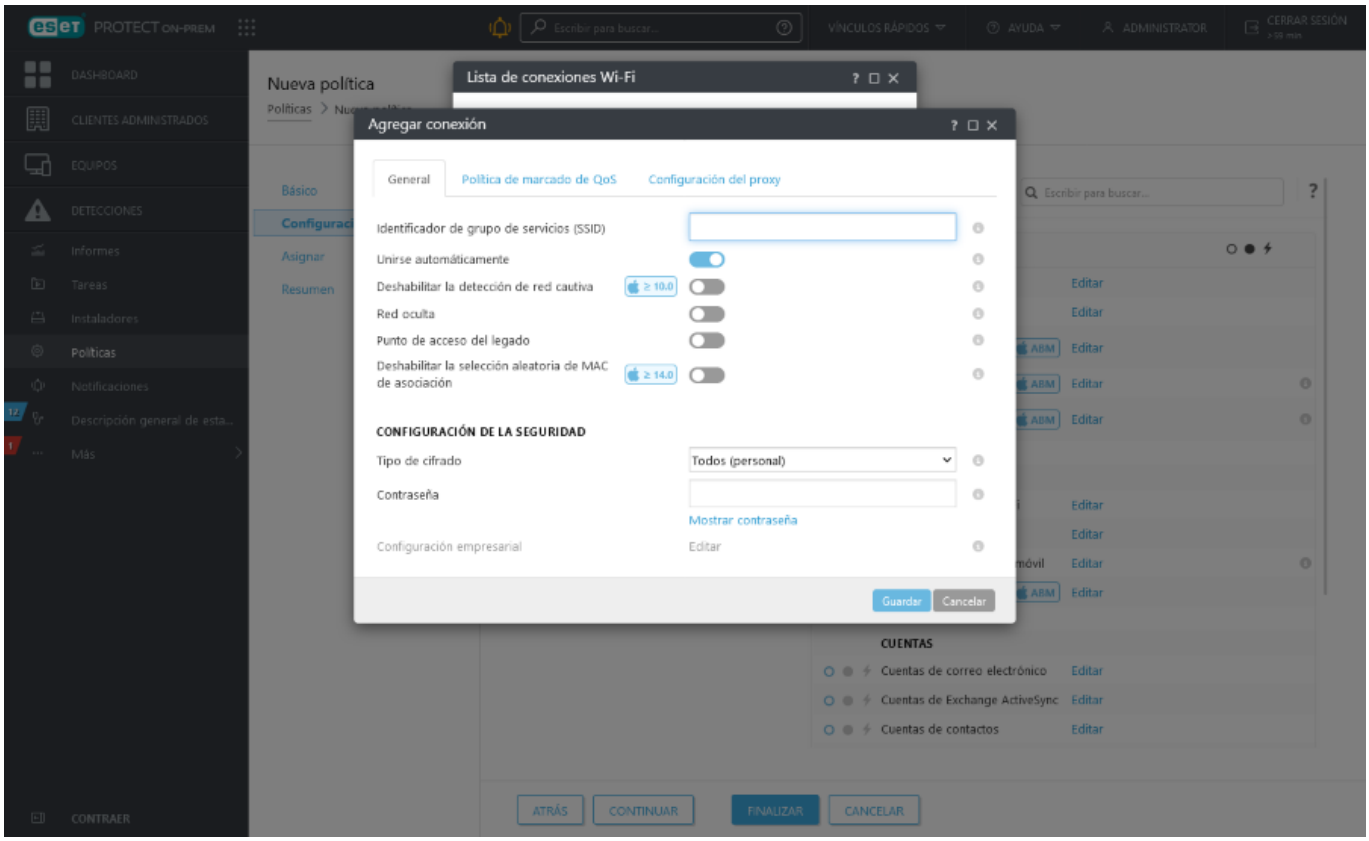
Ingrese un **Nombre** para esta política. El campo **Descripción** es opcional.

Configuración

Seleccione **ESET MDM para iOS/iPadOS**, haga clic en **Restricciones** para ver las categorías. Use el conmutador junto a **Permitir el uso de la cámara** para desactivarlo. Debido a que la cámara está desactivada, FaceTime se desactivará también de forma automática. Si solo desea desactivar FaceTime, deje la cámara habilitada y use el conmutador junto a **Permitir FaceTime** para desactivarlo.



Después de que haya configurado las **Restricciones**, haga clic en **Otros** y luego haga clic en **Editar** junto a la **Lista de conexiones wifi**. Se abrirá una ventana con la lista de las conexiones wifi. Haga clic en **Agregar** y especifique los detalles de conexión de la red wifi que desea agregar. Haga clic en **Guardar**.



- **Identificador de grupo de servicios (SSID)**: el SSID de la red wifi que se va a usar.
- **Unirse automáticamente**: opcional (habilitado por defecto), el dispositivo se unirá automáticamente a

esta red.

Configuración de la seguridad

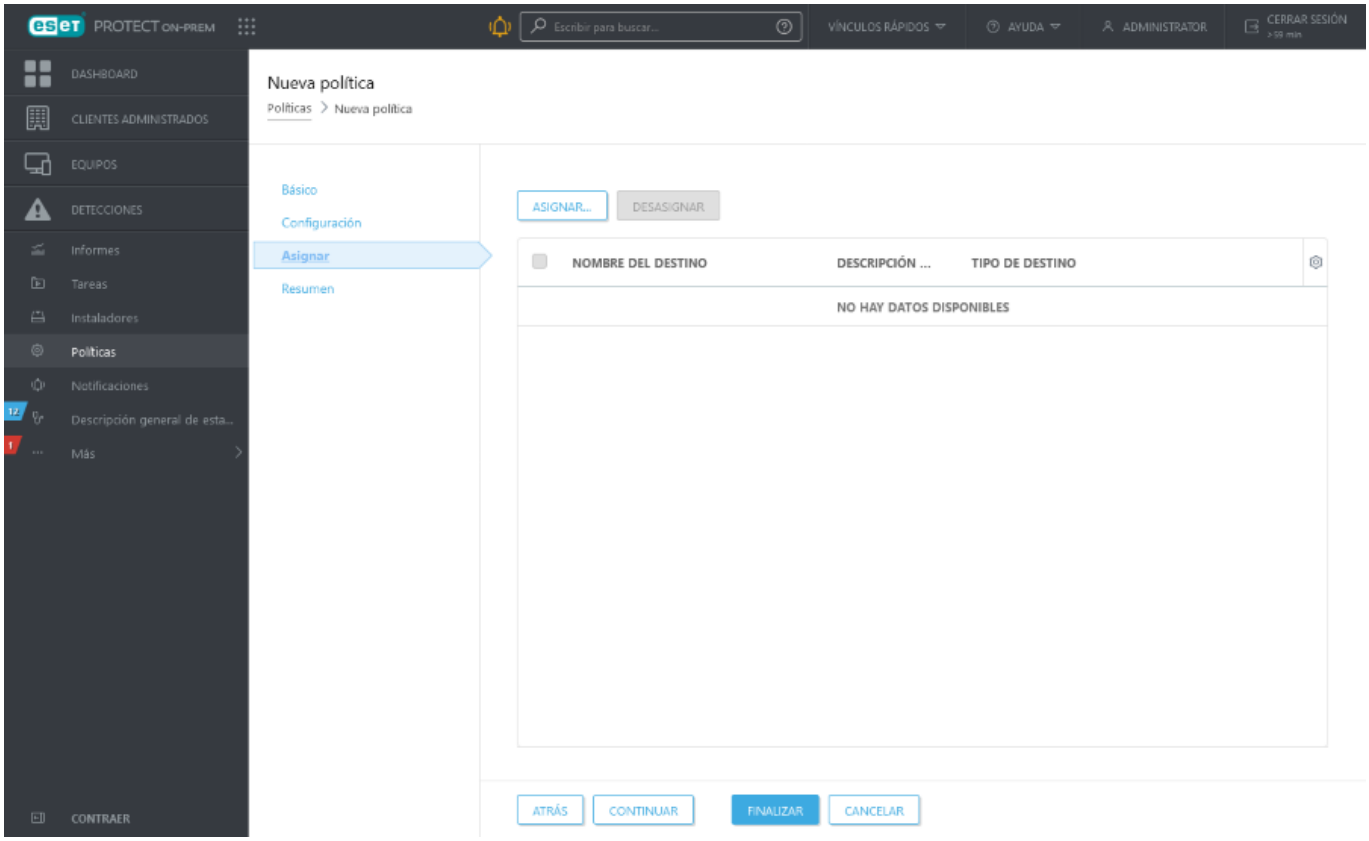
- **Tipo de cifrado**: Seleccione el cifrado adecuado de la lista desplegable, asegúrese de que este valor coincida exactamente con las capacidades de la red wifi.

- **Contraseña**: introduzca la contraseña que se usará para autenticarse al conectarse con la red wifi.

Configuración de proxy: opcional. Si la red usa un servidor proxy, especifique los valores según corresponda.

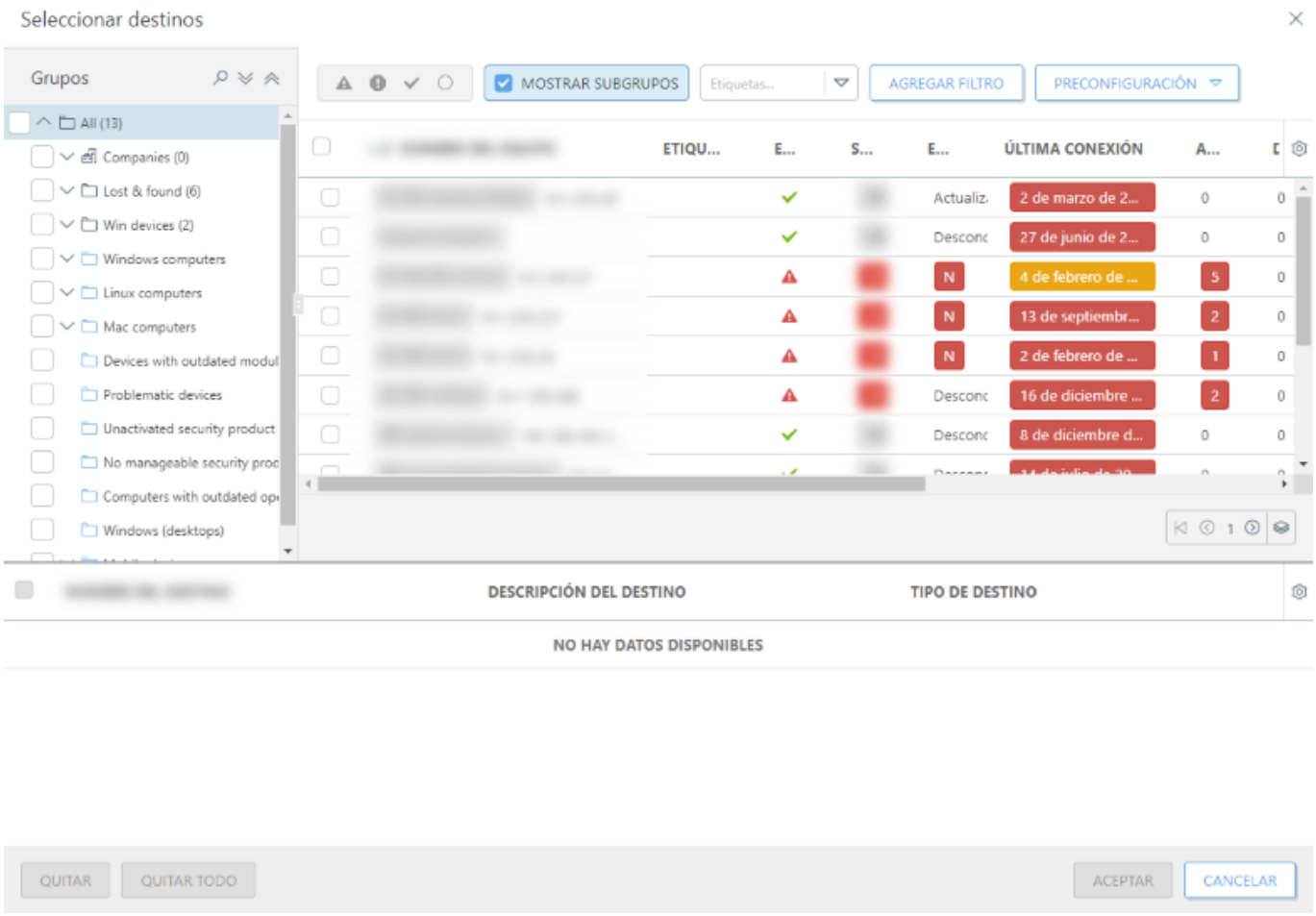
Asignar

Especifique los clientes (equipos/dispositivos móviles individuales o grupos completos) que serán los destinatarios de esta directiva.



Haga clic en **Asignar** para visualizar todos los Grupos estáticos y dinámicos y a sus miembros. Seleccione los equipos o grupos que desee y haga clic en **Aceptar**.

Para asignar todos los equipos de un grupo, asigne el grupo en lugar de los equipos individuales para evitar que la consola web se ralentice.
Si selecciona una gran cantidad de equipos, la consola web muestra una advertencia.



Resumen

Revise la configuración de esta política y haga clic en **Finalizar**. La política se aplica a los destinos después de su próxima conexión con el servidor de ESET PROTECT (en función del intervalo de conexión del agente).

Perfiles de configuración de MDM

Puede configurar el perfil para imponer políticas y restricciones en el dispositivo móvil administrado.

Nombre del perfil	Descripción breve
Código de acceso	Requiere a los usuarios finales códigos de acceso para proteger sus dispositivos cada vez que regresan del estado de reposo. Esto asegura que la información confidencial de la empresa en los dispositivos administrados permanezca protegida. Si varios perfiles requieren códigos de acceso en un solo dispositivo, se aplicará la política más restrictiva.
Restricciones	Los perfiles de restricción limitan las funciones disponibles para los usuarios en los dispositivos administrados al restringir el uso de permisos específicos relacionados con la funcionalidad, las aplicaciones, iCloud, la seguridad y la privacidad del dispositivo.
Lista de conexiones wifi	Los perfiles de Wi-Fi envían la configuración de Wi-Fi corporativa directamente a los dispositivos administrados para un acceso instantáneo.

Nombre del perfil	Descripción breve
Lista de conexiones VPN	Los perfiles VPN envían la configuración de la red privada virtual corporativa a los dispositivos corporativos para que los usuarios puedan acceder de forma segura a la infraestructura corporativa desde ubicaciones remotas. **Nombre de la conexión**: Vea el nombre de la conexión que se muestra en el dispositivo. **Tipo de conexión**: Elija el tipo de conexión habilitado por este perfil. Cada tipo de conexión permite diferentes capacidades. **Servidor**: Introduzca el nombre de host o la dirección IP del servidor al que se está conectado.
Cuentas de correo electrónico	Permite al administrador configurar cuentas de correo electrónico IMAP / POP3.
Cuentas de Exchange ActiveSync	Los perfiles de Exchange ActiveSync permiten a los usuarios finales acceder a la infraestructura de correo electrónico corporativa basada en la tecnología push. Tenga en cuenta que hay campos de valores de consulta y opciones pre-llenados que sólo se aplican a iOS 5+.
CalDAV - Cuentas de calendario	CalDAV proporciona opciones de configuración para permitir a los usuarios finales sincronizar de forma inalámbrica con el servidor CalDAV de la empresa.
CardDAV - Cuentas de contactos	Esta sección permite la configuración específica de los servicios CardDAV.
Cuentas de calendario suscritas	Los calendarios suscritos proporcionan configuraciones de calendario.

Control web para Android

Use ESET Endpoint Security for Android para regular el acceso a sitios web desde sus dispositivos Android administrados. El control web puede regular el acceso a sitios web que puedan vulnerar los derechos de propiedad intelectual y proteger a su empresa del riesgo de responsabilidad legal. El objetivo es impedir que los empleados accedan a páginas con contenido inapropiado o perjudicial, así como páginas que puedan afectar negativamente a la productividad.

> El control web para Android es compatible con ESET Endpoint Security para Android versión 3.0 y posteriores.

El control web está desactivado de forma predeterminada. Para activarla, deberá crear una nueva política:

1. Haga clic en **Políticas** > **Nueva política**.
2. En la ventana **Nueva política**, vaya a **Configuración** y seleccione **ESET Endpoint Security for Android**.
3. En la sección **Protección web** de la política, expanda Control web y habilite el botón de alternancia **Control web**.
4. Enlaces o categorías específicos de las listas blanca y negra.

Reglas de control web

Use la política control web para especificar una lista de URL para tres categorías distintas:

- **Lista negra**: bloquea la URL sin opción ni acceso

- **Lista blanca**: permite acceso a la URL
- **Advertencia**: advierte al usuario sobre la URL, pero ofrece una opción de acceso

Cada una de estas secciones puede administrarse con las siguientes acciones:

- **Agregar**: agrega un registro nuevo con una dirección URL concreta
- **Editar**: modifica una dirección URL existente
- **Quitar**: elimina un informe existente de una dirección URL
- **Importar**: importa una lista de direcciones URL nuevas en la categoría
- **Exportar**: exporta una lista de direcciones URL de la categoría seleccionada

> En el caso de reglas que controlen el acceso a un sitio web determinado, ingrese la URL completa en el campo **URL**.
> Símbolos especiales * (asterisco) y ? (signo de interrogación) en el campo URL.
> Al agregar una dirección de dominio, todo el contenido ubicado en este dominio y todos los subdominios (por ejemplo, `subdomain.domain.com`) se bloqueará o permitirá en función de la acción elegida.

Otra opción es permitir o bloquear un conjunto completo de URL en función de su categoría en **Reglas de categoría**.

En la ventana **Reglas de categoría**, seleccione una acción para una categoría específica de URL y especifique qué subcategoría se debe ver afectada:

- **Permitir**: permite el acceso a la URL desde una categoría seleccionada
- **Bloquear**: bloquea el acceso a la URL desde una categoría seleccionada
- **Advertir**: advierte al usuario sobre la URL de una categoría seleccionada

Administración de actualizaciones del sistema operativo

ESET Endpoint Security para Android permite a un administrador administrar las actualizaciones del sistema operativo Android en dispositivos Android administrados.

> Esta funcionalidad requiere ESET Endpoint Security for Android versión 3.0, Android versión 8.x y posteriores, y el dispositivo Android debe estar inscrito en modo Propietario del dispositivo.

Para administrar las actualizaciones del sistema operativo en dispositivos administrados, cree una nueva política:

1. Haga clic en **Políticas** > **Nueva política**.
2. En **Configuración**, seleccione **ESET Endpoint Security for Android**.
3. En **Seguridad del dispositivo**, seleccione **Seguridad del dispositivo** y active la configuración **Habilitar seguridad del dispositivo**.

4. Para activar la función de administración del sistema operativo, diríjase a **Administración de actualizaciones del sistema** y habilite **Administrar actualizaciones del sistema**.

Desde esta sección puede definir las diferentes reglas del sistema operativo Android actualizadas en sus dispositivos Android administrados:

- **Política de actualización del sistema**:
  - **Automático**: la actualización del sistema operativo Android se ejecutará sin demora.
  - **Con ventana**: la actualización del sistema operativo Android solo se ejecutará durante una ventana de mantenimiento específica en la configuración **Ventana de mantenimiento diario**.
  - **Pospuesto durante 30 días**: la actualización del sistema operativo Android se ejecutará 30 días después de su fecha de lanzamiento.
- **Periodo de mantenimiento diario**: defina una hora específica para que la actualización del sistema operativo se ejecute en el dispositivo Android administrado.
- **Periodos de bloqueo**: especifique varios periodos de tiempo en los que no se puedan actualizar los dispositivos.

Resolución de problemas de MDM

Configuración y archivos de registro de MDMCore

Consulte también los archivos de registro de otros componentes de ESET PROTECT.

Ubicación	Detalles del archivo
Windows: *%ProgramData%\ESET\RemoteAdministrator\MDMCore\Configuration* Linux: */etc/opt/eset/RemoteAdministrator/MDMCore*	• *startupconfiguration.ini* (Windows), *startupconfiguration.ini* (Linux): información de conexión de la base de datos. • *loggerLevel.cfg*: una sola línea que especifica el nivel de registro de anulación para el registro. Este archivo tiene prioridad sobre la configuración de cualquier política (y se puede usar en aquellos casos en los que no puede ofrecerse la política). Si se reconoce, la línea "Setting log level from loggerLevel.cfg override file to XYZ" se genera en el registro de seguimiento (nivel de información). Valores reconocidos: all, trace, debug, information, warning, error, critical, fatal. Cuando se configura en all, también registra toda la comunicación con los teléfonos. • *shouldLogPhoneComm.cfg*: una sola línea que especifica si la comunicación con los teléfonos debe iniciarse en un archivo de registro independiente. Valores reconocidos: 1, true, log. • *skipPnsCertCheck.cfg*: una sola línea que especifica si se debe validar el certificado del servicio PNS.
Windows: *%ProgramData%\ESET\RemoteAdministrator\MDMCore\Data\MultiAgent* Linux: */var/opt/eset/RemoteAdministrator/MDMCore/MultiAgent*	Registros de seguimiento de agentes individuales en subcarpetas por agente.
Windows: *%ProgramData%\ESET\RemoteAdministrator\MDMCore\Dumps* Linux: */var/opt/eset/RemoteAdministrator/MDMCore/Dumps*	Bloqueos que aún no se han enviado al servicio de generación de informes de fallas de ESET.
Windows: *%ProgramData%\ESET\RemoteAdministrator\MDMCore\Logs* Linux: */var/log/eset/RemoteAdministrator/MDMCore*	• *trace.log, trace.log.<N>.gz*: el registro de seguimiento de MDMCore. Los archivos comprimido mediante gzip con número son contenidos antiguos del registro.
Windows: *%ProgramData%\ESET\RemoteAdministrator\MDMCore\Logs\Proxy* Linux: */var/log/eset/RemoteAdministrator/MDMCore/Proxy*	• *trace.log, trace.log.<N>.gz*: el registro de seguimiento del componente MultiProxy de MDMCore. Los archivos comprimido mediante gzip con número son contenidos antiguos del registro.
Windows: *%ProgramData%\ESET\RemoteAdministrator\MDMCore\Modules* Linux: */var/opt/eset/RemoteAdministrator/MDMCore/Modules*	• *em*.dat*: motor de configuración y módulos del cargador.
Windows: *%ProgramFiles%\ESET\RemoteAdministrator\MDMCore* Linux: */opt/eset/RemoteAdministrator/MDMCore*	Todos los archivos ejecutables necesarios para MDMCore.

Mensajes de error de MDM

El token de inscripción ya está en uso o no es válido.

Es posible que esté intentando la reinscripción con un token de inscripción antiguo. Cree un nuevo token de

reinscripción en la Consola web y utilice ese. También es posible que esté intentando una segunda reinscripción poco tiempo después de la primera. Verifique que el token de reinscripción sea diferente del primero. Si no lo es, espere unos minutos y vuelva a intentar generar un nuevo token de reinscripción.

Falló la validación del certificado de servicio

Este mensaje de error indica que existe un problema con el certificado de servicio APNS o GCM. El mismo se anuncia en la consola Web de ESET PROTECT como una de las siguientes advertencias en las alertas de núcleo MDM:

- **Falló la validación del certificado de servicio de FCM** (0x0000000100001002)
- **Falló la validación del certificado de servicio de APNS** (0x0000000100001000)
- **Falló la validación del certificado de servicio de retroalimentación de APNS** (0x0000000100001004)

Asegúrese de contar con la autoridad de certificado correcta disponible en el sistema:

- Autoridad de certificado APNS: **Autoridad de certificado de Entrust**, necesita validar el certificado desde gateway.push.apple.com:2195;
- Autoridad de certificado de retroalimentación de APNS: **Autoridad de certificado de Entrust**, necesita validar el certificado desde feedback.push.apple.com:2196;
- Autoridad de certificado FCM: **GeoTrust Global CA**, necesita validar el certificado desde android.googleapis.com:443.

Se debe incluir a la autoridad de certificado deseada en el almacén de certificados en el equipo host de MDM. En un sistema Windows, puede buscar "Administrar certificados raíz de confianza". E un sistema Linux, la ubicación del certificado depende de la distribución que utilice. Algunos ejemplos de destinos de almacenes de certificados incluyen:

- en Debian, CentOS: */usr/lib/ssl/cert.pem*, */usr/lib/ssl/certs*;
- en Red Hat: */usr/share/ssl/cert.pem*, */usr/share/ssl/certs*;
- comando `openssl version -d` por lo general devuelve la ruta deseada.

Si la autoridad de certificado deseada no está instalada en el sistema en el cual se ejecuta el núcleo MDM, instálela. Luego de la instalación, reinicie el servicio MDC de ESET PROTECT.

Tenga cuidado, la validación de certificados es una característica de seguridad; por lo tanto, si la advertencia ocurre en la consola Web, también puede indicar una amenaza a la seguridad.

Herramienta de migración de administración de dispositivos móviles

Los siguientes pasos le ayudarán a migrar dispositivos móviles de ESET PROTECT On-Prem al entorno ESET PROTECT:

Requisitos previos

- Entorno de trabajo ESET PROTECT On-Prem con el componente Administración de dispositivos móviles
- Entorno de trabajo ESET PROTECT
- Cuenta de ESET PROTECT con privilegios de **superusuario**.

Limitaciones

- Esta migración solo está disponible para dispositivos Android
- Esta migración requiere ESET Endpoint Security para Android versiones 3.5+ y ESET PROTECT On-Prem 10.0+
- La migración de dispositivos iOS administrados requiere la desinscripción manual en ESET PROTECT On-Prem y la inscripción en ESET PROTECT

1. Abra la consola web de ESET PROTECT.

2. Haga clic en **Más** > **Configuración** > **Migración de dispositivos móviles ESET PROTECT On-Prem**.

3. Seleccione la **licencia** que desee utilizar para la activación de los dispositivos móviles administrados una vez que finalice la migración.

4. Seleccione el **grupo principal** para la colocación inicial de los dispositivos tras la migración.

5. **Límite de uso del token**: puede limitar la cantidad de dispositivos que se pueden migrar con el token de migración.

Si administra una gran cantidad de dispositivos móviles, le recomendamos que pruebe primero el proceso de migración con una cantidad reducida para supervisar que la migración no tenga ningún problema. A continuación, podrá realizar un seguimiento de la migración del resto de los dispositivos móviles administrados.

6. Seleccione **Generar token** para generar un token de migración con los parámetros establecidos para el proceso de migración.

El token generado tiene una validez de 14 días y solo está disponible mientras permanece en la página. No cierre ni actualice la página antes de copiar primero el token.

7. El token de migración aparece como una cadena de caracteres en el campo que aparece a continuación. Cópielo en un editor de texto.

8. Abra la consola web de ESET PROTECT On-Prem.

9. Haga clic en **Políticas** > **Nueva política**.

10. En la sección **Básico**, complete el **nombre** y la **descripción** de la política. Esta política migrará los dispositivos móviles administrados actualmente del entorno local al entorno en la nube.

11. En la sección **Configuración**, seleccione **ESET Mobile Device Connector**.

12. En **General** > **Migración de ESET PROTECT**, pegue el token de migración en el campo de texto **Token de migración**.

13. En la sección **Asignar**, seleccione el dispositivo en el que se ejecuta Mobile Device Connector.

14. Una vez aplicada la política, se iniciará el proceso de migración.

El servidor aplicará la política de migración a todos los dispositivos móviles administrados que se conecten desde este momento. Asegúrese de que todos sus dispositivos móviles administrados puedan conectarse al servidor mientras el token de migración sea válido (durante los próximos 14 días). Si un dispositivo móvil administrado no se conecta al servidor en este período, no se migrará y tendrá que repetir el procedimiento de migración.

15. Puede supervisar el proceso de migración desde la consola web ESET PROTECT. Una vez migrado el dispositivo móvil, se conectará a ESET PROTECT y estará visible en la sección **Equipos** de la consola web ESET PROTECT.

16. Tras migrar correctamente el dispositivo al entorno ESET PROTECT, puede quitarlo de la consola web ESET PROTECT On-Prem de forma segura.

17. Tras migrar correctamente todos los dispositivos móviles al entorno ESET PROTECT, puede retirar de forma segura el componente Administración de dispositivos móviles.

ESET PROTECT On-Prem para proveedores de servicios administrados

Qué es un MSP

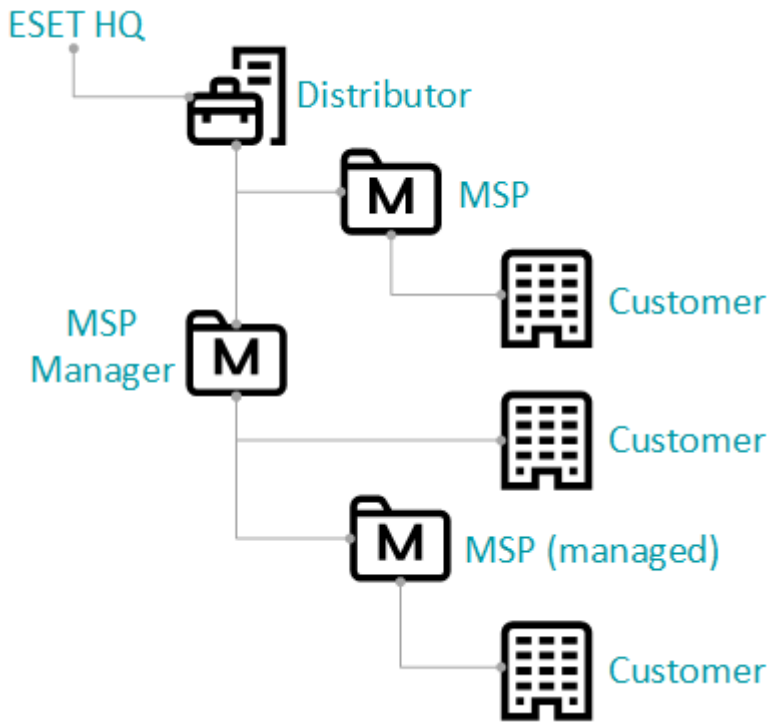
La abreviatura MSP significa "proveedor de servicios administrados". Los usuarios de MSP suelen prestar servicios de TI a sus clientes, por ejemplo, la administración de productos de seguridad (por ejemplo, ESET Endpoint Antivirus).

- Los usuarios de MSP tienen distintos requisitos y maneras de usar ESET PROTECT On-Prem que, por ejemplo, los usuarios empresariales o SMB (negocios pequeños y medianos). Vea los escenarios de instalación recomendados para MSP.

- Para obtener más información sobre el programa MSP de ESET, póngase en contacto con su socio de ESET local o visite la página del Programa de proveedores de servicios administrados de ESET.

Estructura de las entidades de los MSP

ESET PROTECT On-Prem sincroniza su estructura ESET MSP Administrator con el Árbol del grupo estático en **Equipos** en la consola web.



- **Distribuidor** : un distribuidor es un socio de ESET y un socio administrador de MSP o MSP.

- **Administrador de MSP**: administra varias empresas de MSP. Un administrador de MSP también puede tener clientes directos.

- **MSP**: audiencia de destino para esta guía. Un MSP brinda servicios a sus clientes. Por ejemplo, los MSP: administran en forma remota los equipos de los clientes e instalan y administran productos de ESET.

- **MSP administrado** : es muy similar a un MSP. Sin embargo, el MSP administrado se encuentra bajo la administración de un administrador de MSP.

- **Cliente:** el usuario final de las licencias de productos de ESET. El cliente no debería interactuar con productos ESET. El cliente puede tener diferentes estados marcados por un ícono:

  - o : el cliente aún no se ha configurado.

  - o : el cliente se ha configurado o se ha omitido la configuración del cliente.

  - o : se ha eliminado el cliente.

Después de sincronizar la cuenta MSP, el usuario MSP puede ver la lista de clientes administrados en la sección Clientes administrados del menú principal de ESET PROTECT On-Prem.

Detalles específicos sobre el entorno de MSP

El modelo de negocios de MSP utiliza una configuración de infraestructura diferente en comparación con una empresa o SMB. En el entorno de MSP, los clientes suelen estar ubicados fuera de la red de la empresa del MSP. El servidor de ESET PROTECT en sí puede estar alojado con frecuencia fuera de la empresa del MSP, también. Los agentes de ESET Management precisan tener conectividad directa al servidor de ESET PROTECT a través de Internet pública. Las configuraciones recomendadas del servidor ESET PROTECT para MSP son:

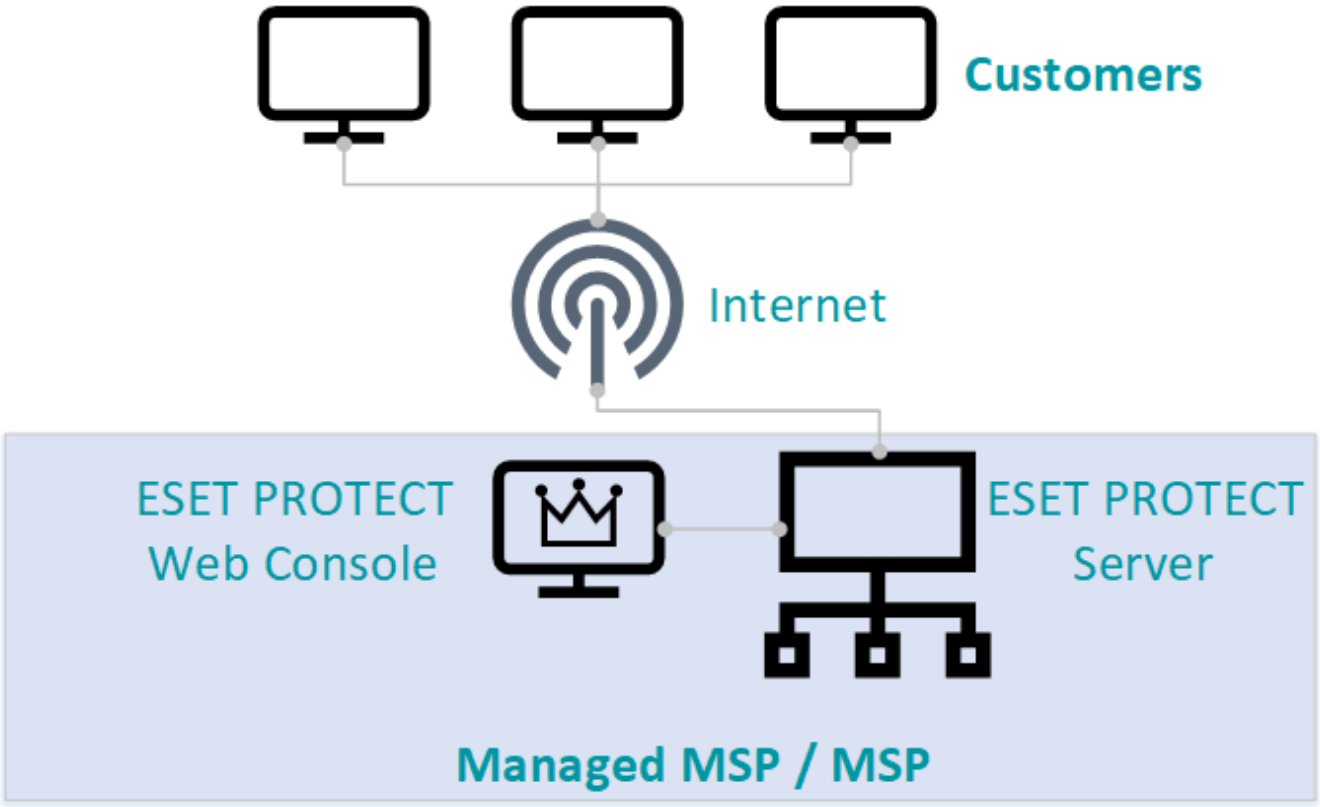
- Alojado en una nube pública.

• Alojado en una nube privada del MSP. (Debe abrir ciertos puertos para que ESET PROTECT On-Prem pueda verse desde Internet)

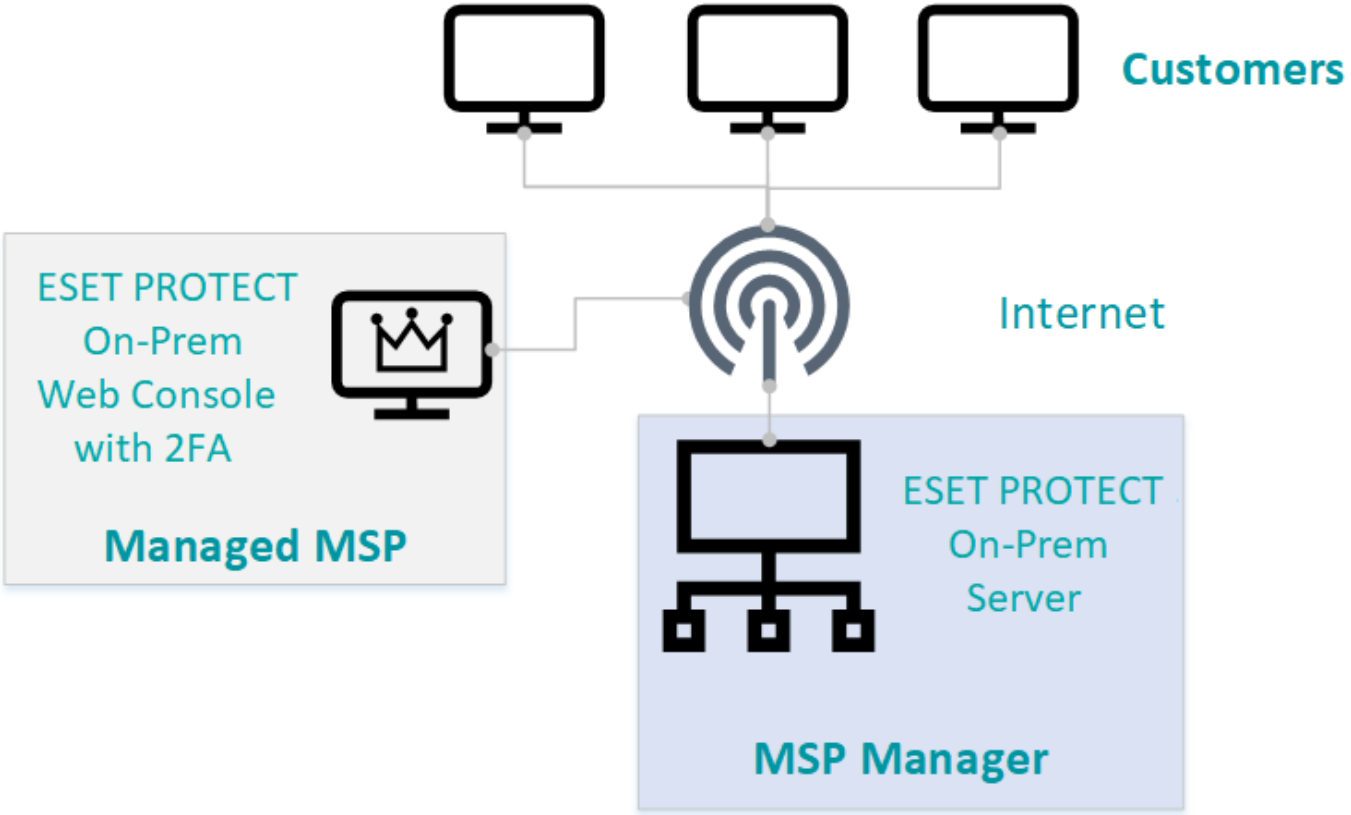
• Alojado en una red privada del MSP. (Utilice el proxy HTTP para reenviar conexiones por Internet, en caso de que el servidor no sea visible en forma directa).

Configuración básica

• **Configuración centralizada**: los clientes acceden al servidor de ESET PROTECT a través de Internet. Es posible acceder a la consola web de ESET PROTECT únicamente desde la red de la empresa del MSP.



• **Configuración distribuida**: los clientes acceden al servidor de ESET PROTECT a través de Internet. Es posible acceder a la consola web de ESET PROTECT del MSP a través de Internet. Si configura la consola web para que pueda accederse a ella desde Internet, asegúrese de habilitar la autenticación de dos factores (2FA).



Funciones de ESET PROTECT On-Prem para usuarios de MSP

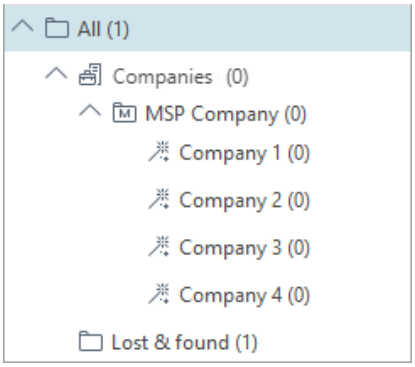
ESET PROTECT On-Prem ofrece un conjunto de funciones orientadas a usuarios de MSP. Todas las funciones relacionadas con MSP se habilitan luego de importar una cuenta EMA 2 a ESET PROTECT On-Prem.

Asistente de configuración de cliente

La función clave de MSP en ESET PROTECT On-Prem . es la configuración de cliente de MSP. Esta función lo ayuda a crear usuarios y un instalador de agente ESET Management personalizado para su cliente.

Árbol de MSP

Luego de importar la cuenta EMA 2, ESET PROTECT On-Prem se sincroniza con el portal MSP de ESET (EMA 2) y crea el árbol de MSP. El árbol de MSP es una estructura ubicada en el menú Equipos, que representa la estructura de las compañías en su cuenta EMA 2. Los elementos del árbol de MSP usan íconos diferentes que los dispositivos y grupos estándares de ESET PROTECT On-Prem. No puede modificar la estructura del árbol MSP en la consola web. Solo después de quitar la cuenta EMA 2 en Administración de licencias, puede comenzar a editar y quitar clientes del árbol. Al suspender una empresa en EMA 2, no se quita a la compañía del árbol de MSP en ESET PROTECT On-Prem.

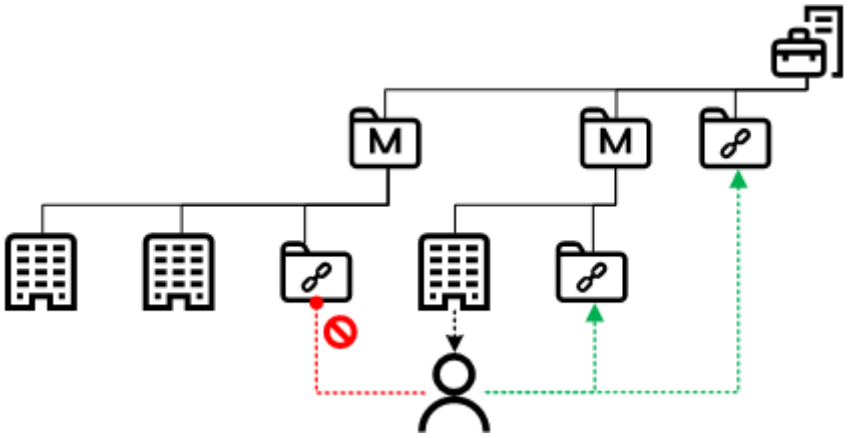


Grupo de objetos compartidos

Luego de sincronizar la cuenta de MSP, ESET PROTECT On-Prem crea el árbol de MSP. Hay un grupo de acceso **Objetos compartidos** para cada MSP y administrador de MSP. El grupo de acceso configura el grupo estático del objeto y el acceso al objeto en función de los derechos de acceso del usuario. No puede almacenar equipos en

Objetos compartidos. Los **Objetos compartidos** no están visibles en **Grupos** en **Equipos**. Los MSP pueden compartir objetos como políticas y tareas a través del grupo de acceso **Objetos compartidos**.

Cada usuario de MSP que se crea con el asistente de configuración de la compañía tiene acceso de lectura y escritura a todos los grupos de **Objetos compartidos** ubicados por encima del usuario. Puede inspeccionar los Conjuntos de permisos asignados al usuario para ver la lista de grupos de acceso. Los usuarios pueden acceder únicamente a los grupos de objetos compartidos y no a los grupos de administradores de MSP paralelos.



Clientes administrados

Después de sincronizar la cuenta MSP, el usuario MSP puede ver la lista de clientes administrados en la sección Clientes administrados del menú principal de ESET PROTECT On-Prem.

ESET PROTECT certificados y MSP

Cuando importa la cuenta EMA 2 en ESET PROTECT On-Prem, ESET PROTECT Server crea una nueva Autoridad de certificación (CA) de MSP. La CA de MSP se almacena en el grupo estático **Objetos compartidos** debajo del grupo raíz de MSP. Hay una sola CA de MSP, incluso si importa varias cuentas. Si quita la CA de MSP, ESET PROTECT On-Prem crea una nueva CA de MSP luego de la siguiente sincronización con los servidores de la licencia. La sincronización tiene lugar en forma automática una vez por día.

ESET PROTECT On-Prem crea un nuevo certificado de agente de pares luego de que se configura una compañía por medio del asistente de configuración de cliente. La CA de MSP firma estos certificados de pares. Cada certificado está etiquetado con el nombre de la compañía. Al crear un certificado individual para cada compañía, se mejora la seguridad general.

Si quita una CA, todos los equipos que usan certificados firmados por la CA no deberían poder conectarse a ESET PROTECT Server. Sería necesario realizar una reinstalación manual del agente de ESET Management.

MSP en la Información general de estado

Puede obtener acceso al mosaico del nuevo MSP en Información general de estado luego de importar la cuenta EMA 2. En el mosaico MSP, se muestra información básica sobre la cuenta.

Proceso de instalación de MSP

Si no tiene ESET PROTECT On-Prem instalado, le recomendamos usar el instalador Todo en uno de Windows y seguir la guía de instalación, mientras se toman en cuenta las siguientes recomendaciones:

• No escoja la opción de instalar **ESET Bridge** (proxy HTTP). Sus clientes se contactarán con los servidores de ESET en forma directa (para descargas, activaciones, actualizaciones). Los clientes más grandes pueden tener su propia solución local de proxy HTTP. Puede configurarlo más adelante.

• ESET PROTECT Server debe tener conectividad también al servidor de ESET (para sincronizarse con EMA 2, descargar actualizaciones, y otros asuntos).

Luego de instalar ESET PROTECT Server, siga el proceso que se detalla abajo:

1.Asegúrese de tener una cuenta EMA 2 elegible.

2.Prepare un cliente con, al menos, una licencia. También puede usar un cliente existente.

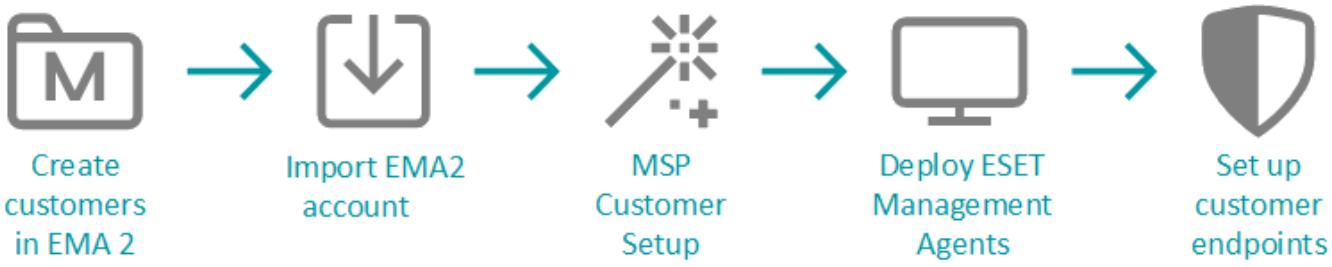
3.Importe su cuenta EMA 2 en ESET PROTECT On-Prem.

4.Complete la configuración de cliente de MSP. Cuando se le indique, seleccione el instalador **solo Agente**.

5.Distribuya e instale el instalador de agente ESET Management a nivel local o en forma remota.

6.Instale los productos de seguridad ESET y configure las políticas.

En el esquema de abajo, se muestra una descripción de alto nivel de un proceso de inscripción de cliente de MSP.



Instalación local de agente

Instalación local de instalador de solo agente

El **instalador solo agente** es un script (*.bat* para Windows y *.sh* para Linux y macOS) que incluye toda la información necesaria para que un equipo cliente descargue e instale el agente ESET Management. Si instala en un equipo Linux, asegúrese de que este cumpla con los requisitos previos.

Puede ejecutar el instalador a nivel local o a partir de un medio extraíble (por ejemplo, una unidad flash USB).

El equipo cliente necesita una conexión a Internet para descargar el paquete de instalación del agente y conectarse al ESET PROTECT On-Prem.

Puede editar el script en forma manual para ajustar ciertas configuraciones, en caso de ser necesario. Lo recomendamos solo para usuarios avanzados.

Instalación local del instalador todo en uno

El instalador todo en uno contiene el producto de seguridad de ESET que usted elija y un instalador de agente ESET Management preconfigurado.

Consulte el manual del instalador para obtener instrucciones específicas.

Instalación remota de agente

Instalación remota del instalador de solo agente

El **instalador solo agente** es un script (*.bat* para Windows y *.sh* para Linux y macOS) que incluye toda la información necesaria para que un equipo cliente descargue e instale el agente ESET Management. Si instala en un equipo Linux, asegúrese de que este cumpla con los requisitos previos. Puede distribuir el instalador por correo electrónico y dejar que el usuario lo instale. Si está disponible, utilice una herramienta de administración remota de terceros para distribuir y ejecutar el script.

El equipo cliente necesita una conexión a Internet para descargar el paquete de instalación del agente y conectarse al ESET PROTECT On-Prem.

Instalación remota del instalador todo en uno

El instalador todo en uno puede instalarse en forma remota, dentro de una red local, mediante el uso de ESET Remote Deployment Tool. Consulte la documentación de ESET Remote Deployment Tool para obtener instrucciones detalladas.

Licencias MSP

Cuentas elegibles

Para habilitar las funciones de MSP en ESET PROTECT On-Prem debe importar su cuenta de MSP en la administración de licencias de ESET PROTECT On-Prem.

- Puede importar los siguientes tipos de cuentas EMA 2: MSP, MSP administrado y Administrador de MSP.
- Todas las cuentas deben tener, como mínimo, permiso de lectura respecto de, al menos, una compañía, que puede ser su compañía matriz o un cliente.
- No es necesario tener acceso a la compañía matriz.
- No puede importarse la cuenta del distribuidor.

Información sobre licencias y compañías

- Las licencias que se importan desde la cuenta de MSP se encuentran etiquetadas con el nombre de la compañía. Si se le cambia el nombre a la compañía más adelante, no se les modifica el nombre a las etiquetas en forma automática. Puede realizar la edición en forma manual.
- Todas las licencias se importan en un modo compatible con el modelo de seguridad de ESET PROTECT On-Prem. Cada usuario que se crea con la configuración de cliente de MSP solo puede ver y usar sus licencias.
- Si una compañía incluida en su estructura de MSP no tiene licencia en el momento de la sincronización, dicha compañía se sincroniza únicamente en el árbol de MSP del equipo, y no en el árbol de MSP ubicado

dentro de la Administración de licencias.

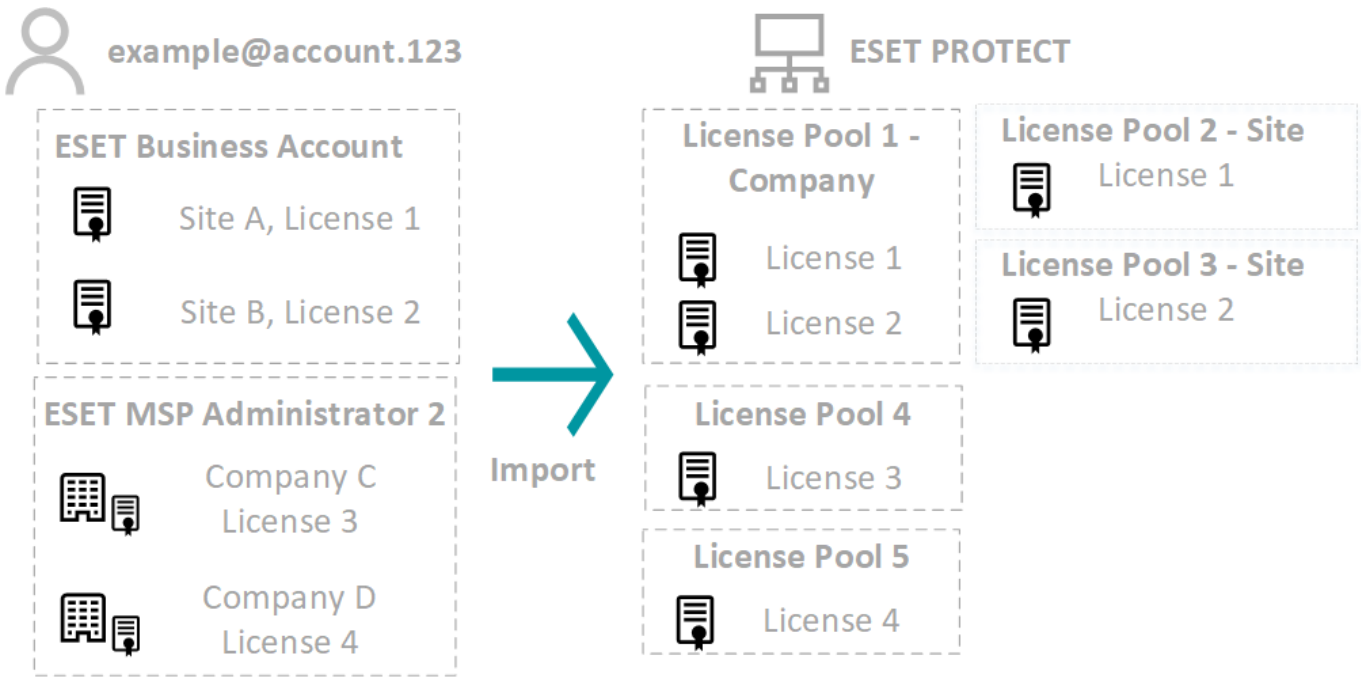
• Si agrega una nueva compañía en ESET MSP Administrator 2, ESET PROTECT On-Prem agrega a la compañía al árbol de MSP con posterioridad a la sincronización de la siguiente licencia.

• Las licencias de ESET MSP Administrator 2 se dividen en un conjunto para cada compañía. No puede mover una licencia fuera del grupo.

• Puede buscar los nombres de las compañías y los sitios en la columna **Usuario de licencia** en Administración de licencias. Puede usar los datos de **Usuario de licencia** al crear un informe.

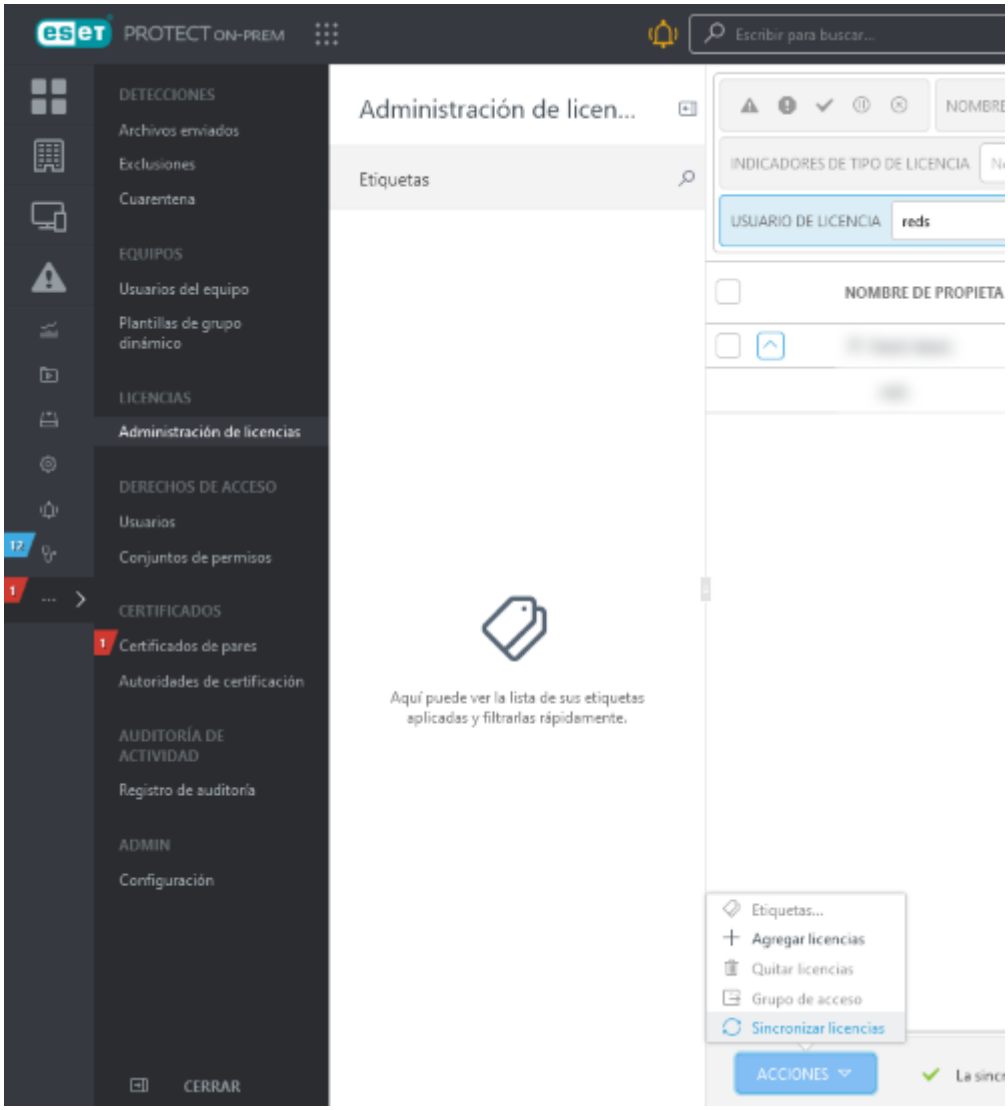
• Si tiene licencias tanto en ESET Business Account como en ESET MSP Administrator 2 con las mismas credenciales, ESET PROTECT On-Prem sincroniza todas las licencias de ambas cuentas. Todas las licencias ESET Business Account se guardan en múltiples conjuntos de licencias. Las licencias de ESET MSP Administrator 2 se dividen en un conjunto para cada compañía. Desde la versión 8.0, ESET PROTECT On-Prem es compatible con los sitios de ESET Business Account para dividir licencias.

• Al quitar cualquier grupo de licencia, se quitan de manera automática todos los otros grupos de licencia asociados con la misma cuenta. Obtenga más información sobre cómo quitar una compañía.



Sincronización a pedido

ESET PROTECT On-Prem se sincroniza con los servidores de licencias una vez por día. Si realizó cambios en su cuenta de MSP y quiere actualizar la pantalla de la licencia y el árbol de MSP, vaya a **Administración de licencias** > **Acciones** y haga clic en **Sincronizar licencias**.

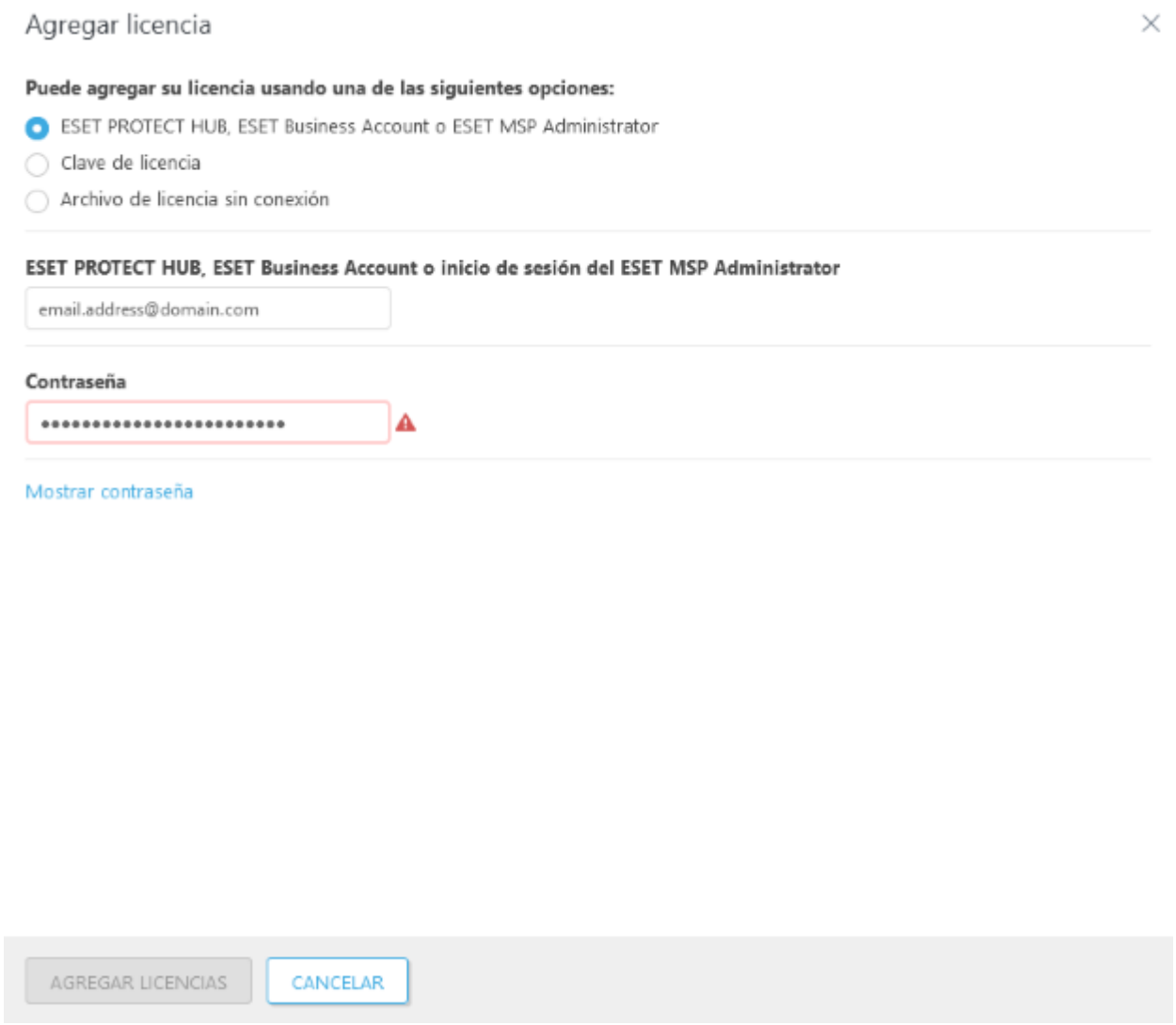


Importar una cuenta de MSP

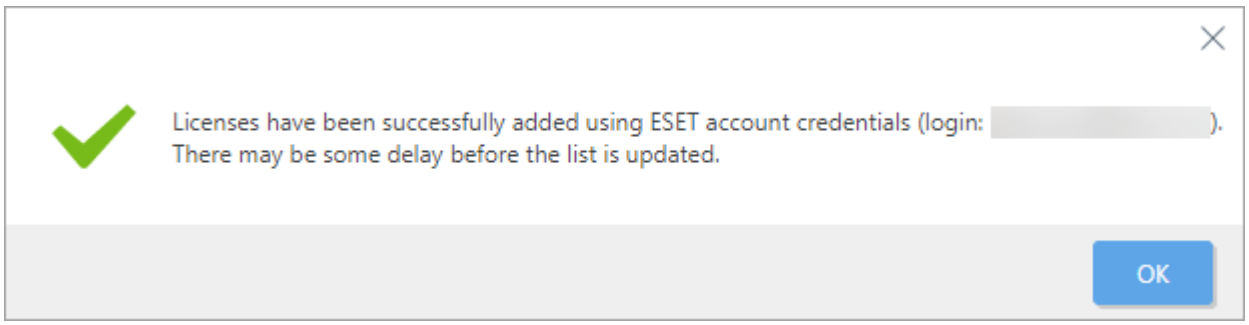
1. Inicie sesión en la consola web y vaya a **Más** > **Administración de licencias**.

2. Haga clic en **Acciones** > **Agregar licencias**.

3. Seleccione la opción **ESET PROTECT Hub, ESET Business Account o ESET MSP Administrator**. Ingrese sus credenciales de MSP (inicio de sesión en EMA 2) en los campos **Iniciar sesión** y **Contraseña** de abajo.



4. Haga clic en **Agregar licencias** para confirmar.



5. ESET PROTECT On-Prem ahora sincroniza su estructura desde el portal de MSP hasta el Árbol de grupo estático en el menú **Equipos** en la consola web. La estructura sincronizada se denomina *árbol de MSP*.

> Importar una cuenta de MSP con una gran cantidad de clientes (miles) puede demorar bastante tiempo, incluso horas.

Iniciar configuración de cliente de MSP

Después de importar su cuenta MSP y sincronizar el árbol MSP se sincroniza y puede comenzar a configurar empresas. A partir de la configuración de cliente de MSP, se crean:

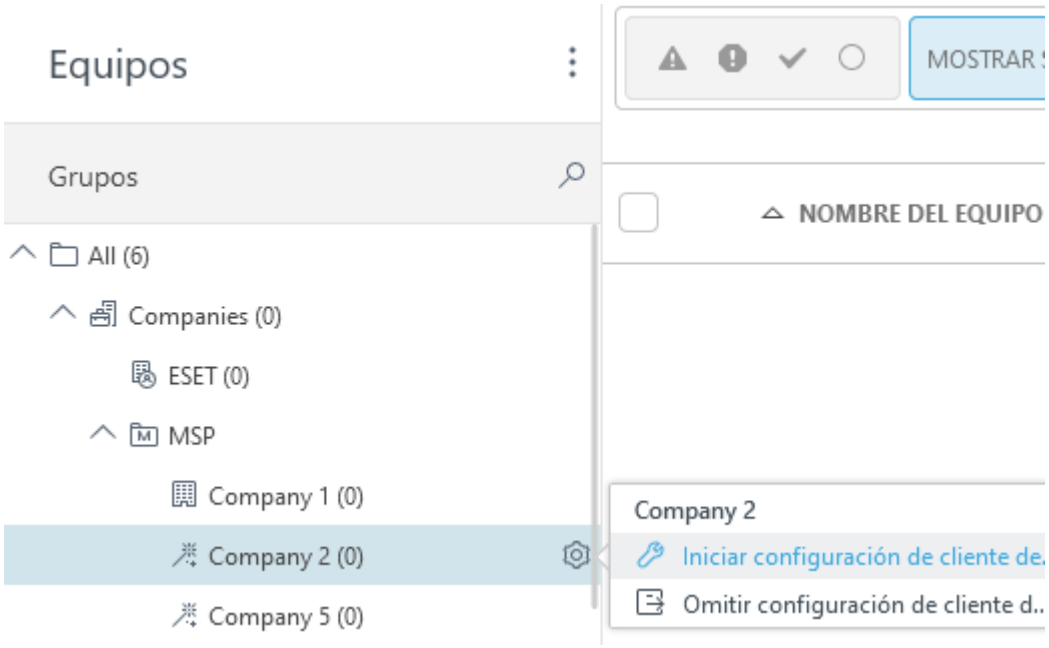
• Un ESET Management personalizado o un Agente agrupado e instalador de producto de seguridad de ESET. La configuración de clientes MSP no es compatible con la creación de instaladores ESET Full Disk Encryption ni instaladores del conector ESET Inspect.

• Un usuario de MSP que puede administrar equipos de la compañía mediante el uso de la consola web.

También puede omitir la configuración de cliente de MSP. Sin embargo, le recomendamos que lo haga.

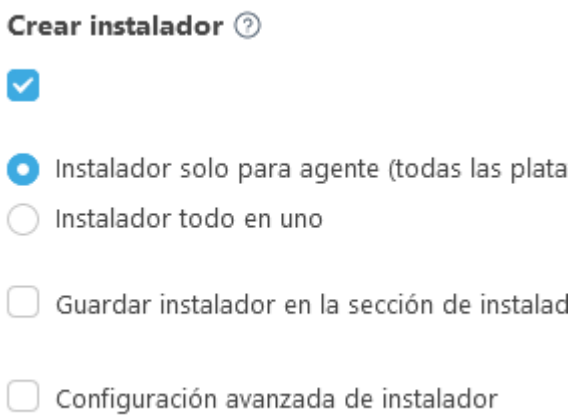
Puede configurar solo una compañía con, al menos, 1 puesto de licencia válido.

1. En la ventana **Equipos**, haga clic en el ícono del engranaje junto a la compañía que quiere configurar y seleccione **Iniciar configuración de cliente de MSP**.



2. Si quiere guardar esta configuración como configuración predeterminada, seleccione la casilla de verificación ubicada debajo de la opción **Recordar la configuración**. Haga clic en **Continuar**.

3. Si quiere crear un instalador personalizado durante la configuración (recomendado), seleccione la casilla de verificación debajo de la opción **Crear instalador**.



4. Puede crear dos tipos de instaladores:

• **Instalador solo del agente (todas las plataformas)**: puede instalar este Instalador de script del agente en ordenadores Windows, macOS y Linux.

• **Instalador todo en uno**: el instalador está compuesto por el agente de ESET Management y el producto de seguridad empresarial de ESET seleccionado (Windows).

Si no ve la opción **Instalador todo en uno**, asegúrese de que haya una licencia asignada a la compañía.

^ He seleccionado el Instalador todo en uno

Producto/Versión: seleccione el producto de seguridad de ESET que se instalará junto con el agente de ESET Management. De forma predeterminada, se selecciona previamente la versión más reciente (recomendada). Puede seleccionar una versión anterior.
Seleccione el idioma en el menú desplegable **Idioma**.
Seleccione la casilla de verificación **Acepto el Acuerdo de licencia de usuario final y confirmo estar de acuerdo con la Política de privacidad**. Consulte el Acuerdo de licencia de usuario final (EULA), los Términos de uso y la Política de privacidad de los productos ESET.

Para guardar el instalador en Instaladores para un uso posterior, marque la casilla de verificación junto a **Guardar instalador en la sección de instaladores**.

^ Configuración avanzada de instalador (recomendado)

Nombre de host del servidor: dirección con la que los agentes de ESET Management se conectan a ESET PROTECT Server. Seleccione otro puerto para la comunicación agente - servidor, de ser necesario. Si modifica el puerto, tiene que modificarlo también para todos los agentes de conexión y, además, en la **Más** > Configuración.

Asegúrese de que todos los dispositivos de cliente que usarán el instalador puedan alcanzar la dirección del **nombre de host del servidor**. Consulte las recomendaciones de entorno de MSP.

Habilitar la configuración del proxy HTTP

Si usa un proxy HTTP (recomendamos usar ESET Bridge), seleccione la casilla de verificación **Habilitar la configuración del proxy HTTP** y especifique la configuración del proxy (**Host**, **Puerto**, **Nombre de usuario** y **Contraseña**) para descargar el instalador a través del proxy y definir la conexión del agente ESET Management al proxy para habilitar el reenvío de comunicaciones entre el agente ESET Management y el servidor ESET PROTECT. El campo **Host** es la dirección del equipo que ejecuta el proxy HTTP. ESET Bridge usa el puerto 3128 de forma predeterminada. Puede definir otro puerto, de ser necesario. Asegúrese de configurar el mismo puerto también en la configuración del proxy de HTTP (consulta la ESET Bridge Política).

> 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.

La casilla de verificación **Utilice una conexión directa si el proxy HTTP no está disponible** está preseleccionada. El asistente aplica la configuración como alternativa para el instalador: no puede anular la selección de la casilla de verificación. Puede deshabilitar la configuración mediante una política de agente de ESET Management:

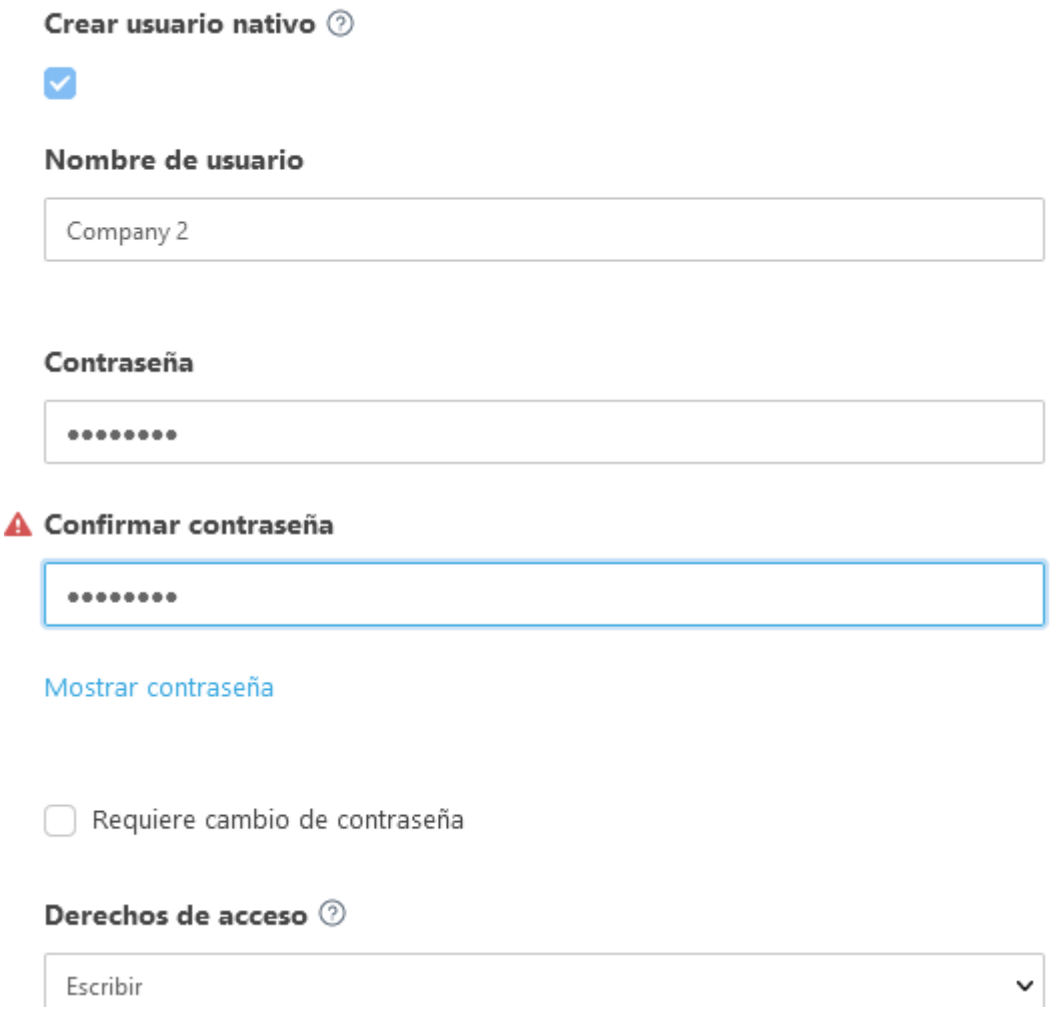
- Durante la creación del instalador: incluya la política en la **Configuración inicial**.
- Tras la ESET Management instalación del agente: asigne la política al equipo.

5. Haga clic en **Continuar** para pasar a la sección **Usuario**.

6. Si quiere crear un nuevo usuario para la compañía (recomendado), seleccione la casilla de verificación junto a la opción **Crear usuario nativo**. El usuario puede iniciar sesión en la consola web y administrar los dispositivos de la compañía. Ingrese un nombre de usuario (que no contenga los caracteres , ; ") y una contraseña válidos para el nuevo usuario.

a.**Requiere cambio de contraseña**: el usuario tiene que modificar la contraseña luego del primer inicio de sesión.

b.**Derechos de acceso**: seleccione si el usuario tiene acceso de **Lectura y uso** o **Escritura** a los objetos de la compañía (equipos, políticas, tareas).



La sincronización de AD no se encuentra disponible para usuarios creados con la configuración de compañía de MSP.

¿Problemas para crear un usuario? Asegúrese de que tiene los permisos necesarios.

Haga clic en **Finalizar** para preparar los instaladores. Haga clic en el enlace y descargue el instalador que necesita. También puede volver a descargar el instalador desde el menú Instaladores en caso de que haya seleccionado guardar el instalador.

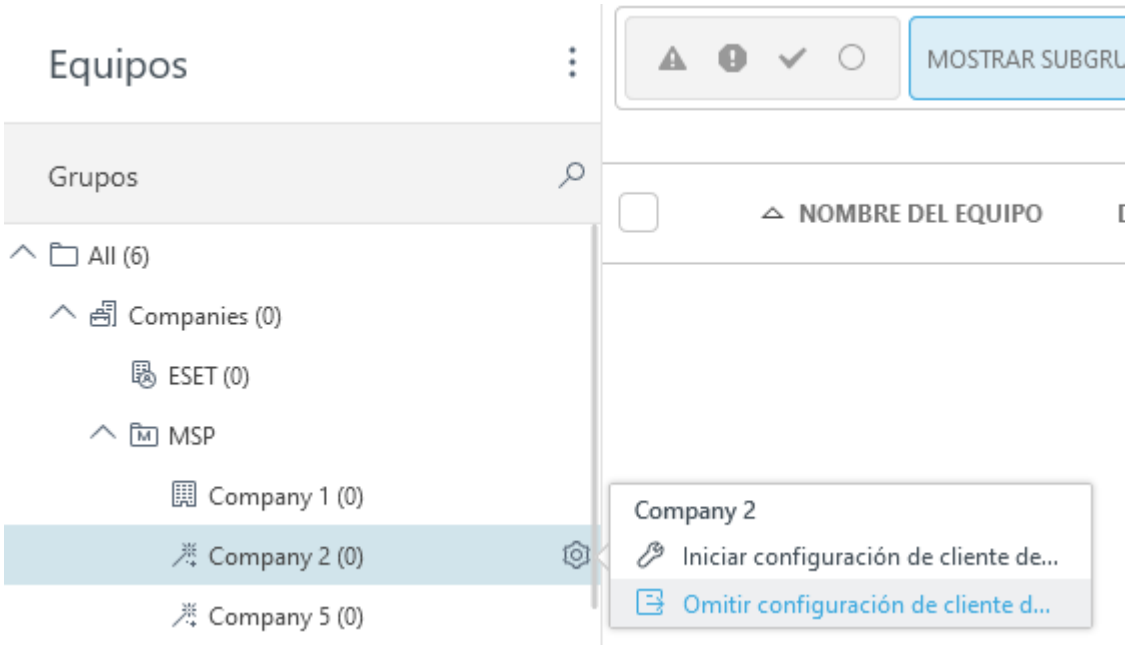
Lea cómo instalar el agente de ESET Management a nivel local o en forma remota.

Omitir configuración de cliente de MSP

Puede **omitir la configuración de cliente de MSP** si no desea realizarla. De manera opcional, puede crear un instalador y un nuevo usuario más adelante. No recomendamos omitir la configuración.

Luego de omitir la configuración, se modifica el ícono de la compañía como si se hubiese configurado:

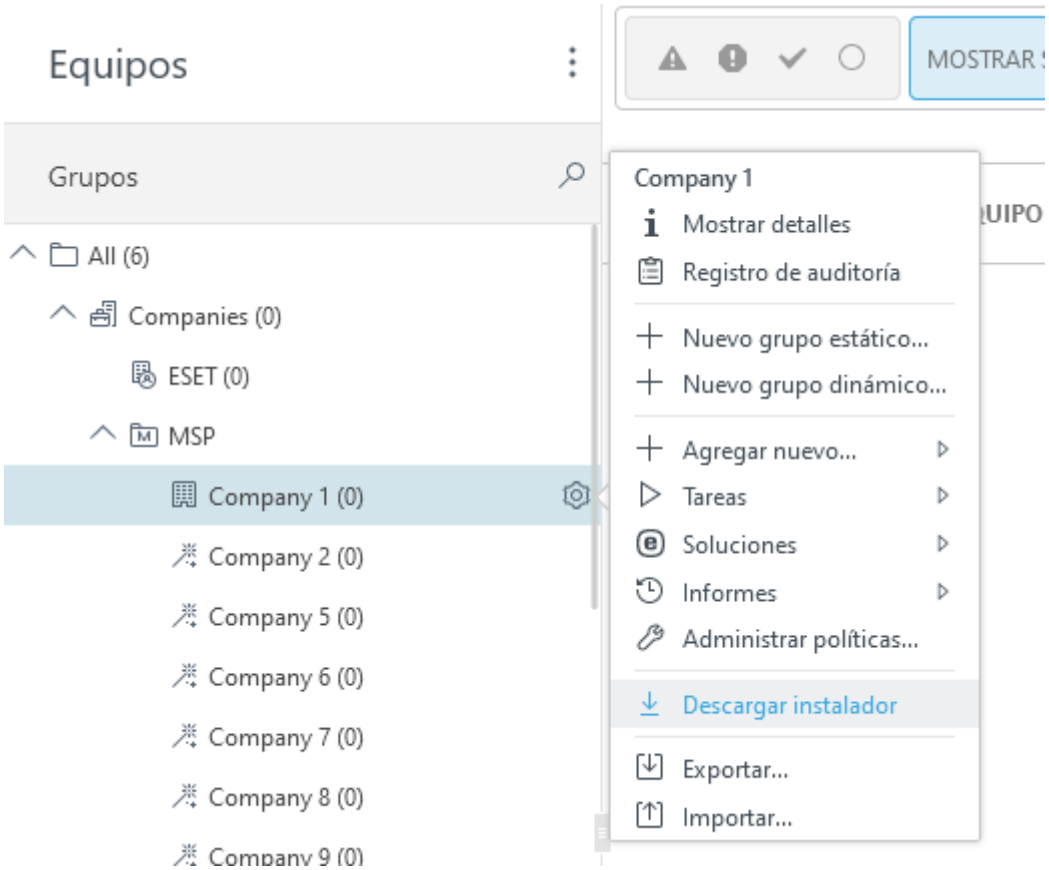
Si omite la configuración, no puede ejecutar el asistente de configuración para la compañía nuevamente en la misma instancia de ESET PROTECT On-Prem



Crear instalador personalizado

1. En la consola web, vaya al menú **Equipos**.

2. Haga clic en el ícono del engranaje junto a la compañía para la cual quiere crear el instalador y seleccione **Descargar instalador**.



3. Puede crear dos tipos de instaladores:

• **Instalador solo del agente (todas las plataformas)**: puede instalar este Instalador de script del agente en ordenadores Windows, macOS y Linux.

• **Instalador todo en uno**: el instalador está compuesto por el agente de ESET Management y el producto de seguridad empresarial de ESET seleccionado (Windows).

Si no ve la opción **Instalador todo en uno**, asegúrese de que haya una licencia asignada a la compañía.

He seleccionado el Instalador todo en uno

Producto/Versión: seleccione el producto de seguridad de ESET que se instalará junto con el agente de ESET Management. De forma predeterminada, se selecciona previamente la versión más reciente (recomendada). Puede seleccionar una versión anterior.
Seleccione el idioma en el menú desplegable **Idioma**.
Seleccione la casilla de verificación **Acepto el Acuerdo de licencia de usuario final y confirmo estar de acuerdo con la Política de privacidad**. Consulte el Acuerdo de licencia de usuario final (EULA), los Términos de uso y la Política de privacidad de los productos ESET.

Para guardar el instalador en Instaladores para un uso posterior, marque la casilla de verificación junto a **Guardar instalador en la sección de instaladores**.

Configuración avanzada de instalador (recomendado)

Nombre de host del servidor: dirección con la que los agentes de ESET Management se conectan a ESET PROTECT Server. Seleccione otro puerto para la comunicación agente - servidor, de ser necesario. Si modifica el puerto, tiene que modificarlo también para todos los agentes de conexión y, además, en la **Más** > Configuración.

Asegúrese de que todos los dispositivos de cliente que usarán el instalador puedan alcanzar la dirección del **nombre de host del servidor**. Consulte las recomendaciones de entorno de MSP.

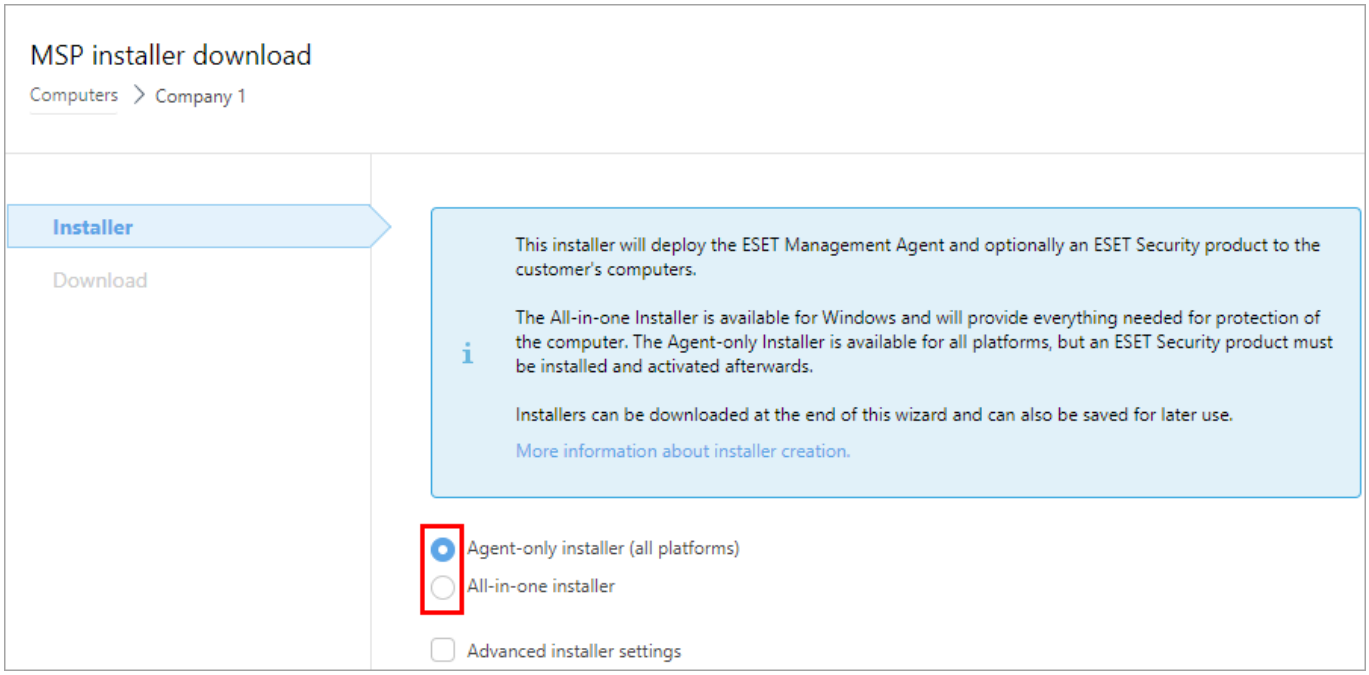
Habilitar la configuración del proxy HTTP

Si usa un proxy HTTP (recomendamos usar ESET Bridge), seleccione la casilla de verificación **Habilitar la configuración del proxy HTTP** y especifique la configuración del proxy (**Host**, **Puerto**, **Nombre de usuario** y **Contraseña**) para descargar el instalador a través del proxy y definir la conexión del agente ESET Management al proxy para habilitar el reenvío de comunicaciones entre el agente ESET Management y el servidor ESET PROTECT. El campo **Host** es la dirección del equipo que ejecuta el proxy HTTP. ESET Bridge usa el puerto 3128 de forma predeterminada. Puede definir otro puerto, de ser necesario. Asegúrese de configurar el mismo puerto también en la configuración del proxy de HTTP (consulta la ESET Bridge Política).

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.

La casilla de verificación **Utilice una conexión directa si el proxy HTTP no está disponible** está preseleccionada. El asistente aplica la configuración como alternativa para el instalador: no puede anular la selección de la casilla de verificación. Puede deshabilitar la configuración mediante una política de agente de ESET Management:

- Durante la creación del instalador: incluya la política en la **Configuración inicial**.
- Tras la ESET Management instalación del agente: asigne la política al equipo.



4. Haga clic en **Crear** para crear el instalador.

5. Haga clic en el enlace y descargue el instalador que necesita.

Usuarios de MSP

Si configura su empresa con la configuración de cliente de MSP, puede crear un tipo especial de usuario nativo (usuario de MSP). Para revisar y editar el usuario, vaya al menú **Más** > **Derechos de acceso** > **Usuarios**.

También puede crear un usuario personalizado de MSP, por ejemplo, para un MSP o un revendedor.

Permisos necesarios

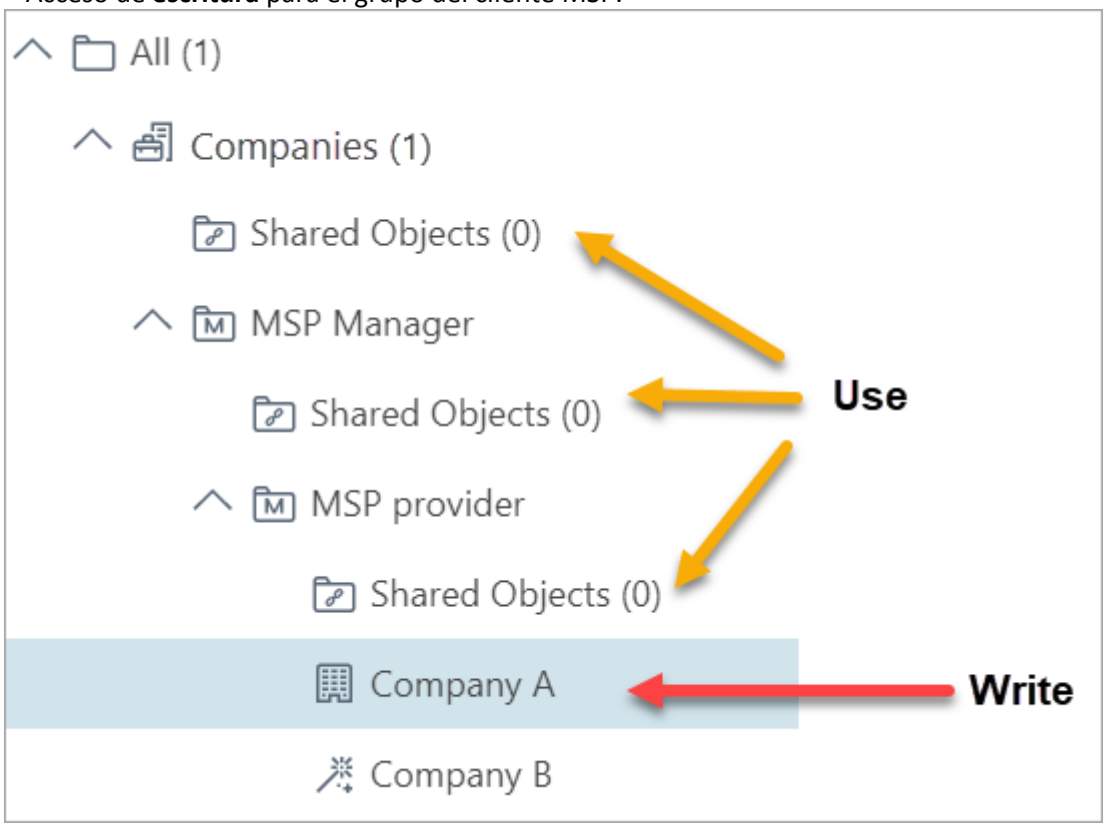
Para crear el nuevo usuario en la Configuración de clientes MSP, necesita los derechos de acceso a la empresa que ha configurado y los **grupos de objetos compartidos**.

Esquema de permisos detallado

Configurar una sola empresa

Derechos de acceso necesarios para crear un usuario durante la configuración de *Empresa A*:

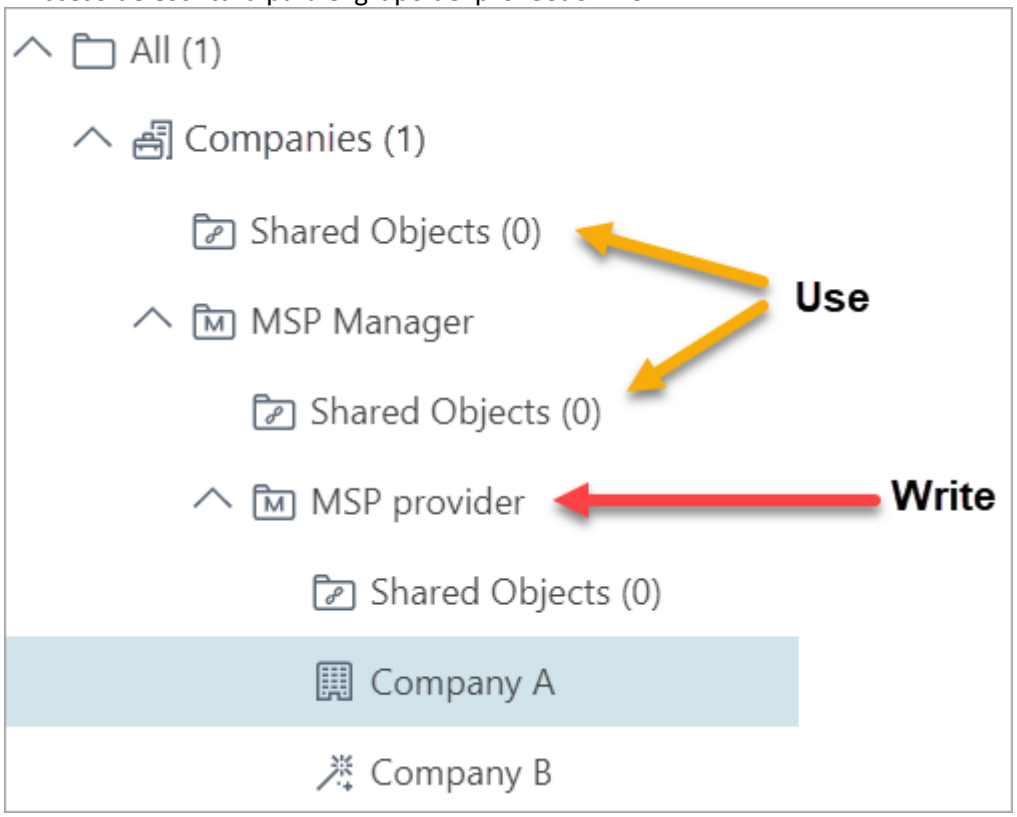
- **Utilice** el acceso para todos los grupos de **Objetos compartidos.**
- Acceso de **escritura** para el grupo del cliente MSP.



Configurar todas las empresas de un MSP

Derechos de acceso necesarios para crear usuarios para todas las empresas que pertenezcan al *Proveedor MSP:*

- **Utilice** el acceso para todos los grupos de **Objetos compartidos.**
- Acceso de **escritura** para el grupo del proveedor MSP.



Tener derechos de acceso significa que el usuario actual (en funciones) tiene conjuntos de permisos asignados con acceso a los grupos mencionados anteriormente. Si no tiene los derechos de acceso necesarios, la configuración de clientes MSP termina con un error.

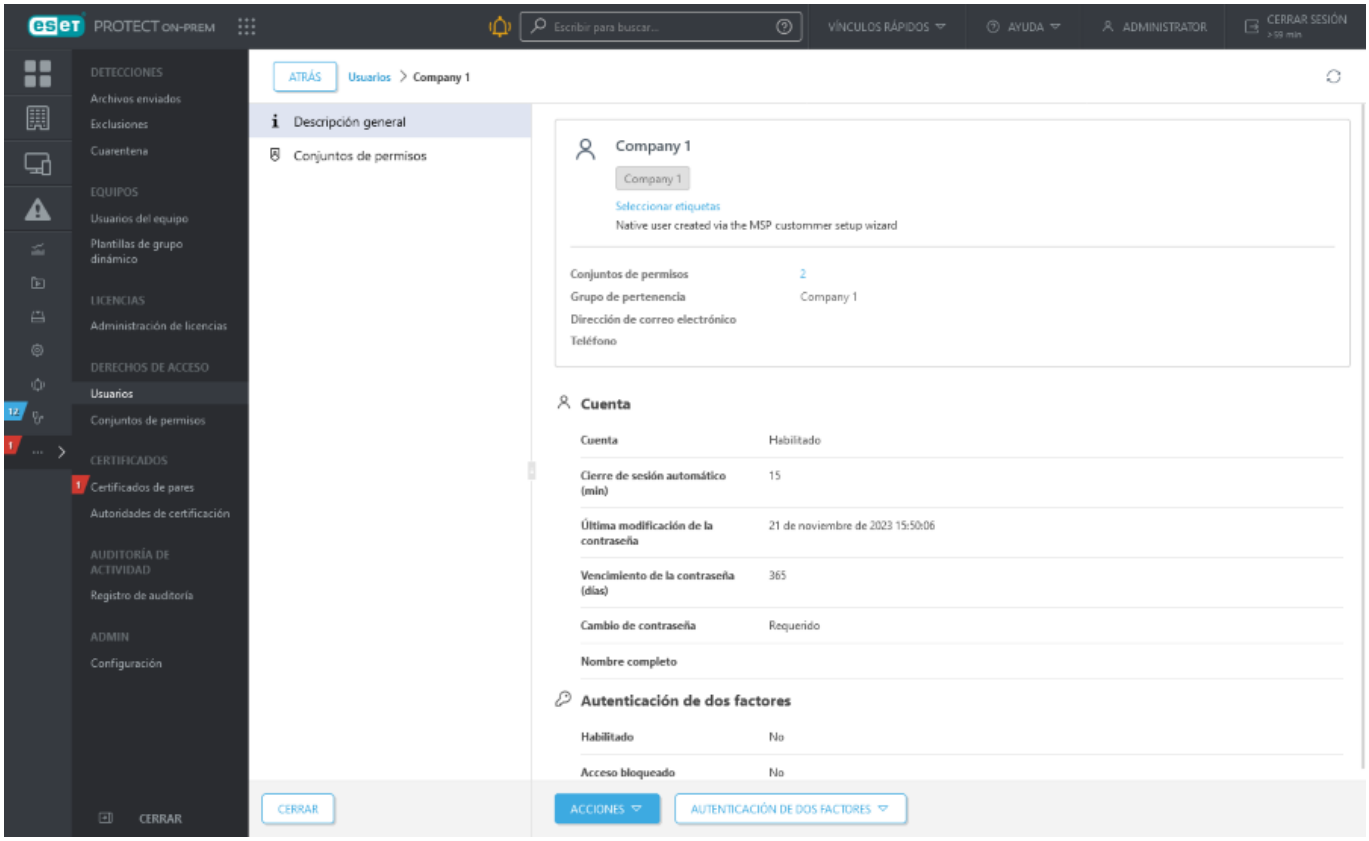
Funciones del usuario de MSP:

- Pueden iniciar sesión en la consola web de ESET PROTECT y administrar dispositivos y otros objetos respecto de los cuales tienen derechos de acceso.
- Pueden crear otro usuario nativo con los mismos permisos o menos permisos.
- No pueden crear Usuarios de equipos. Si es necesario crear un Usuario del equipo, el administrador debe ocuparse de hacerlo.

La sincronización de AD no se encuentra disponible para usuarios creados con la configuración de compañía de MSP.

ESET PROTECT On-Prem posee las siguientes configuraciones para cada nuevo usuario de MSP:

- **Descripción**: usuario nativo creado por medio del asistente de configuración de cliente de MSP
- **Etiquetas**: el usuario se encuentra etiquetado con el nombre de la compañía
- **Grupo hogar**: grupo estático de la compañía
- **Cierre automático de sesión**: a los 15 minutos
- Se habilita la cuenta y no es necesario cambiar la contraseña
- **Conjuntos de permisos**: cada usuario de MSP tiene 2 conjuntos de permisos. Uno para su grupo hogar y otro para los grupos de **Objetos compartidos**.

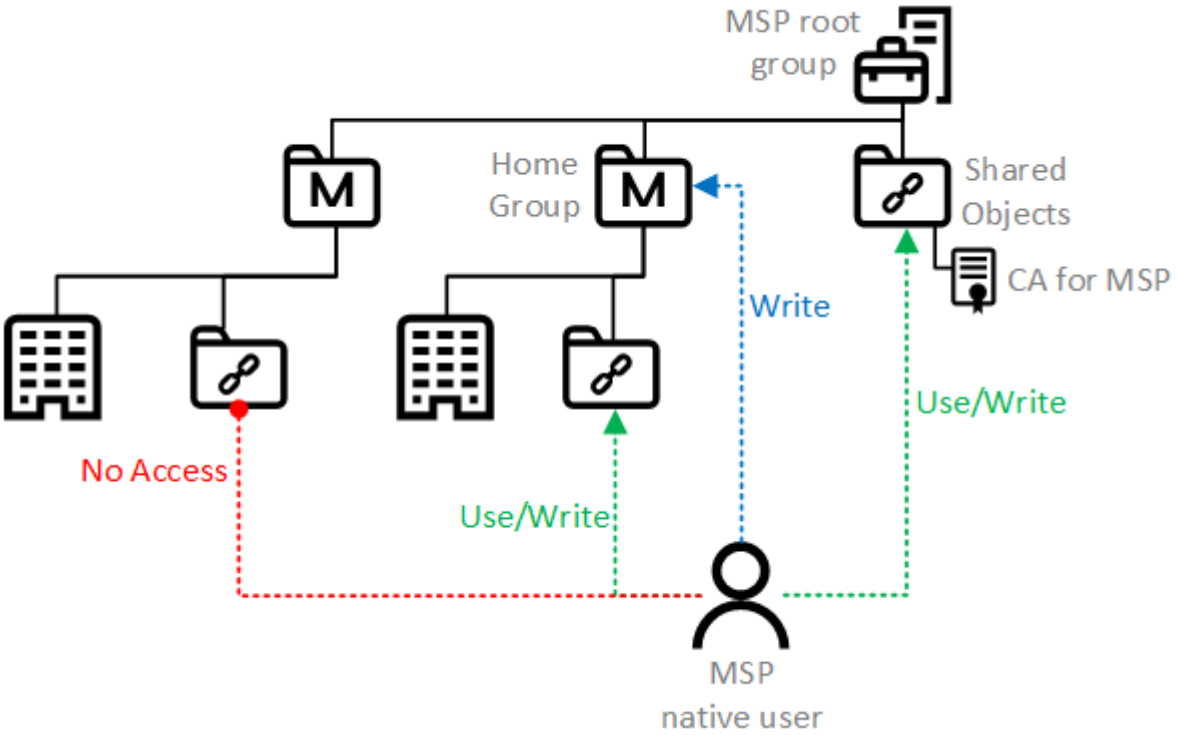


Crear un usuario personalizado de MSP

Puede crear usuarios nativos de la consola web para administrar clientes, por ejemplo, un MSP o revendedor.

1. La compañía de MSP se debe crear en EMA 2.
2. Asegúrese de que la compañía de MSP esté sincronizada en el árbol de MSP.
3. Crear un Usuario nativo. Configuraciones clave para un usuario personalizado de MSP:
    a. El grupo hogar del usuario debe estar configurado con el grupo estático de MSP correspondiente.
    b. Cree y asigne los siguientes conjuntos de permisos para el usuario:
        i. **Escriba** los permisos para el grupo hogar.
        ii. **Use** o **escriba** los permisos para los grupos de **objetos compartidos**.

> El grupo superior **Objetos compartidos** contiene la CA de MSP. Es necesario tener acceso a la CA de MSP para que el usuario pueda crear un instalador.



Esquema de acceso para el usuario personalizado de MSP.

El usuario personalizado de MSP creado a partir de estos pasos resulta elegible para administrar dispositivos de cliente y crear instaladores. No obstante, el usuario no puede administrar ESET PROTECT Server ni importar licencias.

Etiquetado de objetos de MSP

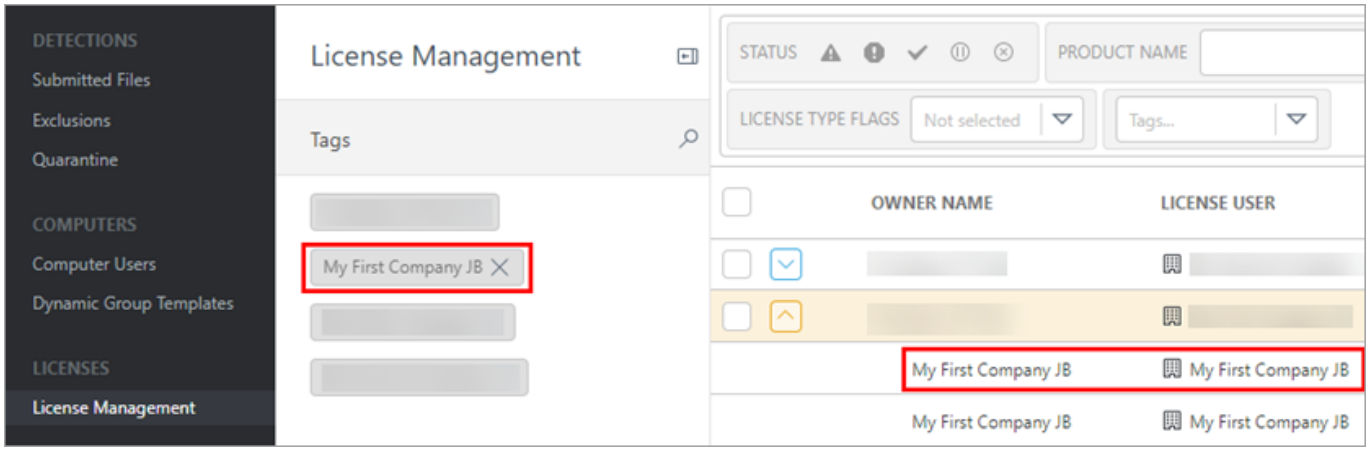
Si importa una cuenta MSP válida a ESET PROTECT On-Prem, habilitará el etiquetado automático de objetos MSP. Los siguientes objetos se etiquetan en forma automática:

- Licencias importadas a través de la cuenta de MSP
- Instaladores
- Usuarios y Conjuntos de permisos creados con la configuración de cliente de MSP

La etiqueta es una forma de rótulo que se usa para mejorar el filtrado de objetos.

- El nombre automático de la etiqueta es el mismo que el **usuario de licencia** (nombre de la compañía en EMA 2, excepto por los caracteres , " que ESET PROTECT On-Prem extrae de la etiqueta).
- Si después de la sincronización cambia el nombre al cliente en EMA 2, las etiquetas no se actualizan.
- Puede agregar más etiquetas personalizadas a cualquier objeto, si así lo desea.
- Puede quitar las etiquetas sin afectar a los objetos etiquetados.

Haga clic en el ícono de ampliación para ver la ficha **Etiquetas**.



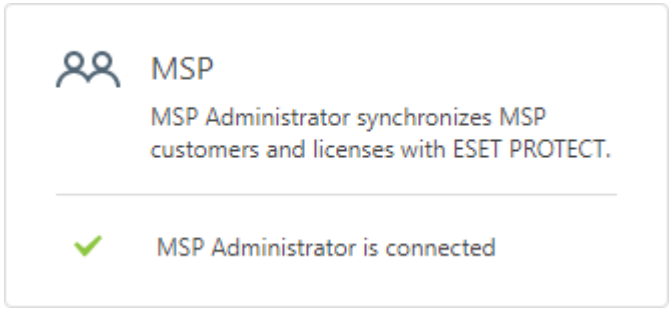
Información general de estado de MSP

En la sección Información general de estado, se proporciona información compleja sobre el estado de ESET PROTECT On-Prem. Si importa una cuenta de MSP, hay un mosaico de MSP disponible con información relacionada con MSP.

Estados de MSP

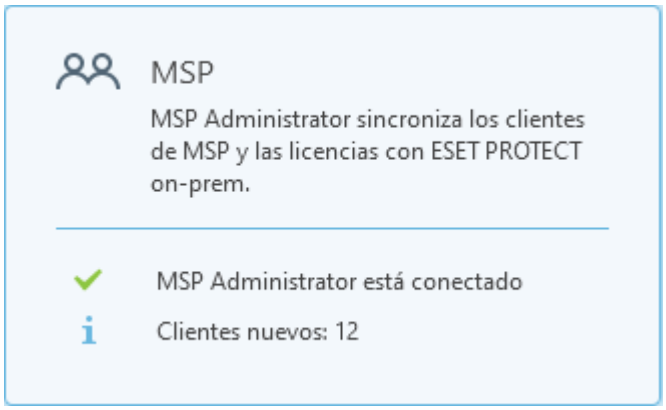
Cuenta sincronizada

Su cuenta está sincronizada y no deben realizarse otras acciones.



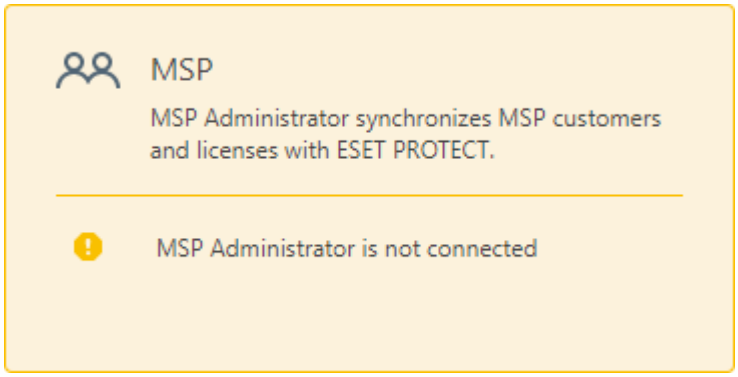
Sincronización en curso

Hay una sincronización en curso de la cuenta de MSP ejecutándose en segundo plano. La sincronización puede demorar varias horas para cuentas grandes. El mosaico se torna blanco luego de la sincronización.



Cuenta desconectada

Hay ciertos grupos de MSP (partes del árbol de MSP) en su estructura de grupos estáticos, pero no se ha importado la cuenta de MSP correspondiente. Esto puede ocurrir si quita su cuenta de MSP de la Administración de licencias.



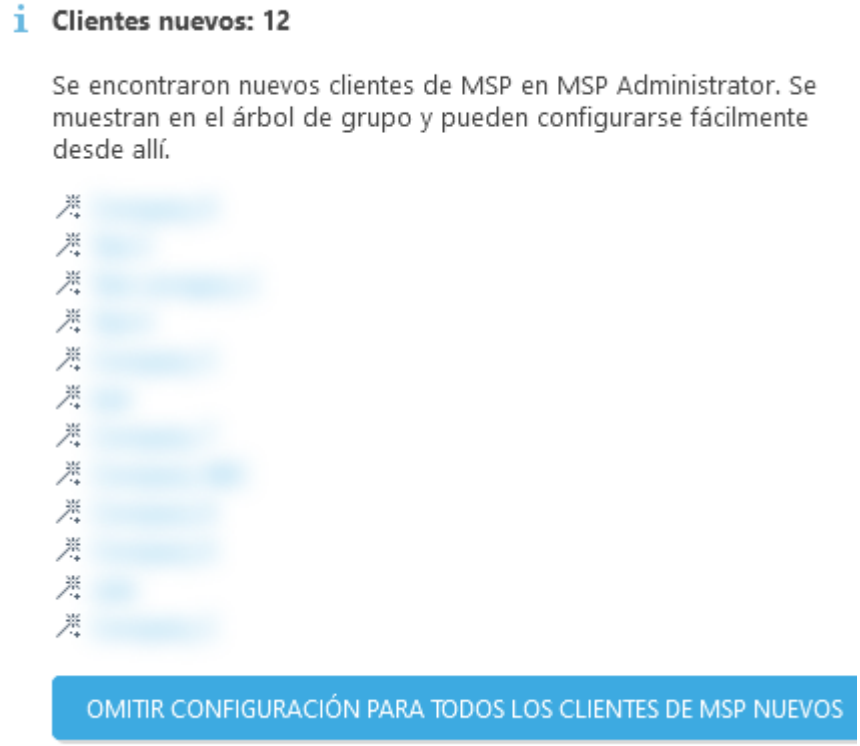
Acciones disponibles

Haga clic en el mosaico de MSP para obtener información detallada.

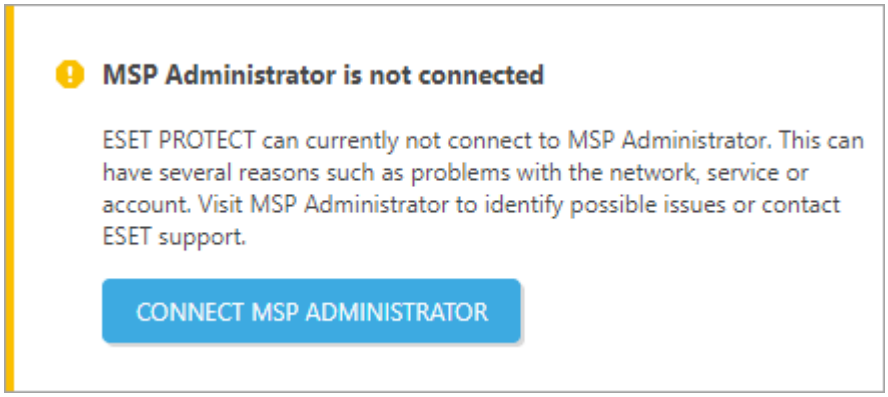
- **Buscar nuevos clientes de MSP**: ejecute la sincronización de licencias a pedido (para actualizar el árbol de MSP).

- **Nuevos clientes**: si tiene algunas compañías no configuradas, puede hacer clic en ellas y seguir las instrucciones que brinda el asistente de configuración de cliente.

- **Omitir configuración para todos los clientes de MSP nuevos**: omita los asistentes de configuración para todas las compañías que no se han configurado.



- **Conectar MSP Administrator**: puede agregar su cuenta de MSP para importar sus licencias y la estructura de MSP.



Cómo quitar una compañía

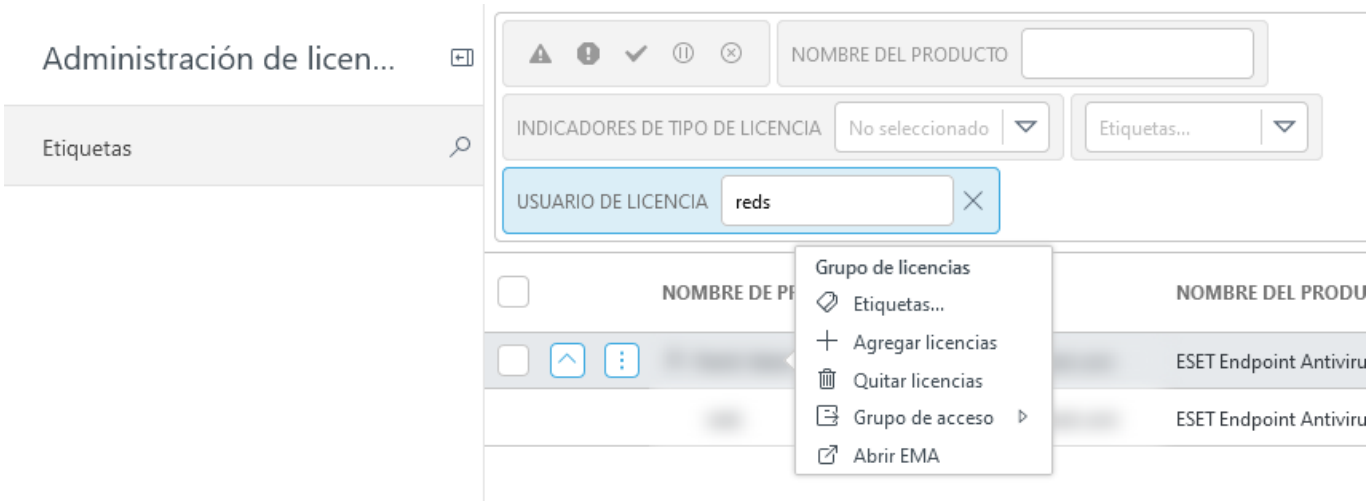
El árbol de MSP se sincroniza con la cuenta de MSP. Debe quitar la cuenta de MSP de la Administración de licencias para desbloquear el árbol de MSP. Una vez que quita la cuenta, todas las compañías bajo la administración de dicha cuenta quedan desvinculadas del árbol de MSP.

Si deja de administrar una compañía, le recomendamos que quite los agentes de ESET Management de los equipos de dicha compañía. No puede quitar la compañía del árbol de MSP sin quitar la cuenta de MSP en su totalidad de la administración de licencias.
El grupo estático de MSP es persistente. Una vez que sincroniza el árbol de MSP, nunca puede quitar el grupo raíz de MSP, sino solo sus grupos secundarios.

Cómo quitar la cuenta y las compañías de MSP del árbol de MSP

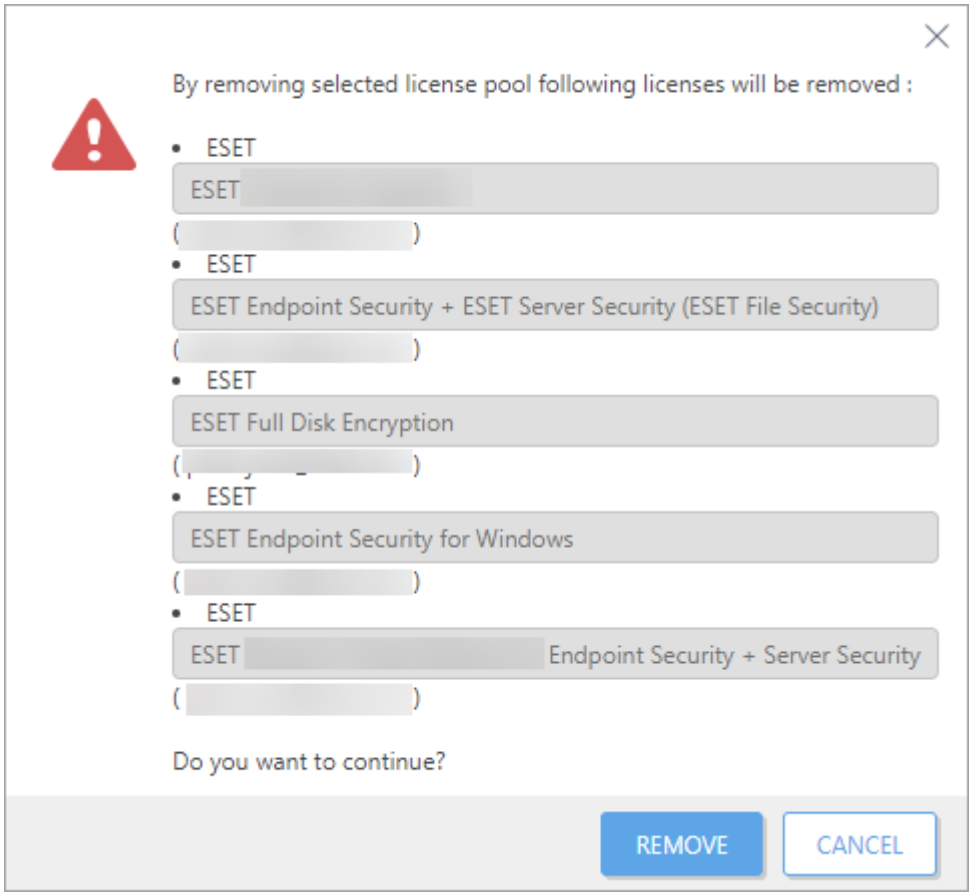
1. Inicie sesión en la consola web de ESET PROTECT y vaya a **Más** > **Administración de licencias**.

2. Haga clic en la licencia que desea quitar > **Quitar licencias**. Tenga en cuenta que, si quita una licencia vinculada a una cuenta de MSP, la cuenta entera y sus licencias vinculadas se quitan de ESET PROTECT On-Prem.



3. Confirme su elección de quitar (desvincular) las licencias incluidas en la lista de la Administración de licencias.

Al quitar cualquier grupo de licencia, se quitan de manera automática todos los otros grupos de licencia asociados con la misma cuenta.
Por ejemplo, las licencias de la *Compañía X* se importaron con las credenciales de la cuenta joe@test.me de EMA 2. Si un usuario quita licencias de la *Compañía X*, todas las licencias importadas desde las cuentas joe@test.me de EBA y EMA 2 se quitan de la Administración de licencias.



4. Aguarde unos instantes luego de la acción y vaya al menú **Equipos**.

5. Los íconos de todas las empresas eliminadas cambian a . Ahora, haga clic y **quite** la compañía que antes formaba parte del árbol de MSP. Solo puede quitar una compañía (su grupo estático) si está vacía.

Luego de quitar la cuenta de MSP de la Administración de licencias, obtiene el estado **Administrador de MSP no está conectado** en la Descripción general del estado. Debe quitar todos los grupos de su ex árbol de MSP (en el menú **Equipos**) para desactivar ese estado.

Actualizaciones automáticas

Hay varios tipos de actualizaciones automáticas de los productos de ESET:

- Actualización automática del agente ESET Management
- Actualización automática de los productos de seguridad de ESET
- Actualización ESET PROTECT On-Prem
- Actualizar componentes de terceros

Consulte también la Política sobre el fin de ciclo de vida de ESET para productos empresariales.
Consulte también ¿Cuáles son los diferentes tipos de versiones y actualizaciones de los productos de ESET?
Las actualizaciones automáticas no funcionan si usa un repositorio sin conexión que no contiene los metadatos (por ejemplo, si ha copiado instaladores en una unidad de red compartida). Use Mirror Tool para crear un repositorio sin conexión que admita actualizaciones automáticas. El repositorio sin conexión de la herramienta de replicación distribuye las actualizaciones automáticas simultáneamente por toda la red (un repositorio en línea distribuye las actualizaciones automáticas de forma gradual).

Actualización automática del agente ESET Management

ESET PROTECT On-Prem ofrece una actualización automática del agente ESET Management en equipos administrados.

Cómo funciona la actualización automática del agente ESET Management

- El agente se actualiza a la versión más reciente compatible con el servidor ESET PROTECT instalado. Esta versión suele ser la versión del servidor ESET PROTECT instalado (por ejemplo, 11.0).

- La actualización automática del agente está habilitada de forma predeterminada. Puede desactivarla en la política del agente ESET Management > **Actualizaciones** > desactive el conmutador **Activar actualización automática**.

- La actualización automática del agente ESET Management se desencadena unas dos semanas después del lanzamiento de la versión más reciente del agente ESET Management en el repositorio.

Cuando haya una versión del agente ESET Management más reciente disponible y la actualización automática aún no se haya producido, puede iniciar la actualización del agente manualmente desde **Dashboard** > Estado de la versión del componente.
Como alternativa, puede utilizar la tarea Cliente de actualización de componentes de ESET PROTECT.

- El diseño de la actualización automática garantiza un proceso de actualización gradual distribuido durante un período más extenso, con el fin de evitar un mayor impacto en la red y los equipos administrados.

- Las actualizaciones automáticas no funcionan si usa un repositorio sin conexión que no contiene los metadatos (por ejemplo, si ha copiado instaladores en una unidad de red compartida). Use Mirror Tool para crear un repositorio sin conexión que admita actualizaciones automáticas. El repositorio sin conexión de la herramienta de replicación distribuye las actualizaciones automáticas simultáneamente por toda la red (un repositorio en línea distribuye las actualizaciones automáticas de forma gradual).

Actualización automática de los productos de seguridad de ESET

La versión de ESET PROTECT On-Prem 9.0 y posteriores incluye una función para mantener los productos de seguridad de ESET actualizados a la última versión en sus equipos administrados.

Las actualizaciones automáticas del producto se habilitan automáticamente en una nueva instalación de ESET PROTECT On-Prem.

- Debe tener un producto de seguridad de ESET válido para poder usar la función de actualizaciones automáticas. Consulte la lista de productos comerciales de ESET compatibles con las actualizaciones automáticas. Otros productos de seguridad de ESET no son compatibles con actualizaciones automáticas; ESET les agregará esta función en el futuro.
- Puede configurar las actualizaciones automáticas a través de una política.
- También, consulte también las Preguntas frecuentes sobre actualizaciones automáticas. La primera actualización automática se realizará cuando se publique una versión futura de la compilación liberada 9.x inicialmente (por ejemplo, 9.1 o 9.0.xxxx.y, donde xxxx es superior a la primera compilación 9.x). Para garantizar la máxima estabilidad de la actualización, las actualizaciones automáticas del producto tienen una distribución retrasada tras el lanzamiento global de una nueva versión del producto de seguridad de ESET. Mientras tanto, la consola web puede informar que el producto de seguridad de ESET está obsoleto.
- Consulte también ¿Cuáles son los diferentes tipos de versiones y actualizaciones de los productos de ESET?
- Las actualizaciones automáticas no funcionan si usa un repositorio sin conexión que no contiene los metadatos (por ejemplo, si ha copiado instaladores en una unidad de red compartida). Use Mirror Tool para crear un repositorio sin conexión que admita actualizaciones automáticas. El repositorio sin conexión de la herramienta de replicación distribuye las actualizaciones automáticas simultáneamente por toda la red (un repositorio en línea distribuye las actualizaciones automáticas de forma gradual).

Siga una de las opciones que se indican a continuación para actualizar los productos de seguridad de ESET de su red a una versión compatible con las actualizaciones automáticas:
- Use la acción de un clic en **Dashboard** > **Descripción general del estado** > **Estado de la versión del componente** > haga clic en el gráfico de barras y seleccione **Actualizar componentes de ESET instalados**.
- En **Equipos**, haga clic en el ícono del engranaje junto al grupo estático **Todos** y seleccione **Tareas** > **Actualizar** > **Actualizar productos ESET**.
- Use la tarea de cliente Instalación de software.

Hay dos formas de actualizar los productos de seguridad de ESET a la versión más reciente:

- Tarea de cliente Instalación de software
- Función de actualizaciones automáticas

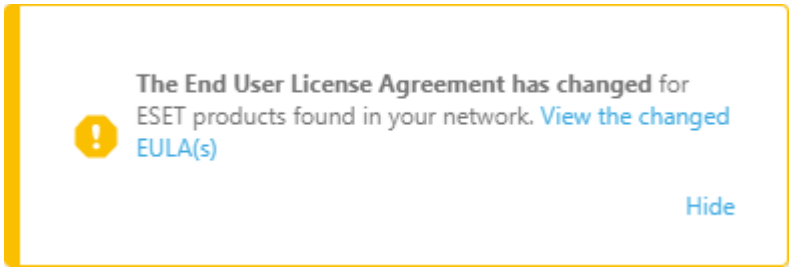
Diferencias entre la tarea de cliente Instalación de software y la función de actualizaciones automáticas:

	Proceso de actualización	Reiniciar tras la actualización	Futuras actualizaciones
Tarea de cliente Instalación de software	El proceso de actualización incluye la reinstalación del producto de seguridad de ESET.	La actualización de un producto de seguridad de ESET requiere un reinicio inmediato del equipo por motivos de seguridad (para garantizar la funcionalidad completa del producto de seguridad de ESET actualizado).	Manual: el administrador debe iniciar cada actualización futura ejecutando la tarea de cliente Instalación de software; consulte las opciones disponibles más arriba.

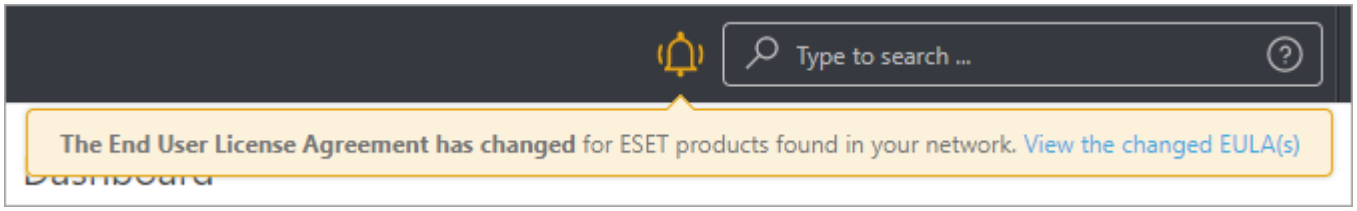
	Proceso de actualización	Reiniciar tras la actualización	Futuras actualizaciones
Actualizaciones automáticas	El proceso de actualización no incluye la reinstalación del producto de seguridad de ESET.	La actualización del producto de seguridad de ESET requiere un reinicio del equipo, pero no inmediatamente (el reinicio no es obligatorio). El administrador de ESET PROTECT On-Prem puede aplicar la actualización y el reinicio del equipo de forma remota desde la consola web mediante la tarea Apagar cliente del equipo con la casilla de verificación **Reiniciar equipos** seleccionada.	Automática: actualizaciones automáticas de productos de seguridad de ESET compatibles cuando se publica una nueva versión (la actualización se retrasa por motivos de estabilidad). Puede aplicar manualmente la comprobación de actualizaciones de productos de seguridad de ESET mediante la tarea Buscar actualizaciones de productos.

Acuerdos de licencia para el usuario final actualizados de productos de seguridad de ESET administrados

La consola web ESET PROTECT informa al administrador de si hay disponible un acuerdo de licencia para el usuario final (EULA) actualizado de un producto de seguridad de ESET administrado.

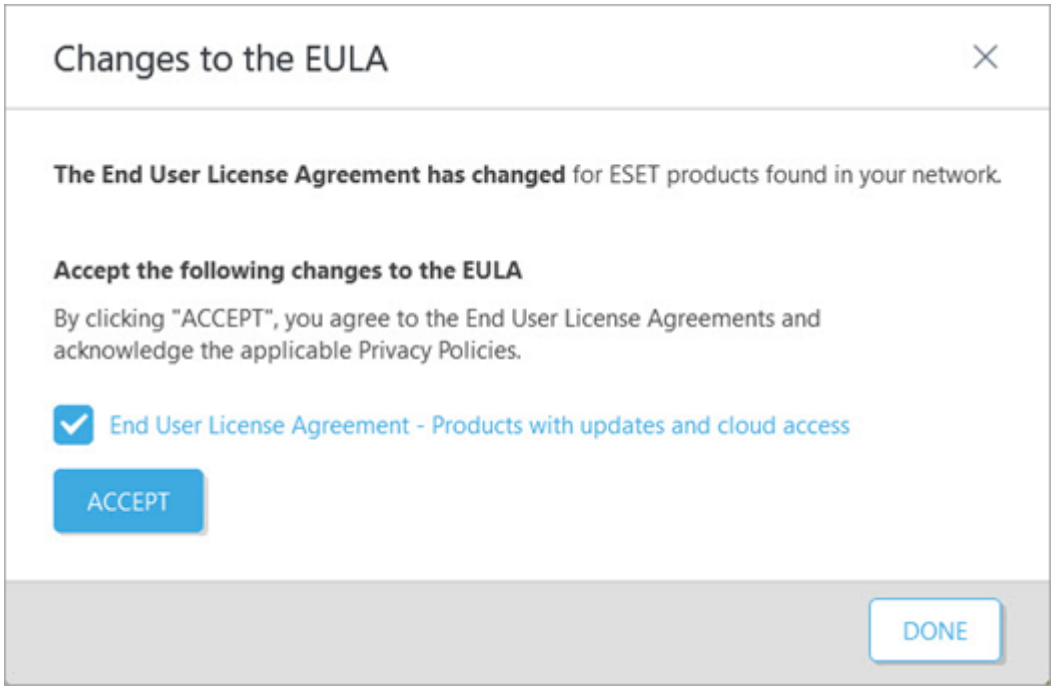


Haga clic en **Ver los EULA modificados** para ver los detalles o en **Ocultar** para mover la notificación bajo un ícono de campana amarillo en la barra de herramientas superior.

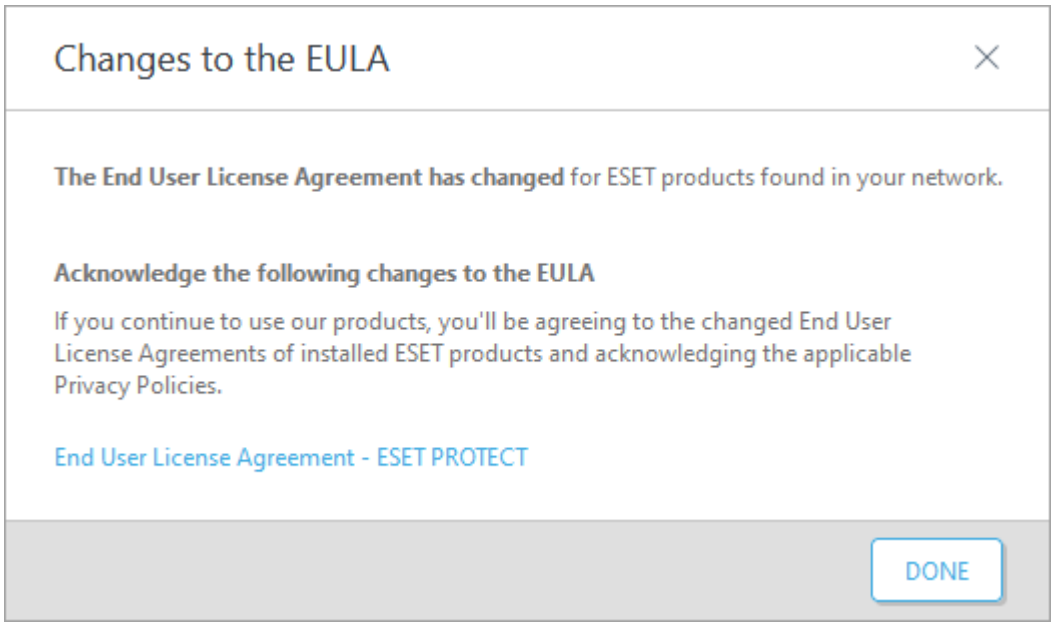


Cuando hace clic en **Ver los EULA modificados**, aparece una ventana nueva con detalles sobre el producto de seguridad de ESET y sus cambios en el EULA:

- Si tiene versiones anteriores de productos de seguridad de ESET que no admiten actualizaciones automáticas (por ejemplo, ESET Endpoint 8.x y versiones anteriores), haga clic en **Aceptar** para aceptar el EULA actualizado y permitir la actualización a una versión compatible con actualizaciones automáticas.



- Si tiene productos empresariales de ESET compatibles con actualizaciones automáticas (por ejemplo, la versión de ESET Endpoint 9 y versiones posteriores), recibirá una notificación sobre el EULA actualizado, pero no tiene que aceptarlo (el botón **Aceptar** no está disponible) para actualizar los productos de seguridad de ESET a versiones posteriores.



Configurar las actualizaciones automáticas del producto

Puede configurar las actualizaciones automáticas mediante la política de funciones **Actualizaciones automáticas** que abarca los productos de seguridad de ESET compatibles con grupo estático **Todos** como destino predeterminado.

Cambie los destinos integrados de la política de actualizaciones

automáticas

En la consola web de ESET PROTECT, haga clic en **Políticas** > expanda **Políticas integradas** > haga clic en la política > seleccione **Cambiar asignaciones** >ajuste los destinos > haga clic en **Finalizar**.

Configurar actualizaciones automáticas

Cree una nueva política de **actualizaciones automáticas** para configurar las actualizaciones automáticas.

1. Inicie sesión en la consola web de ESET PROTECT y haga clic en **Políticas** > **Nueva política** > **Configuración**.

2. Seleccione **Funciones comunes** > **Actualización** en el menú desplegable y configure las opciones de política:

   • **Cambio automático de perfiles**: haga clic en **Editar** y asigne un perfil de actualización según los perfiles de conexión de red.

   • **Actualizaciones automáticas**: las actualizaciones automáticas están habilitadas de forma predeterminada.

> Para deshabilitar las actualizaciones automáticas, desactive el conmutador **Actualizaciones automáticas**. Consulte también Optar por la exclusión de las actualizaciones automáticas.

   • **Detener actualizaciones en** > **Seleccionar versión**: opcionalmente, puede configurar la versión del producto de seguridad de ESET que detendrá la actualización automática:

   oHaga clic en **Seleccionar del repositorio** y seleccione la versión.

   oEscriba la versión; puede usar * como comodín, por ejemplo, 9.*/9.0.*/9.0.2028.*.

> Por ejemplo, si escribe 9.0.*, se instalarán todas las revisiones de la versión secundaria 9.0.

> Este ajuste no se aplica a las actualizaciones de seguridad y estabilidad instaladas automáticamente, sea cual sea la versión definida o el estado de configuración de las actualizaciones automáticas. Consulte también ¿Cuáles son los diferentes tipos de versiones y actualizaciones de los productos de ESET?

3. Haga clic en **Asignar** para seleccionar destinos de la política (grupos o equipos individuales).

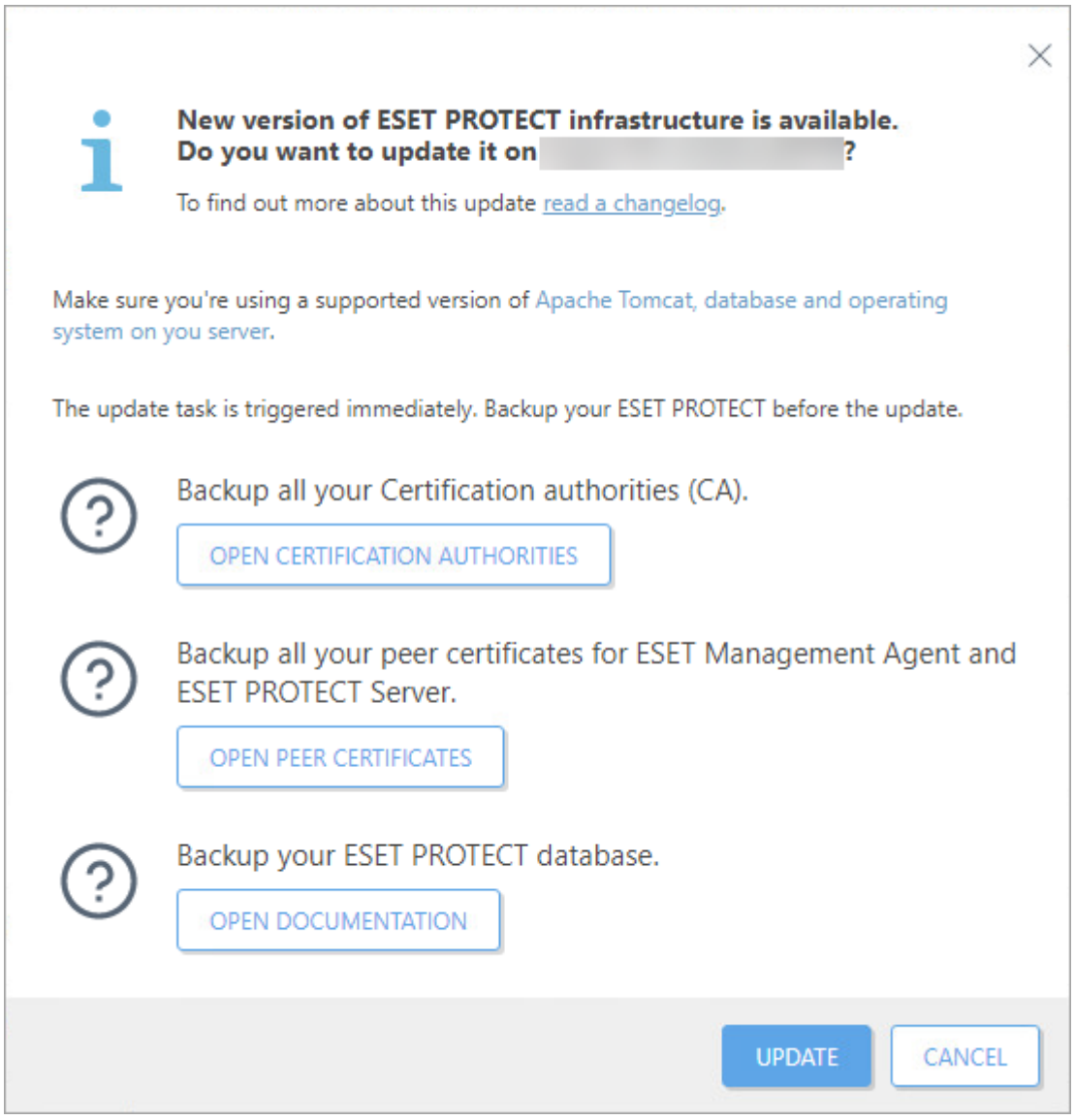
> Asegúrese de que la política de actualizaciones automáticas integrada no sobrescribe la configuración de la política de actualizaciones automáticas que ha creado. Obtenga más información sobre la aplicación de las políticas en los clientes.

4. Haga clic en **Finalizar**.

Actualización ESET PROTECT On-Prem

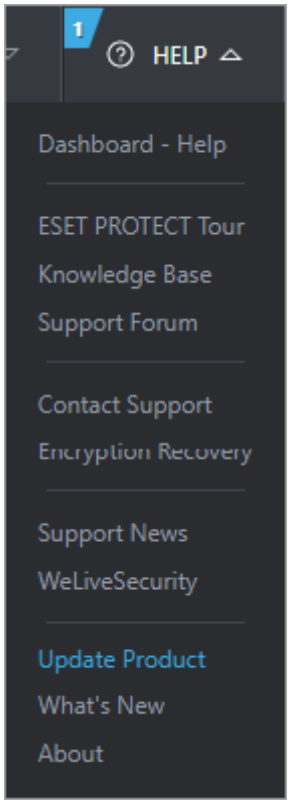
El Servidor ESET PROTECT a menudo revisa si hay actualizaciones disponibles para la infraestructura de ESET PROTECT.

Cuando hay una actualización disponible, aparece una ventana:



Puede obtener información sobre los cambios de actualización de ESET PROTECT On-Prem disponibles haciendo clic en **leer un registro de cambios**.

Si no selecciona realizar la actualización, puede mostrar la ventana de actualización al hacer clic en **Ayuda** > **Actualizar el producto**:



Únicamente los usuarios que pueden ejecutar la tarea de cliente de ESET PROTECT Actualización de los componentes podrán ver la notificación de actualización.

Asegúrese de estar ejecutando una versión compatible de Apache Tomcat, la base de datos y el sistema operativo en su servidor.

1. Haga clic en el botón **Autoridades de certificación abiertas** y haga una copia de seguridad de todas sus AC.

2. Haga clic en el botón **Certificados de pares abiertos** y haga una copia de seguridad de todos sus certificados.

3. Haga clic en el botón **Documentación abierta** y haga una copia de seguridad de la base de datos de ESET PROTECT.

4. Haga clic en el botón **Actualizar**.

5. Seleccione la casilla de verificación **Acepto el Acuerdo de licencia de usuario final y confirmo estar de acuerdo con la Política de privacidad**. Consulte el Acuerdo de licencia de usuario final (EULA), los Términos de uso y la Política de privacidad de los productos ESET.

6. Haga clic en el botón **Actualizar**. Se programa una actualización de ESET PROTECT Server: en **Tareas**, puede buscar una nueva tarea de cliente que actualice los componentes de ESET PROTECT en el equipo en el que está instalado ESET PROTECT Server. Se cerrará su sesión en la consola web cuando comience la actualización. Puede iniciar sesión una vez que se complete la actualización. Puede comprobar la versión de ESET PROTECT On-Prem en **Ayuda** > Acerca de.

Para actualizar componentes de ESET PROTECT en los dispositivos conectados al Servidor ESET PROTECT a su versión más reciente, puede desencadenar la tarea de ESET PROTECT Actualización de los componentes directamente desde la ventana de actualización.

No todos los componentes de ESET PROTECT se actualizan automáticamente: algunos componentes requieren una actualización manual.

ESET PROTECT On-Prem admite la actualización automática de agentes ESET Management en equipos administrados.

Actualizar componentes de terceros

Además de los componentes de ESET, ESET PROTECT On-Prem usa componentes de terceros que requieren una actualización manual.

En la consola web de ESET PROTECT, haga clic en **Enlaces rápidos** > **Componentes del servidor** para ver los componentes de terceros con una versión posterior disponible.

- Se recomienda instalar la versión más reciente de los componentes de terceros lo antes posible. La versión más reciente disponible puede variar en función del sistema operativo que se use para ejecutar el servidor de ESET PROTECT.
- El aparato virtual de ESET PROTECT no informa las actualizaciones disponibles para los componentes de terceros.

La consola web de ESET PROTECT recomienda una actualización para versiones anteriores a las indicadas a continuación:

Componente de terceros:	Versión:	Notas:	Instrucciones de actualización
Microsoft SQL Server	2019 (versión 15.0.4335.1)	Determine su versión y su edición del Motor de base de datos SQL Server e instale la actualización acumulativa más reciente.	Servidor de base de datos
MySQL	8.0.0.0	Haga clic en **Ayuda** > **acerca de** en la consola web de ESET PROTECT para ver la versión de la base de datos instalada.	Servidor de base de datos
Sistema operativo	Windows Server 2016	ESET PROTECT On-Prem no informa las actualizaciones disponibles para Linux.	Sistema operativo
Apache Tomcat	9.0.82	Determine la versión de Apache Tomcat instalada: • Windows: vaya a *C:\Program Files\Apache Software Foundation\[Tomcat carpeta]* y abra el archivo *RELEASE-NOTES* en un editor de texto y verifique el número de versión. • Linux: ejecute el comando de terminal: `tomcat version`	Apache Tomcat
Java	17.0	Determine la versión de Java instalada: • Windows: abra el símbolo del sistema y ejecute: `java -version` • Linux: ejecute el comando de terminal: `java -version`	Java Runtime Environment

Componente de terceros:	Versión:	Notas:	Instrucciones de actualización
Apache HTTP Proxy	-	**Apache HTTP Proxy usuarios** A partir de ESET PROTECT On-Prem 10.0, ESET Bridge reemplaza a Apache HTTP Proxy. Apache HTTP Proxy alcanzó el soporte limitado. Si usa Apache HTTP Proxy, recomendamos migrar a ESET Bridge.	Migrar a ESET Bridge

El componente de conector/administración de dispositivos móviles (MDM/MDC) de ESET PROTECT (solo on-prem) llega al fin de ciclo de vida en enero de 2024. Leer más. Le recomendamos migrar a Cloud MDM.

Preguntas frecuentes

Lista de preguntas

16. No veo información en la ventana del tablero, ¿por qué?
17. ¿Cómo puedo actualizar mi Producto de seguridad ESET?
18. Cómo puedo cambiar el sufijo en la dirección de la consola web

---

Cómo resolver el **error de inicio de sesión: ¿Se produjo un error en la conexión con el estado "No conectado"**?

Verifique si el servicio del servidor ESET PROTECT o Microsoft SQL está funcionando. De lo contrario, inícielo. En caso contrario inícielo. Si está funcionando, reinicie el servicio, actualice la consola de web y, luego, intente volver a iniciar sesión. Para obtener más información, consulte Inicio de sesión de la solución de problemas.

¿Para qué se usa el grupo "**Perdidos y encontrados**"?

Cada equipo que se conecta con el servidor ESET PROTECT y no es un miembro de ningún grupo estático se muestra automáticamente en este grupo. Puede trabajar con el grupo y los equipos dentro de él como con los equipos en cualquier otro grupo estático. El grupo se puede volver a nombrar o mover debajo de otro grupo pero no se puede eliminar.

¿Cómo crea un perfil de actualización doble?

Consulte nuestro artículo de la base de conocimiento de ESET para conocer las instrucciones paso a paso.

¿Cómo actualiza la información en una página o en una sección de la página sin actualizar toda la ventana del explorador?

Haga clic en **actualizar** en el menú contextual en la parte superior derecha de una sección de la página.

¿Cómo realiza una instalación silenciosa del agente ESET Management?

Seguir los métodos le permite realizar instalaciones silenciosas:

- Comando GPO o SCCM
- Tarea de implementación del agente
- ESET Remote Deployment Tool

El sensor RD no detecta todos los clientes en la red.

El sensor RD escucha pasivamente la comunicación de la red en la red. Si los equipos no se están comunicando, no

son listados por el sensor RD. Verifique la configuración de DNS para asegurarse de que los problemas con la búsqueda de DNS no están evitando la comunicación.

¿Cómo restablezco el conteo de detecciones activo que se muestra en ESET PROTECT On-Prem después de limpiar las detecciones?

Para restablecer la cantidad de detecciones activas, se debe iniciar una exploración completa (en profundidad) mediante ESET PROTECT On-Prem en los equipos destino. Si limpió una detección en forma manual, puede marcarla como resuelta.

¿Cómo configuro la expresión CRON para el intervalo de conexión del agente ESET Management?

P_REPLICATION_INTERVAL acepta una expresiónCRON.

¿“R R/20 * * * es predeterminado? *” que significa conectar a segundos al azar (R=0-60) cada minuto 20 al azar (por ejemplo 3, 23, 43 o 17, 37, 57). Los valores a azar se deben usar para el equilibrio de carga a tiempo. Entonces, cada agente ESET Management se conecta en un tiempo al azar diferente. Si se utiliza un CRON preciso, por ejemplo, "0 * * * * ? *", todos los agentes con esta configuración se conectarán simultáneamente (cada minuto en :00 segundo); en esta ocasión existirán picos de carga en el servidor. Para obtener más información, consulte Intervalo de la expresión Cron.

¿Cómo crea un nuevo Grupo dinámico para la implementación automática?

Consulte nuestro artículo de la base de conocimiento para conocer las instrucciones paso a paso.

Al importar un archivo que contiene un listado de equipos para agregar a ESET PROTECT On-Prem, ¿de qué formato debe ser el archivo?

Archivo con las siguientes líneas:

All\Group1\GroupN\Computer1
All\Group1\GroupM\ComputerX

All es el nombre requerido del grupo raíz.

¿Qué certificados de terceros se pueden usar para firmar los certificados de ESET PROTECT?

El certificado tiene que ser certificado CA (CA intermitente) con el indicador 'keyCertSign' de la restricción 'keyUsage'. Esto significa que se puede usar para firmar otros certificados.

¿Cómo se puede **restablecer la contraseña del Administrador** para la consola web (que se ingresó durante la configuración de los sistemas operativos Windows)?

Es posible restablecer la contraseña al ejecutar el instalador del servidor y elegir **Reparar**. Tenga en cuenta que tal vez necesite la contraseña para la base de datos de ESET PROTECT si no usó la Autenticación de Windows durante la creación de la base de datos. Vea el artículo de la base de conocimientos sobre este tema.

- Tenga cuidado, algunas de las opciones de reparación pueden eliminar datos almacenados.
- El restablecimiento de la contraseña deshabilita 2FA.

¿Cómo **reinicio la contraseña de Administrador** desde una consola web (Linux, ingresado durante la configuración)?

Si tiene otro usuario en ESET PROTECT On-Prem con derechos suficiente, debe poder restablecer la contraseña de la cuenta del administrador. Sin embargo, si el administrador es la única cuenta (ya que se crea en la instalación) en el sistema, no puede restablecer esta contraseña. Vea el artículo de la base de conocimientos sobre este tema.

¿Cómo soluciona los problemas si su **sensor RD** no detecta nada?

Si se detecta su sistema operativo como un dispositivo de red, no se enviará a ESET PROTECT On-Prem como un equipo. Los dispositivos de red (impresoras, enrutadores) se filtran. El sensor RD se compiló con *libpcap version 1.3.0*, verifique que tiene esta versión instalada en su sistema. El segundo requerimiento es una red en modo puente desde su máquina virtual donde se instaló el sensor RD. Si se cumplen estos requerimientos, ejecute nmap con detección de sistema operativo (http://nmap.org/book/osdetect-usage.html) para ver si puede detectar el sistema operativo en su equipo.

No veo elementos en la ventana de plantillas de grupos dinámicos, ¿por qué?

Seguramente sus usuarios no tengan los permisos adecuados. Los usuarios solo pueden ver las plantillas si están en un grupo estático en el que se hayan asignado a dichos usuarios como mínimo permisos de **Lectura** en Plantillas de grupos dinámicos.

No veo información en la ventana del tablero, ¿por qué?

Seguramente sus usuarios no tengan los permisos adecuados. Los usuarios deben tener permisos en los ordenadores y también en el Panel principal para que se muestren los datos. Consulte el ejemplo de conjunto de permisos.

¿Cómo puedo actualizar mi Producto de seguridad ESET?

Use la tarea Instalación de software y seleccione el producto que desea actualizar.

Cómo puedo cambiar el sufijo en la dirección de la consola web

Si la dirección de su consola web es, por ejemplo, *10.1.0.5/era* y le gustaría cambiar el sufijo *era*, no cambie el

nombre de la carpeta. No se recomienda cambiar la dirección, pero, si necesita hacerlo, cree un enlace en la carpeta *webapps* con un nombre diferente.

Por ejemplo, en Linux o en aparato virtual, puede usar el siguiente comando:

```
ln -sf /var/lib/tomcat/webapps/era/ /var/lib/tomcat/webapps/protect
```

Después de ejecutar este comando en la terminal, también podrá acceder a su consola web en 10.1.0.5/protect (cambie la dirección IP para usted).

Acerca de ESET PROTECT On-Prem

Para abrir la ventana **Acerca de** ingrese a **Ayuda** > **Acerca de**. En esta ventana, se brinda información detallada sobre la versión de ESET PROTECT On-Prem. La parte superior de la ventana incluye información acerca de la cantidad de dispositivos cliente conectados y de licencias activas. Asimismo, verá la lista de módulos del programa instalados, su sistema operativo y una licencia que usa ESET PROTECT On-Prem para descargar actualizaciones del módulo (la misma licencia que se usó para activar ESET PROTECT On-Prem). La información sobre su base de datos, como el nombre, la versión, el tamaño, el nombre de host y el usuario, se muestra en esta ventana.

Para obtener instrucciones sobre cómo saber qué versión es del componente ESET PROTECT, consulte nuestro Artículo sobre la base de conocimiento.

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